CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de **Cibersegurança**

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

## Energia

Caracterização, Regulamentação e Recomendações no Âmbito do Observatório de Cibersegurança

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

# Índice

# Índice de Gráficos

# Índice de Figuras

# Índice de Tabelas

# Introdução

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

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

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

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

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

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

Os setores considerados para efeitos da consideração como OSE são os seguintes: 1) Energia; 2) Transportes; 3) Bancário; 4) Infraestruturas do mercado financeiro; 5) Saúde; 6) Fornecimento e distribuição de água potável; 7) Infraestruturas digitais. Cada um destes setores pode incluir

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

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

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

subsetores a considerar, bem como tipos de entidades claramente identificados na lei. Estas considerações serão incluídas nos respetivos capítulos.

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

# Contexto do relatório

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

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

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

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

# Objetivos do relatório

Este relatório teve como principais objetivos:

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

O relatório elaborado atenderá aos seguintes pontos na análise setorial:

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

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

# Contexto Geral

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

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

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

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

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

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

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

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

**Tabela 1 - Setores, Subsetores e Tipos de Entidades**

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

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

# Análise do questionário dirigido aos Reguladores de Serviços Essenciais

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

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

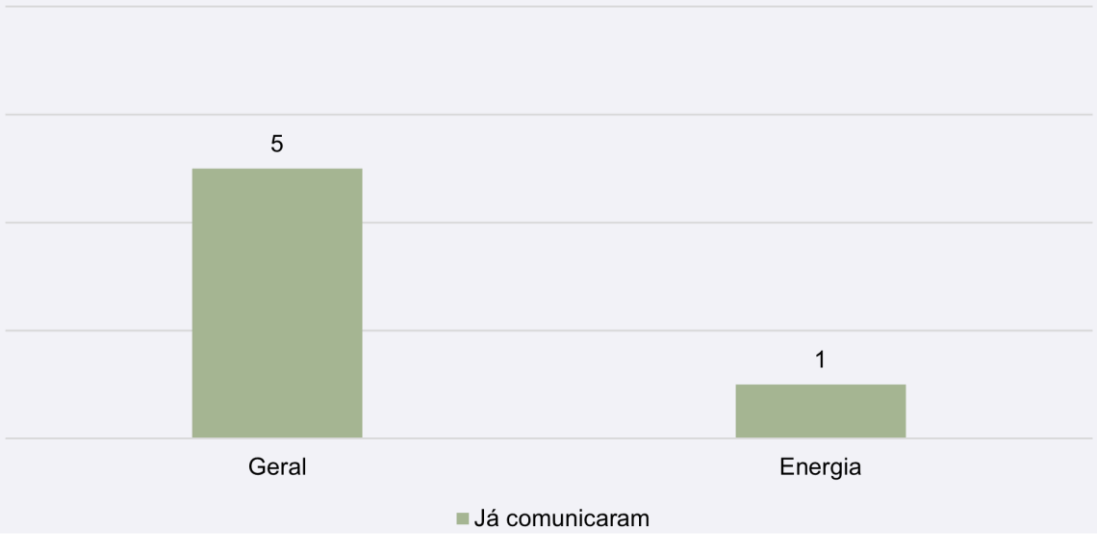
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez,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

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

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

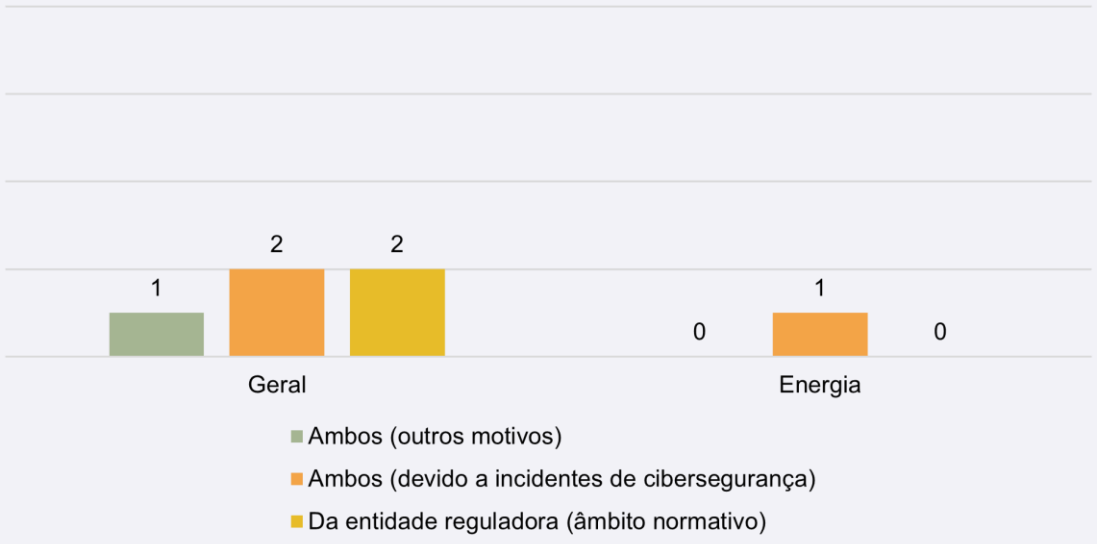
## 1. Comunicação entre OSE e respetivos Reguladores

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




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

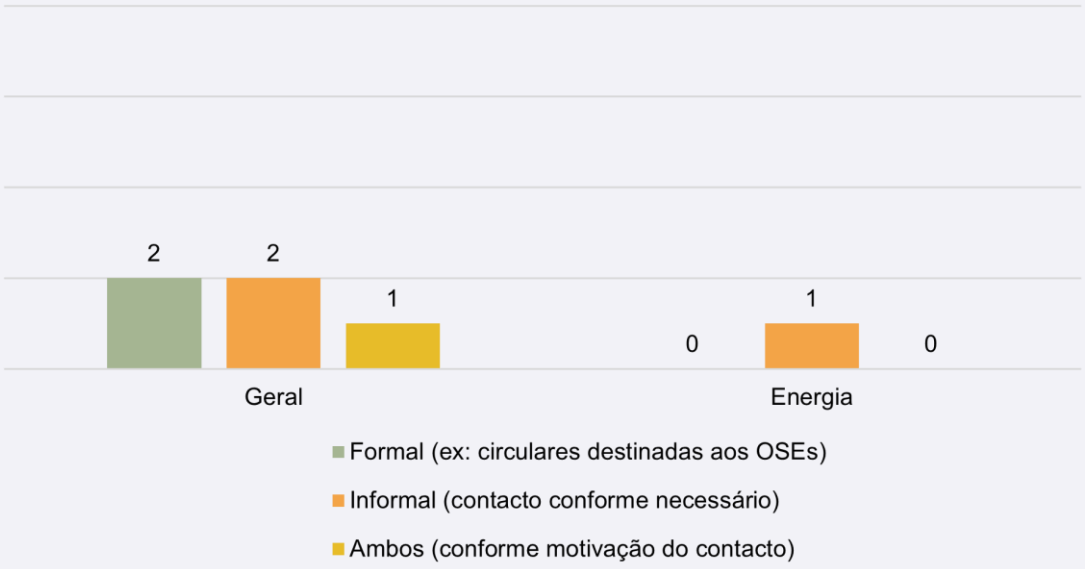
**Gráfico 2 - Origem da comunicação sobre questões de cibersegurança**



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

O regulador do setor bancário foi bastante explícito sobre quais foram esses outros motivos. O mesmo indicou que existe uma interação normal de diálogo no âmbito da supervisão feita pelo regulador, como nas situações recorrentes de análise e avaliação ou de inspeções nas instalações dos OSE. Há também uma interação periódica que ocorre no seio da participação no Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO), fórum esse que inclui momentos específicos para a discussão sobre riscos e incidentes de cibersegurança. Para além destes, existe a comunicação espoletada pela ocorrência de incidentes, em que tanto pode haver a necessidade de o regulador informar os OSE sobre incidentes ocorridos, por exemplo, com o sistema SWIFT[7], ou quando os próprios OSE comunicam detalhes sobre os incidentes que os afetaram a si. Por fim, há a comunicação realizada pontualmente através de instrumentos regulamentares emitidos pela entidade reguladora sobre matérias relevantes de forma transversal.

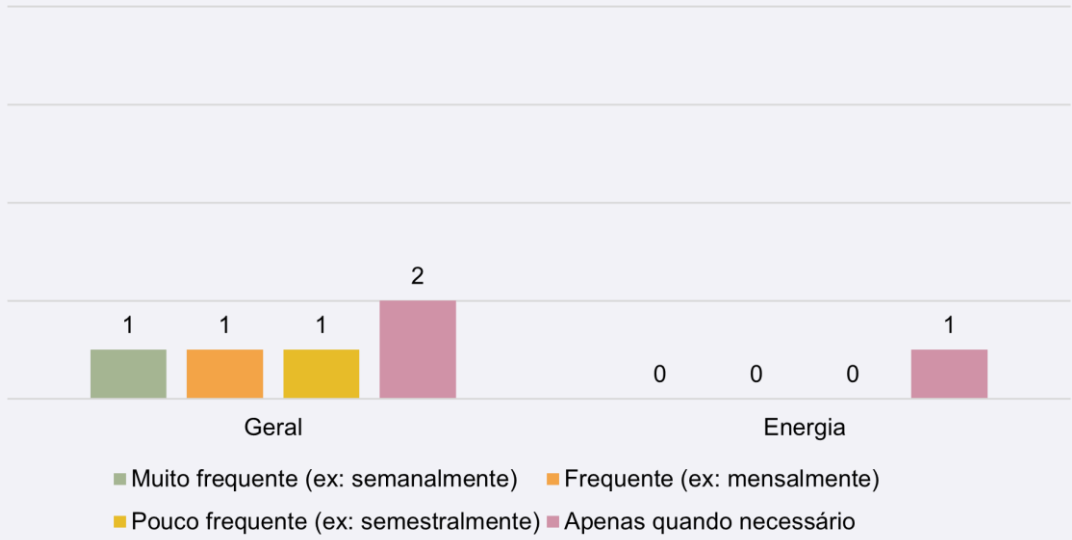
**Gráfico 3 - Formalidade da comunicação realizada**




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

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, consoante a necessidade (um deles sendo o setor da energia) e apenas um regulador indicou haver comunicação tanto de caráter formal como mais informal.

**Gráfico 4 - Frequência da comunicação**



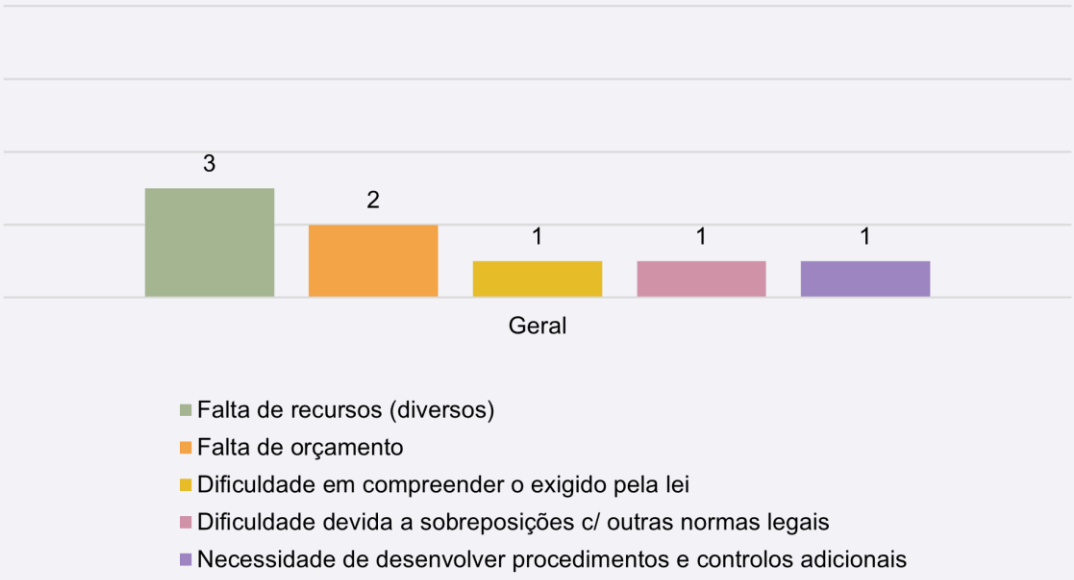

No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. O setor da energia foi um dos que respondeu que a comunicação é realizada apenas quando necessário, não havendo frequência ou periodicidade estimadas.

## 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. O setor da energia mencionou não ter sentido impacto. 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.

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

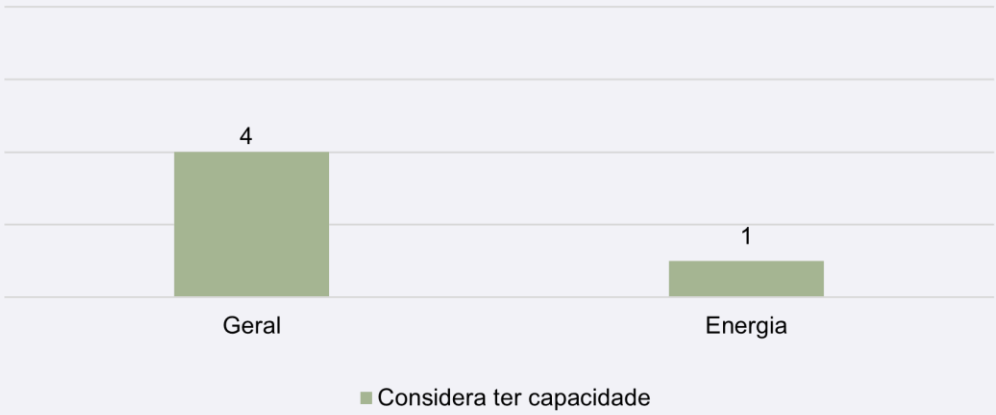
O setor da energia não é abordado pois nenhum inquirido mencionou dificuldades.

Dificuldades relativas à sobreposição com outras normas legais foram indicadas apenas por um dos reguladores. Já a necessidade de desenvolver procedimentos e controlos adicionais foi unicamente indicada por outro regulador.

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[8].

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

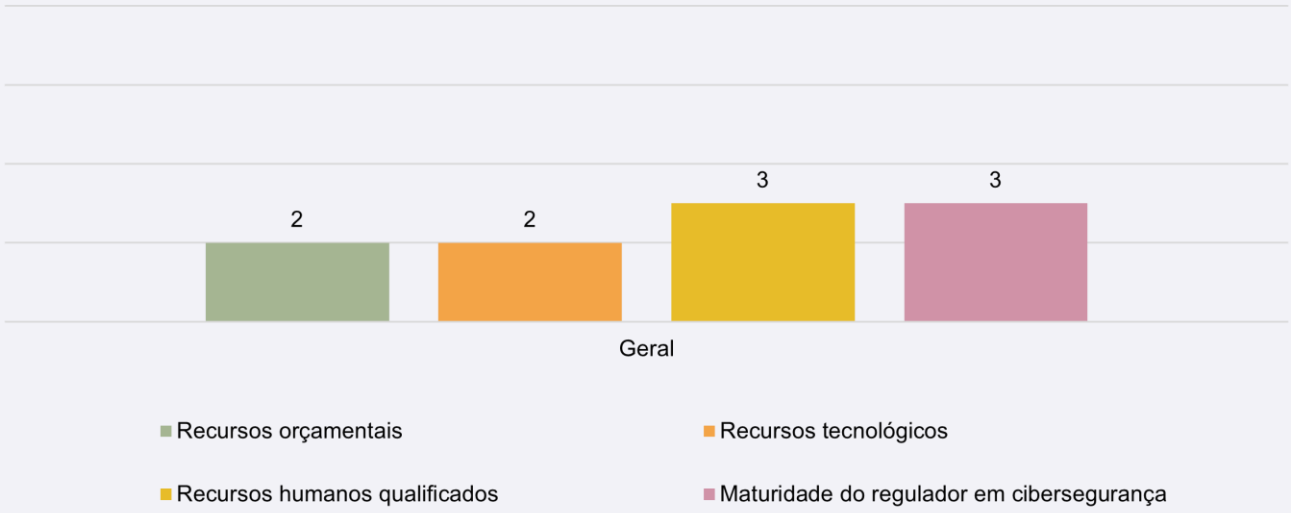
**Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência**




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

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 energia, é um dos que considera 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**



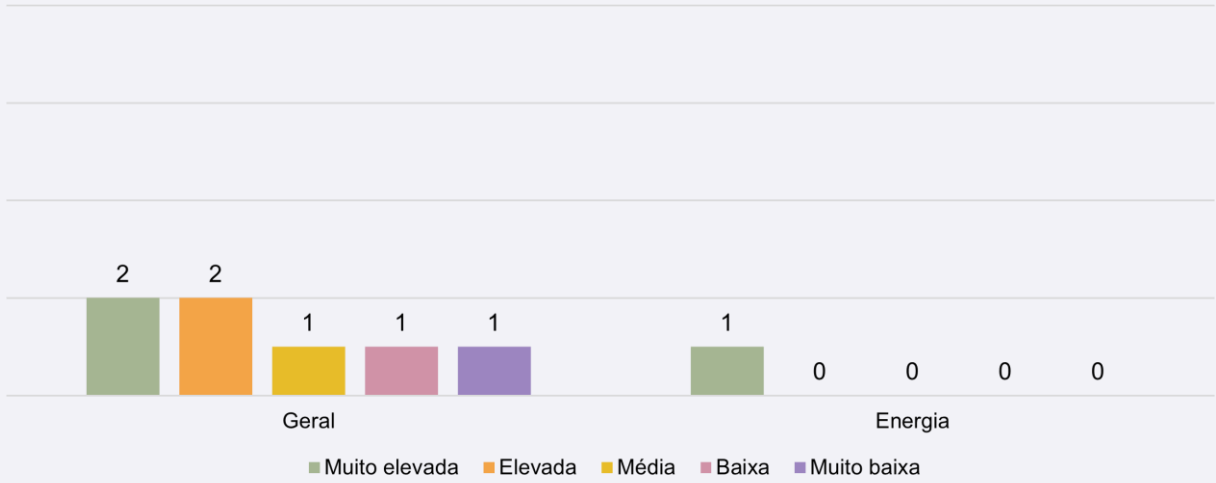

Entre os reguladores que consideram não ter essa capacidade, dois deles indicaram não ter suficientes recursos orçamentais, dois mencionaram suficientes recursos tecnológicos e três suficiente maturidade em cibersegurança. Além destes, três das entidades que consideram não ter a capacidade de realizar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

A falta de recursos humanos qualificados em cibersegurança é um tema que surge repetidamente nas respostas tanto dos reguladores como dos OSE. Dados do Fórum Económico Mundial evidenciam uma escassez global de cerca 4 milhões de profissionais em cibersegurança[9], escassez essa que coloca diversas dificuldades não só aos reguladores e aos OSE dos setores em análise, mas também noutras organizações e setores de atividade. Este tema é explorado em maior detalhe na análise do **Gráfico 44**.

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

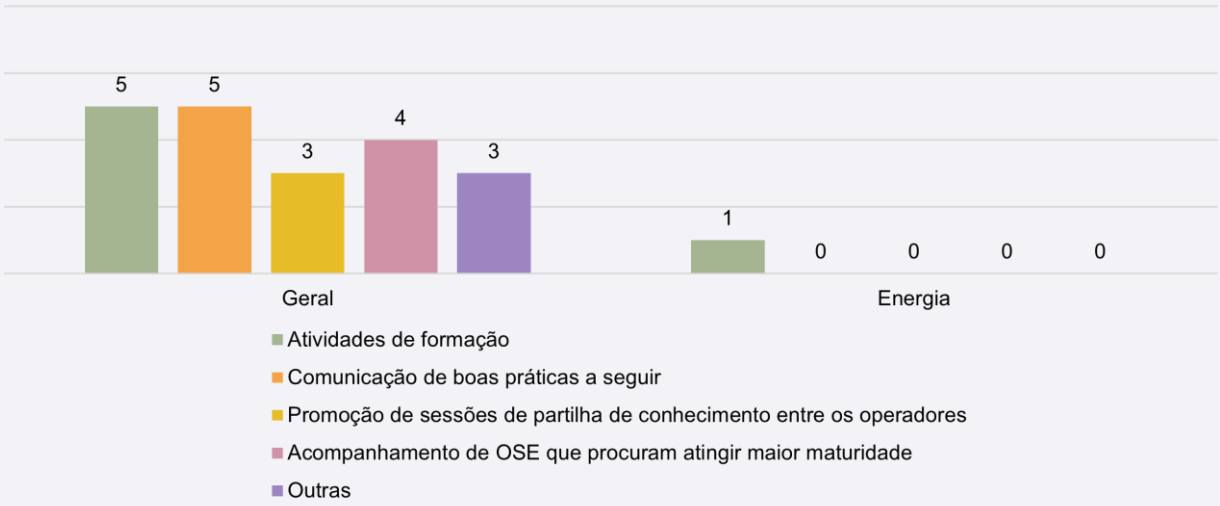
## 4. Maturidade em cibersegurança no setor

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




A perceção dos reguladores sobre a maturidade em cibersegurança dos operadores varia entre os diversos reguladores dos diferentes setores. Entre os inquiridos, apenas dois dos oito reguladores consideram que a maturidade nos seus setores é muito elevada, sendo um deles o regulador da energia.

**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 inquirido, incluindo mais uma vez o regulador do setor da energia, promovem atividades de formação num esforço para aumentar a maturidade no setor. Verifica-se o mesmo número de reguladores a recomendar boas práticas a seguir. O regulador do setor da energia não efetua comunicação de boas práticas.

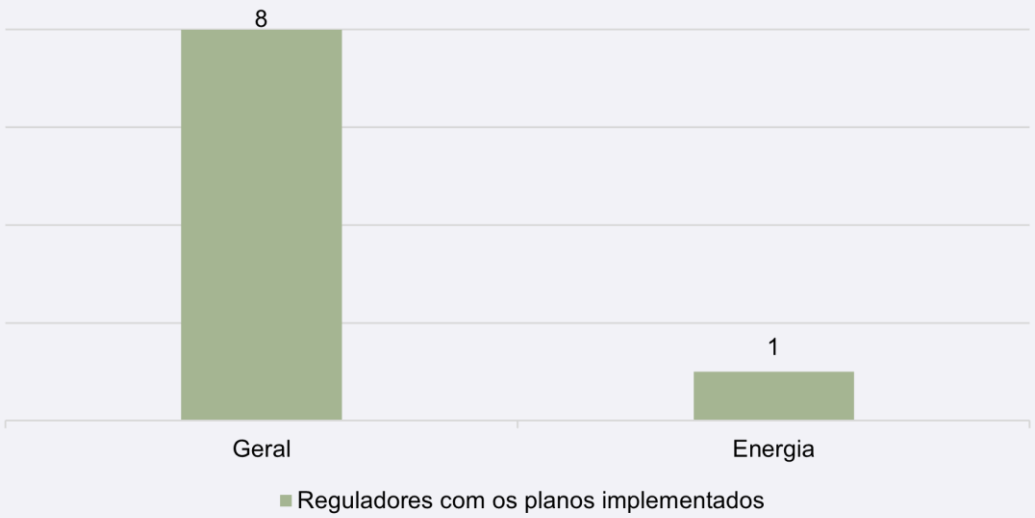
Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo. Quanto ao acompanhamento de OSE que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento.

**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 (sendo um desses seis o regulador do setor da energia) não consideram ter suficientes profissionais capacitados na área.

Novamente, estes resultados prender-se-ão com a escassez global de profissionais em cibersegurança já referida no **Gráfico 8** e que é analisada em detalhe no **Gráfico 44**.

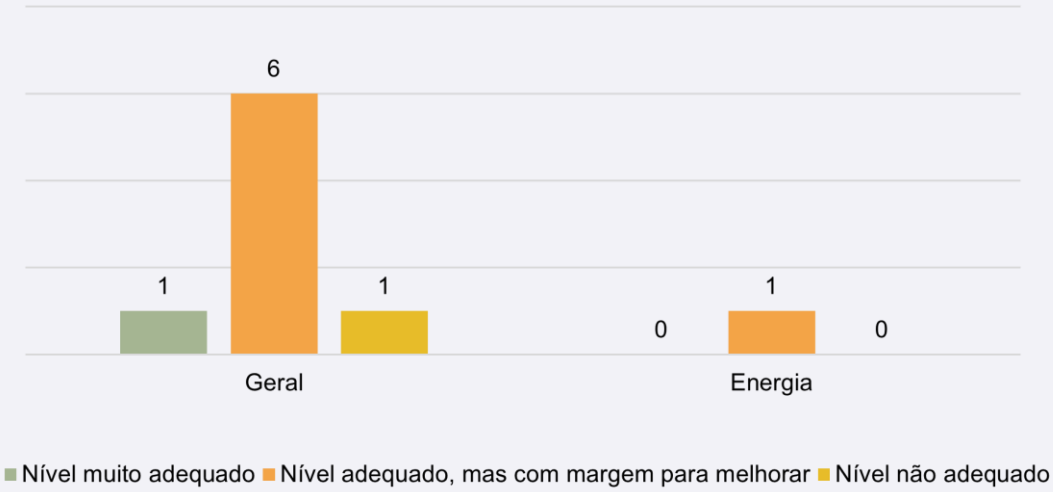
**Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados**




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

## 5. Nível de segurança estabelecido pela legislação em vigor

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




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

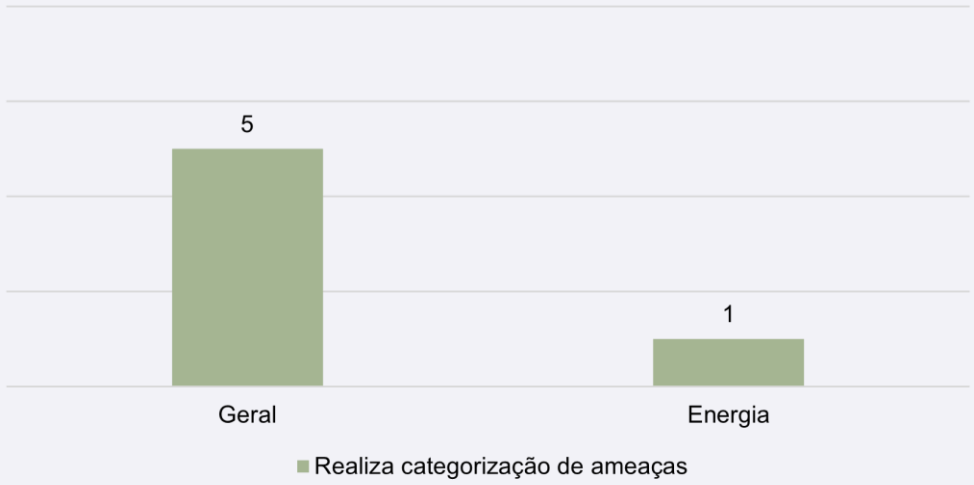
Uma questão semelhante foi colocada, em 2021, não aos reguladores, mas a diversos OSE na União Europeia, no âmbito do relatório *NIS Investments* 2021. As respostas recolhidas indicam que quase 50% (48,9%) dos operadores de serviços essenciais consideram que a Diretiva NIS teve um impacto positivo nas suas organizações e na União, aumentado o nível de cibersegurança das organizações, ao fortalecer as suas capacidades de deteção e de recuperação de incidentes[10].

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.

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

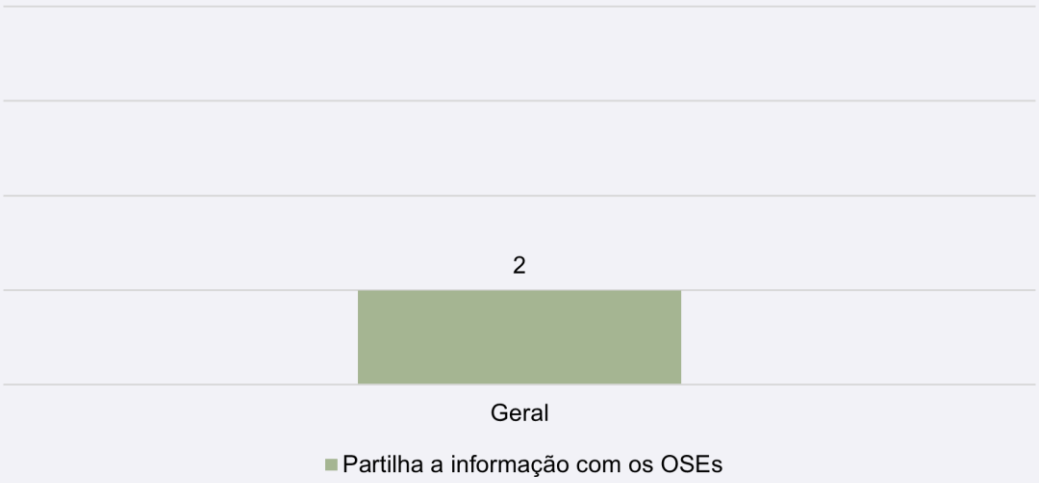
## 6. Categorização de ameaças

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




Cinco dos oito reguladores inquiridos (incluindo o do setor da energia), realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores.

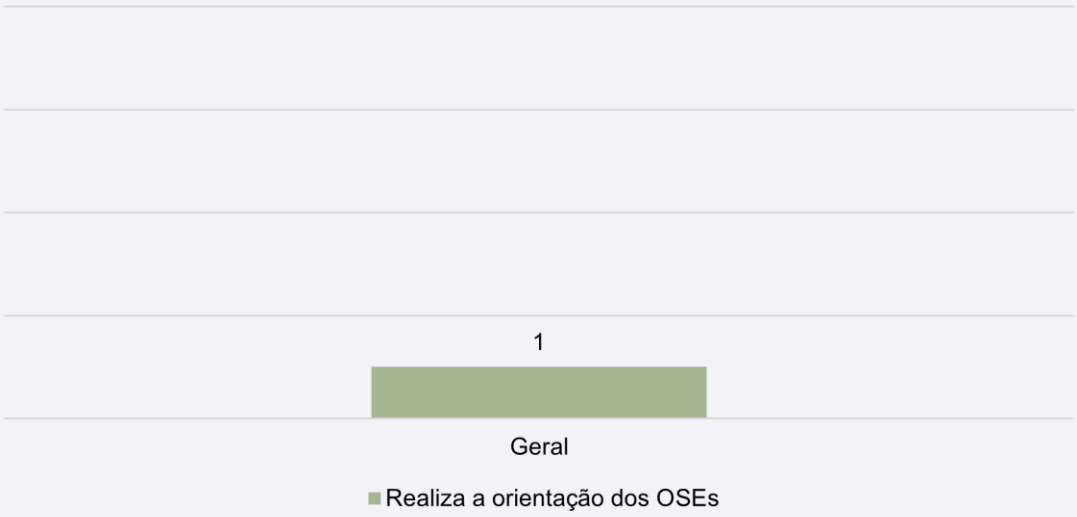
**Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização**




Dos cinco reguladores que realizam categorização de ameaças, apenas dois partilham informação relativa às ameaças com os OSE. Os restantes setores não efetuam a partilha de informação, nomeadamente o setor da energia sendo um deles.

## 7. Orientação dos OSE por parte da entidade reguladora

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



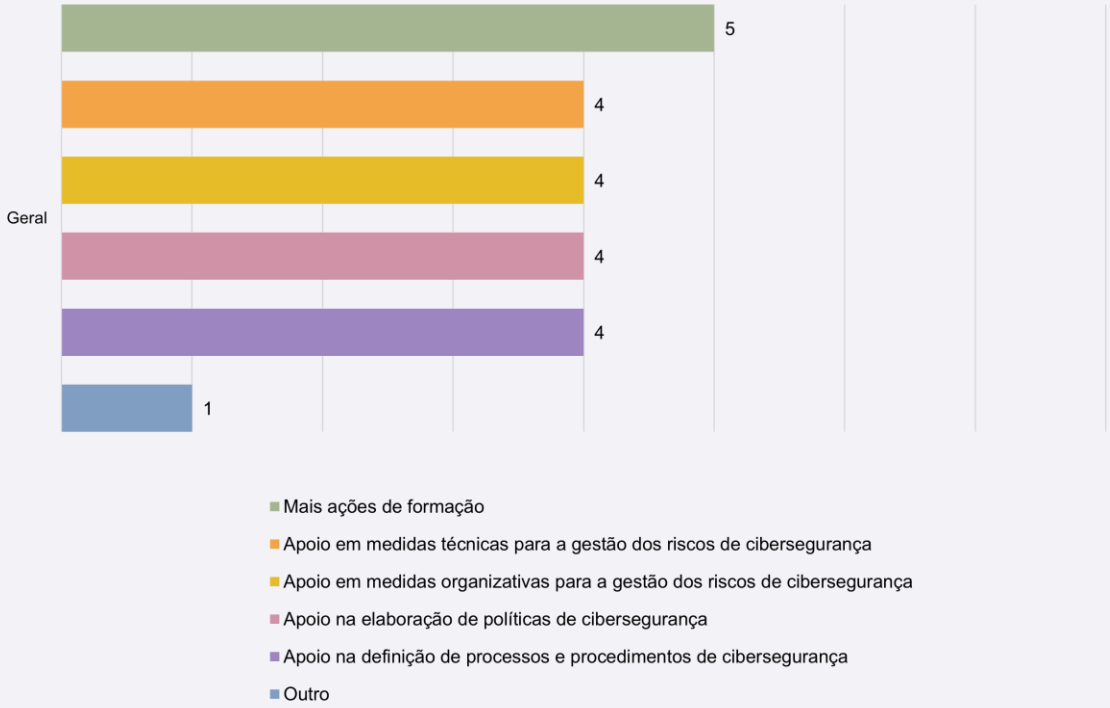

Apenas um dos reguladores (o do setor bancário) indicou fornecer orientação aos OSE na digitalização de processos e na promoção de uma cultura digital, enquanto os restantes sete reguladores indicaram não fazer esse tipo de orientação.

## 8. Apoio por parte do CNCS

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

Entre os reguladores inquiridos, cinco têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional, sendo um deles o regulador do setor da energia.

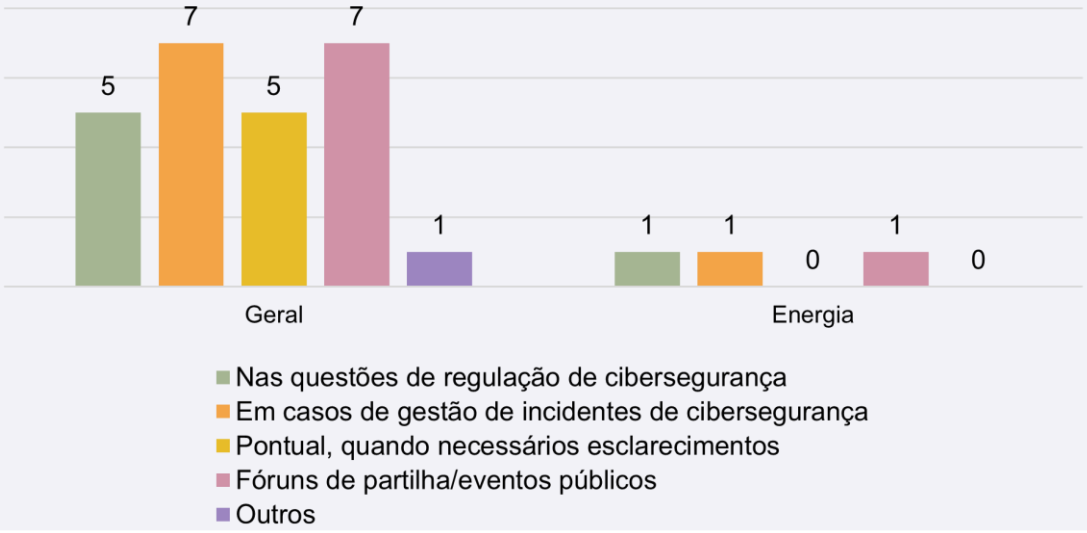
**Gráfico 18 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS**




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, cocriação, nomeadamente gostariam de ver documentos/orientações/guias para o setor feitos em cooperação com as entidades do setor e o próprio CNCS, avaliação de soluções de confiança, recomendações e casos setoriais, referindo-se a haver também recomendações para os OSE com base em casos concretos ocorridos no setor como por exemplo um ataque a uma infraestrutura e como proteger.

Como o regulador do setor da energia entende não haver necessidade de apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, não é considerado nesta questão.

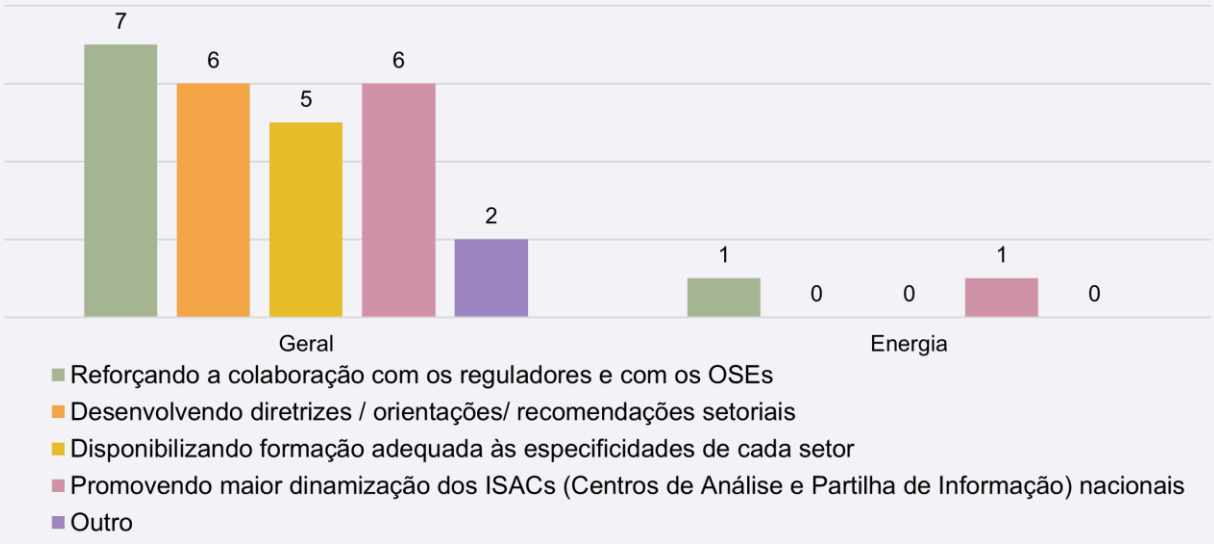
**Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS**




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 energia, indicam 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 fóruns de partilha e eventos públicos, bem como em casos pontuais quando necessário.

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



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

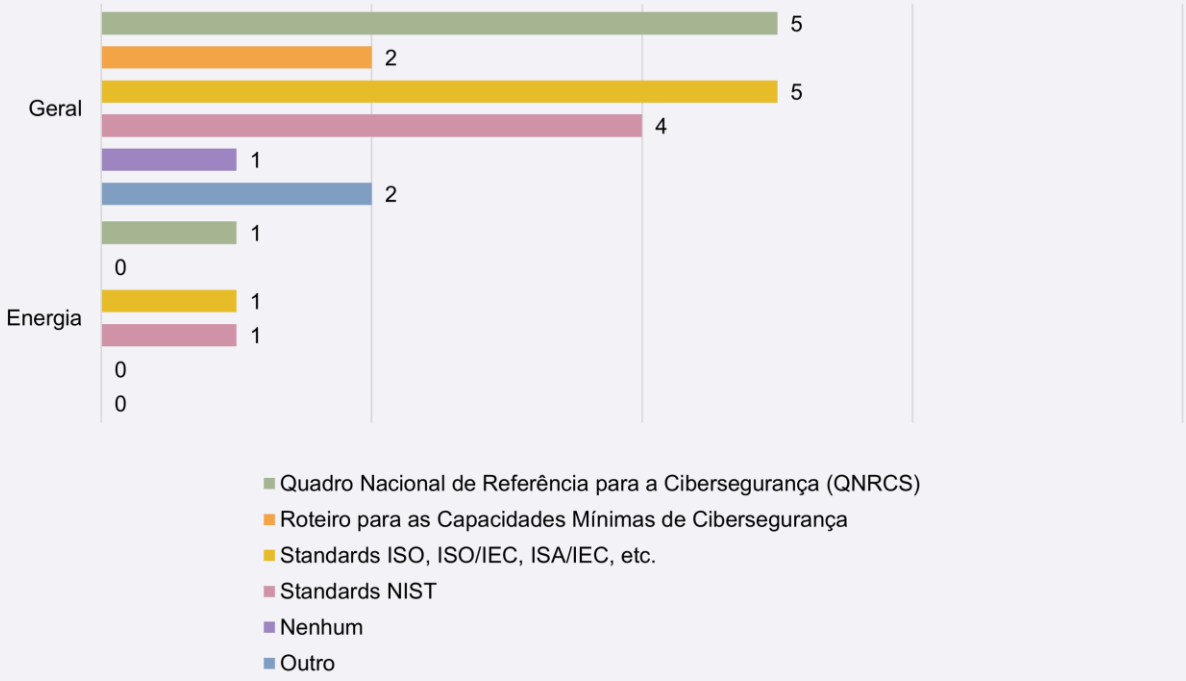
No setor da energia, o regulador inquirido considera que o CNCS poderia promover maior dinamização dos *ISACs* nacionais, também indicaram que poderiam reforçar a sua colaboração com os reguladores e com os OSE.

O Centro Nacional de Cibersegurança lançou um desafio denominado por "Compromisso C-Academy" que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. As organizações poderão escolher, pelo menos, três formações até ao final de 2025. Alguns dos principais benefícios incluem: "Reforço da cibersegurança da organização, setor ou região, aumento da resiliência e da capacidade de resposta a ataques" e "Acesso a conteúdos formativos de elevada qualidade"[11].

[11] CNCS, "Compromisso C-Academy", https://www.cncs.gov.pt/pt/c-academy-compromisso/.

## 9. *Standards* e boas práticas recomendadas

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




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

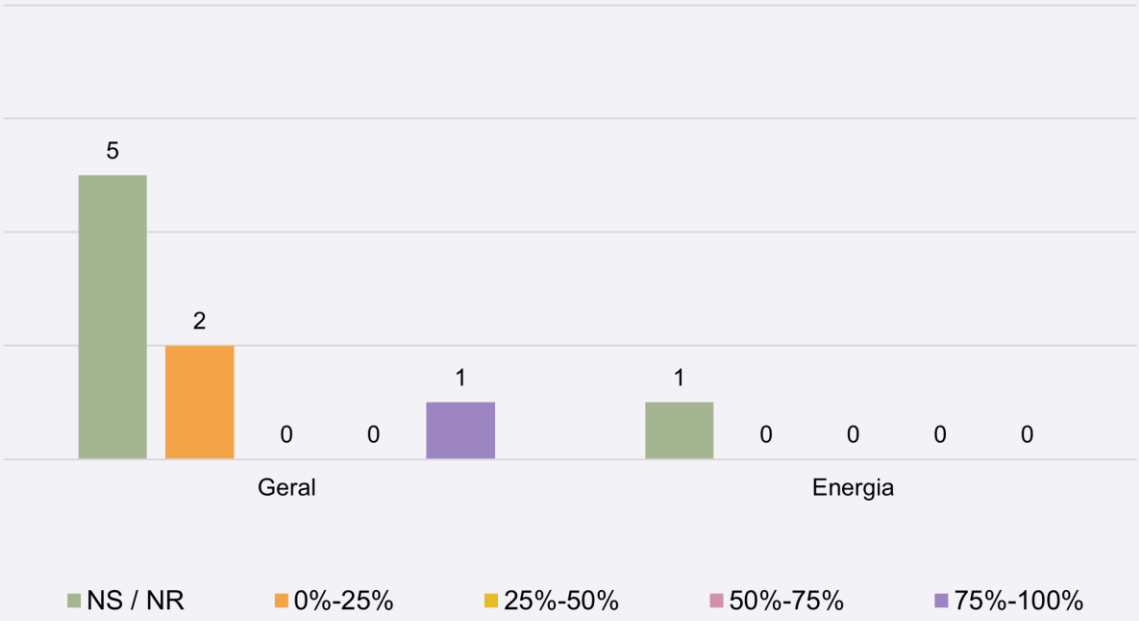
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

No setor da energia, o regulador inquirido recomenda aos operadores a adoção do QNRCS, *standards* ISO e *standards* NIST.

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

[12] 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 da energia indicaram não conhecer a percentagem aproximada de operadores no setor certificados em normas internacionais do tipo referido.

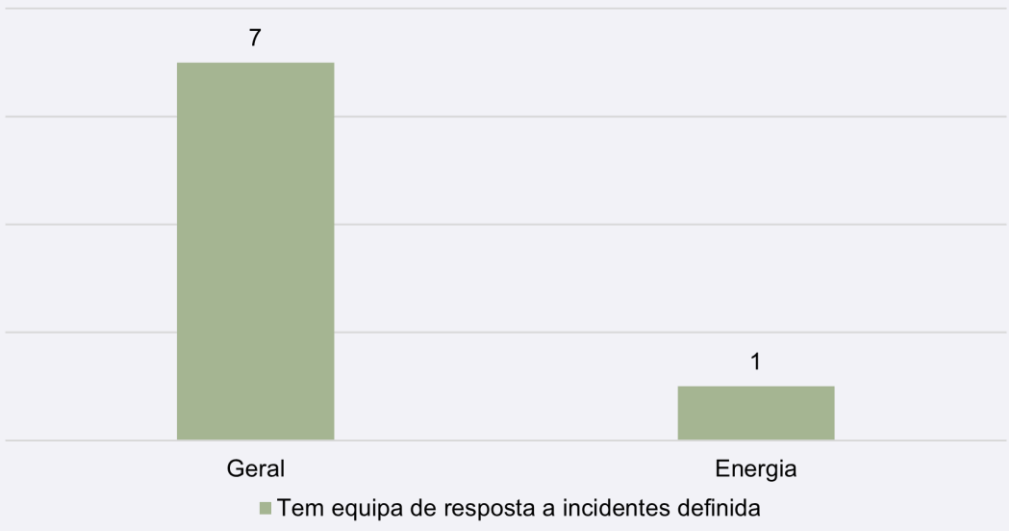
**Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança**

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

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

## 10. Definição de equipa de resposta a incidentes de cibersegurança

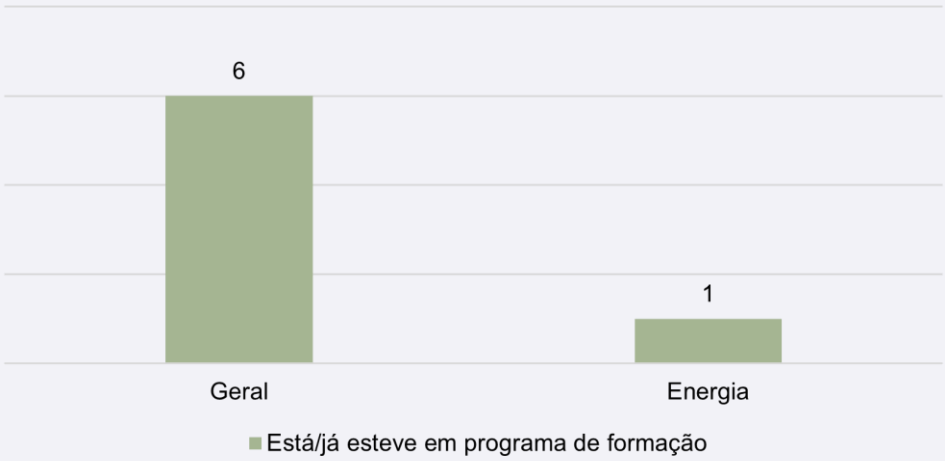
**Gráfico 23 - Reguladores com equipa de resposta a incidentes definida**




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

## 11. Sensibilização e consciencialização

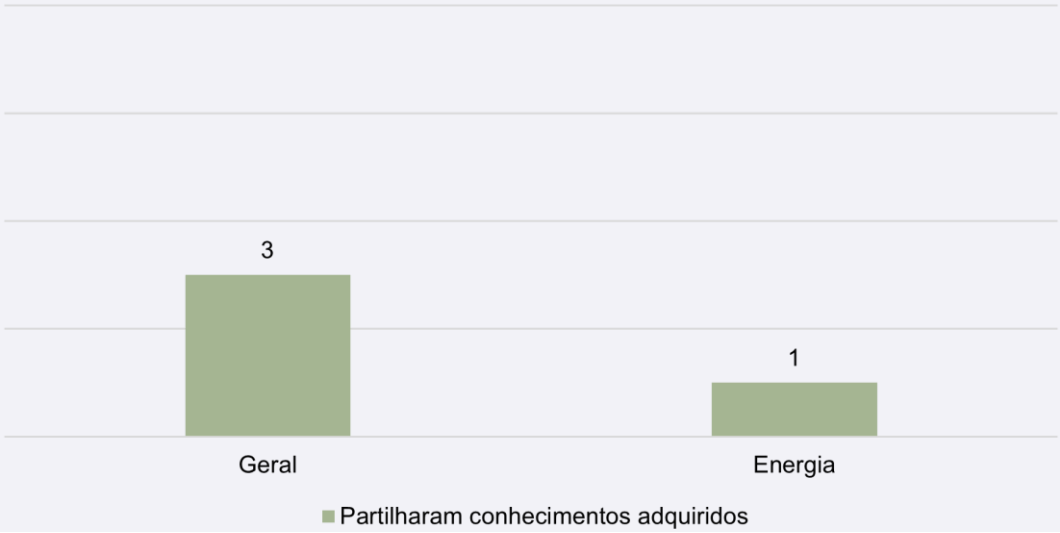
**Gráfico 24 - Reguladores que estão ou já estiveram em programas de formação e sensibilização para os riscos no ciberespaço promovidos pelo CNCS ou por outra entidade**




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

O regulador inquirido do setor da energia, informou estar ou já ter estado em programas de formação e sensibilização para os riscos no ciberespaço.

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

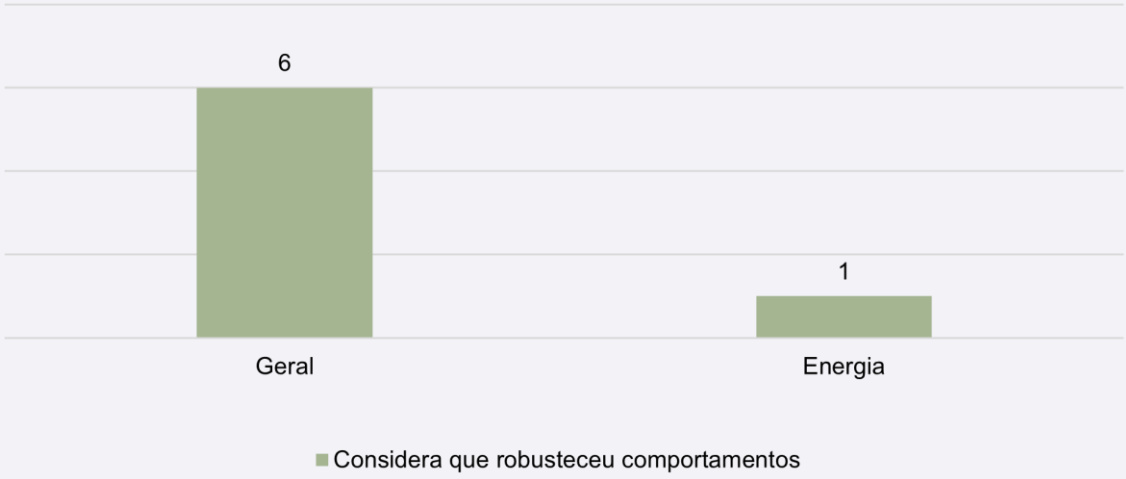



No seguimento da participação nos programas de formação e sensibilização para os riscos no ciberespaço, questionou-se se os conhecimentos adquiridos nesses programas foram partilhados com os OSE do setor. Os setores que fizeram essa partilha e os que não fizeram dividem-se igualmente.

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

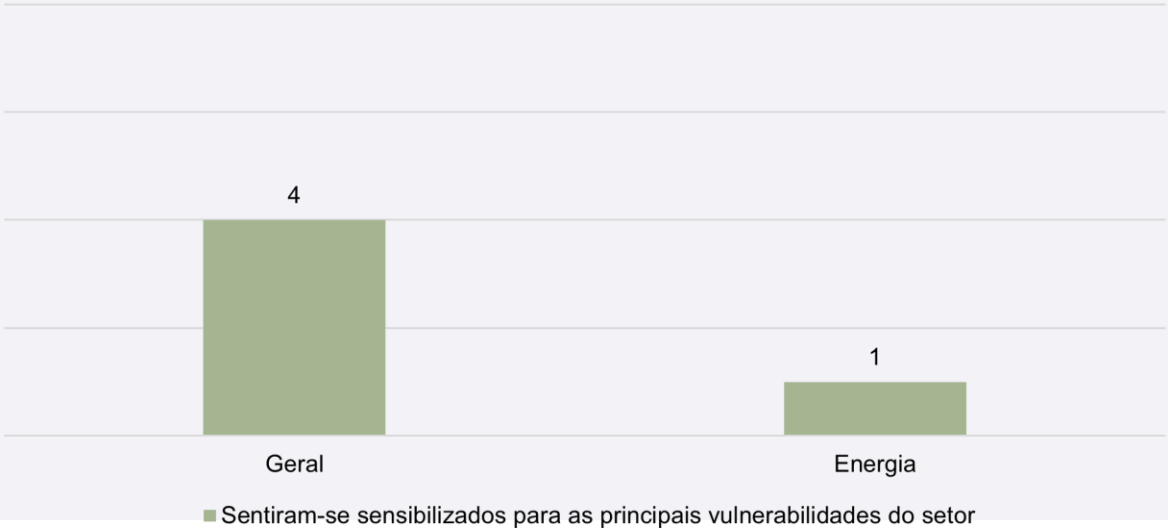
O regulador do setor energia refere ter partilhado os conhecimentos adquiridos com os operadores do seu setor.

**Gráfico 26 - Reguladores recipientes de formação que partilharam os conhecimentos adquiridos com os OSE do setor**




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

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




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

No setor da energia, o regulador inquirido considerou que a entidade formadora o sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto.

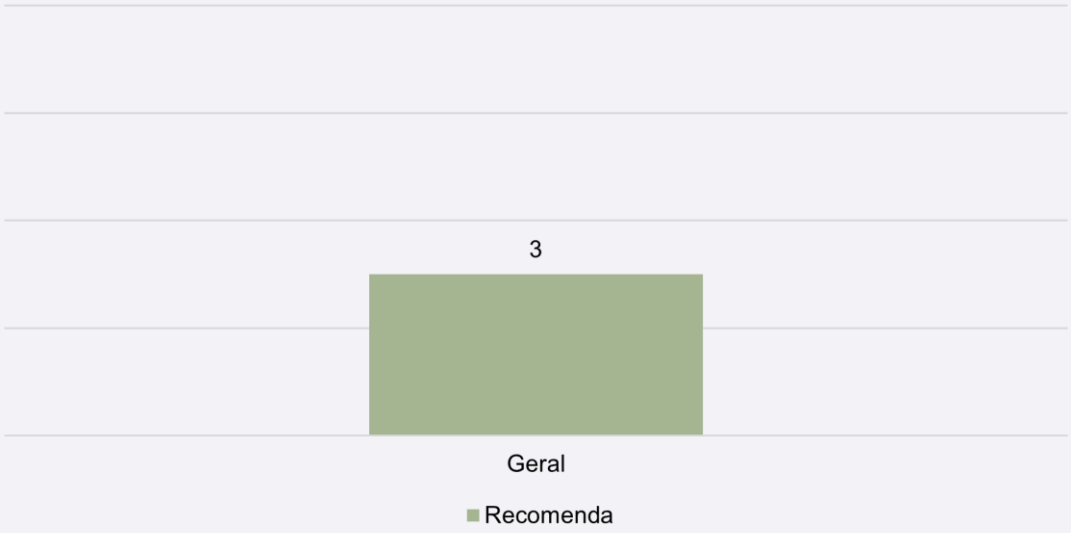
## 12. Cooperação nacional/internacional de proteção do ciberespaço

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


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

O regulador do setor da energia, 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 da energia, 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**

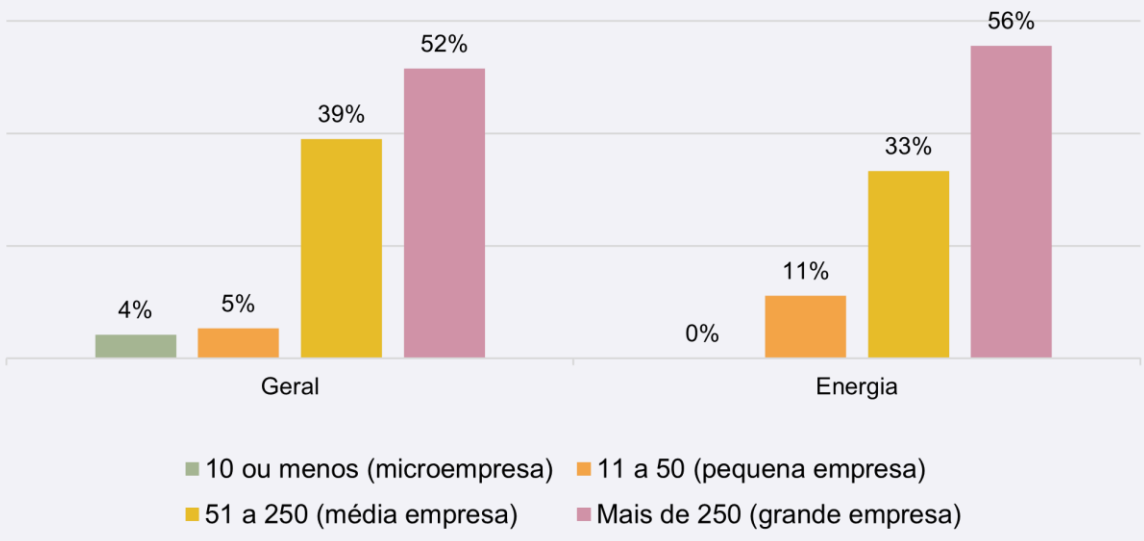
| Setores | Estimativa |
|---|---|
| Energia | 32 |
| Transportes | > 19 000 |
| Bancário | 120 |
| Infraestruturas do Mercado Financeiro | > 1 000 |
| Distribuição de Água Potável | 350 |
| Infraestruturas Digitais | 100 |

**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**

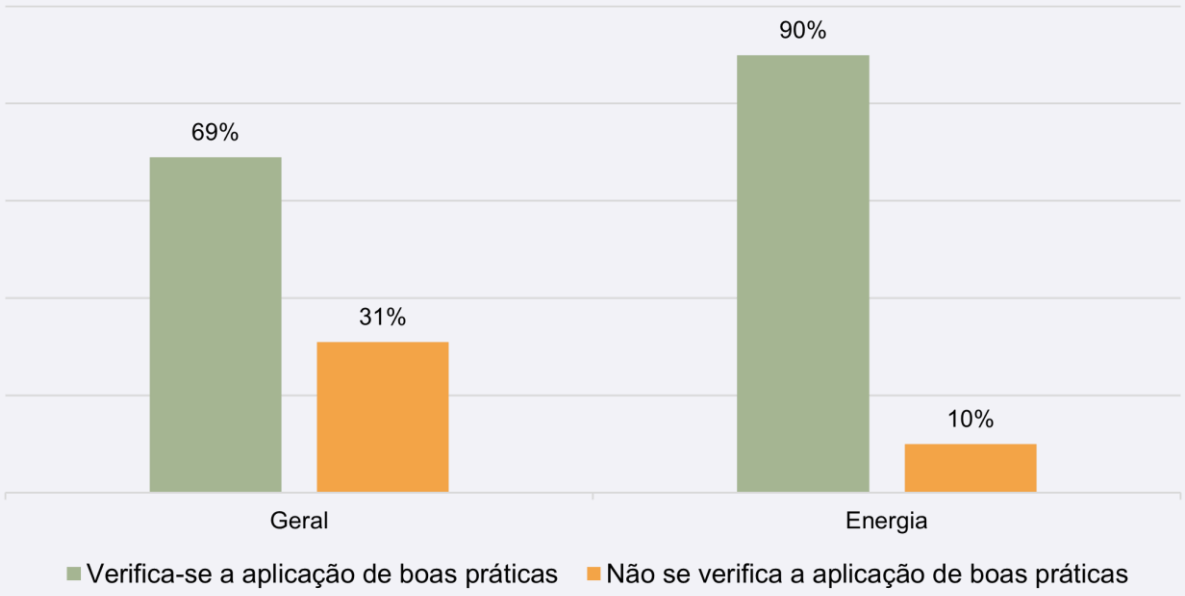



O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas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

Destaca-se os setores da energia, em que as grandes empresas são mais comuns (56%), seguidas pelas médias empresas (33%) e pequenas empresas (11%), não registando nenhuma microempresa.

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[13].

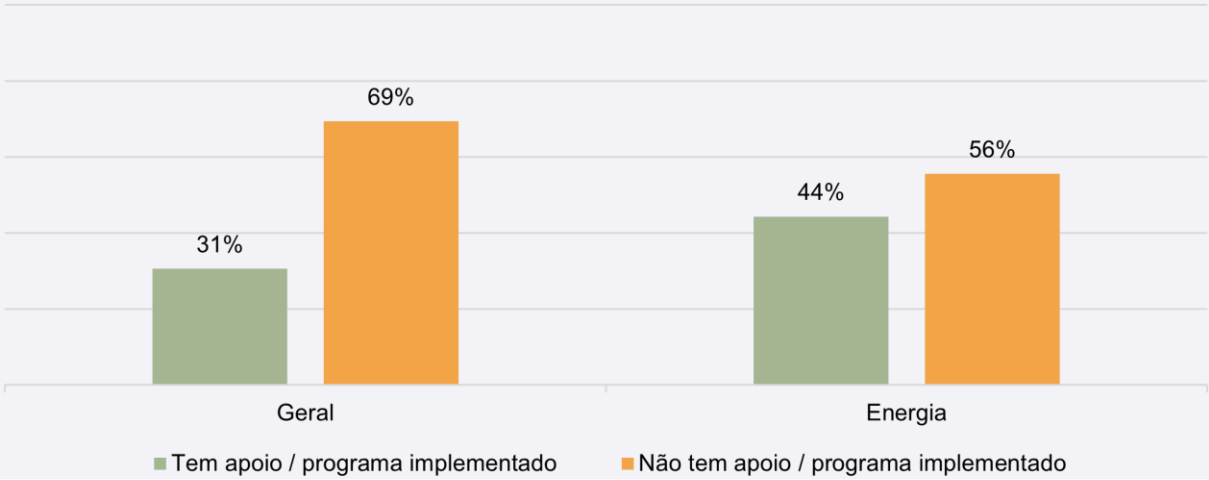
**Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores**




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 energia, destaca-se por ser um setor no qual 90% dos operadores considerarem que boas práticas de cibersegurança são aplicadas pelos seus colaboradores.

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

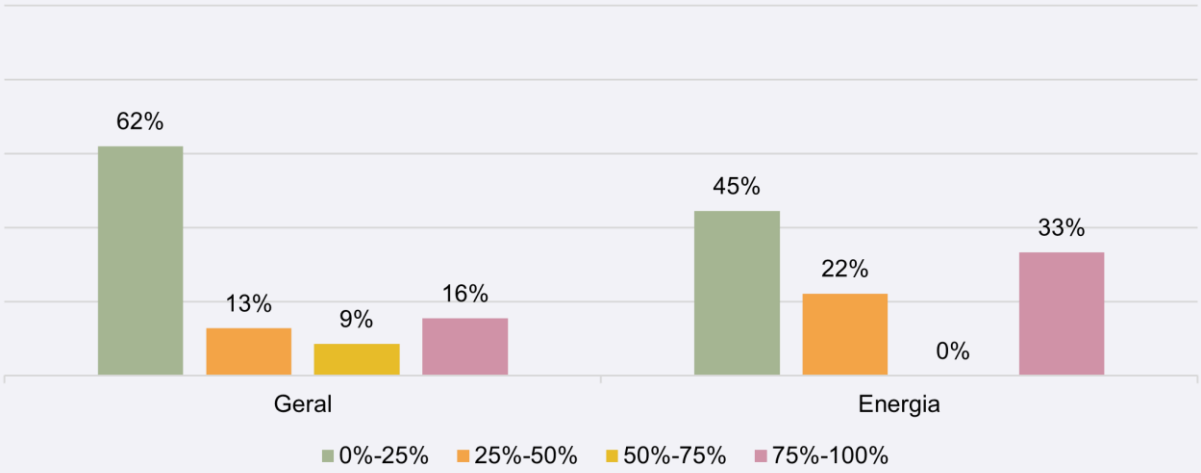
**Gráfico 32 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança**




À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança. No setor da energia 56% dos operadores não têm apoios ou programas próprios ou do Estado para colaboradores que desejem formação em cibersegurança.

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

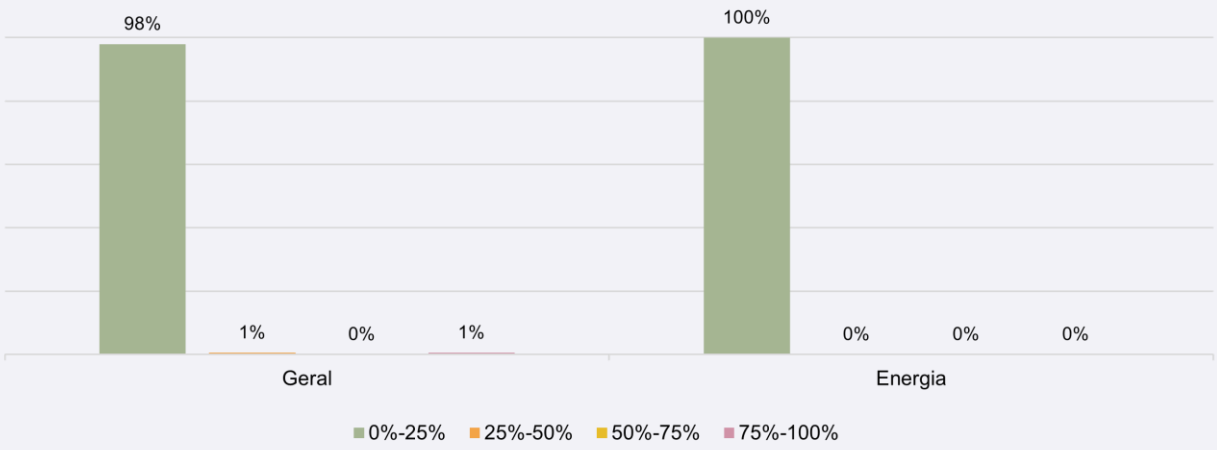
**Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança**




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

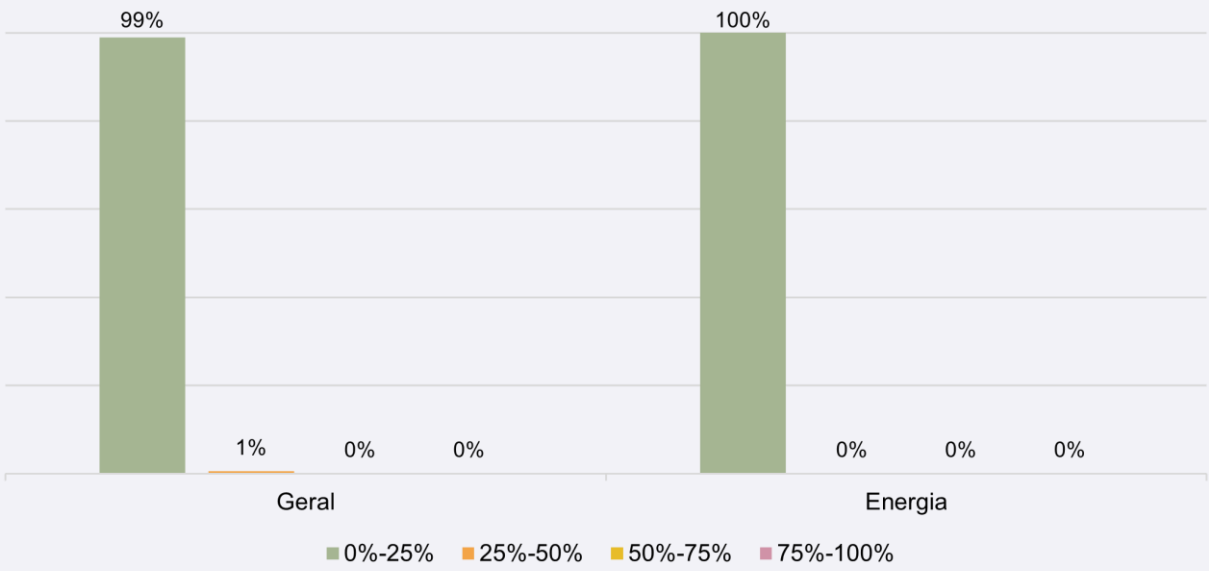
No setor da energia, embora predominem os operadores onde a quantidade de colaboradores com este tipo de formação não ultrapassa os 25%, há mais dos 30% de operadores com percentagens de colaboradores com formação básica em cibersegurança no intervalo 75%-100%.

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




Face aos resultados obtidos na questão anterior, é de esperar que a percentagem de colaboradores com formação superior em cibersegurança seja diminuta. É também de esperar que o seja, dado que cada OSE congrega várias áreas profissionais, como os recursos humanos, as finanças e a cibersegurança, não sendo composta apenas por profissionais da área em análise neste relatório. Em termos gerais, a percentagem de trabalhadores dos operadores com formação superior em cibersegurança situa-se predominantemente na faixa entre 0%-25% em todos os operadores de todos os setores. Existe um número reduzido de colaboradores dos operadores inquiridos, com formação superior em cibersegurança.

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

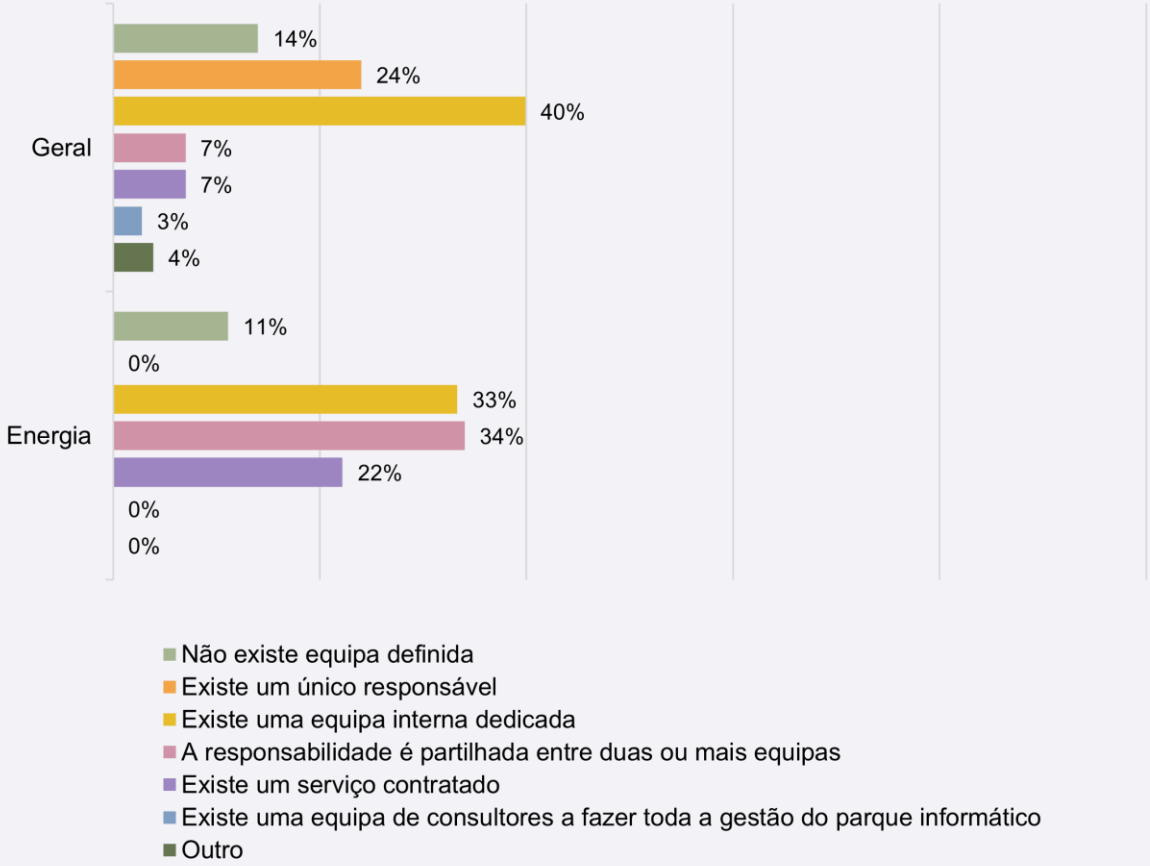



A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Novamente, o resultado geral é um resultado expectável, uma vez que não se espera que colaboradores de outras áreas sejam certificados em cibersegurança.

De acordo com os dados disponíveis no relatório *NIS Investments* 2021, da ENISA, apenas 7,5% dos OSE na UE indicavam ter uma preocupação em certificar os colaboradores da própria organização. A nível setorial, no mesmo relatório, em nenhum dos setores se superava os 11% de OSE a certificar os seus próprios colaboradores[14].

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

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

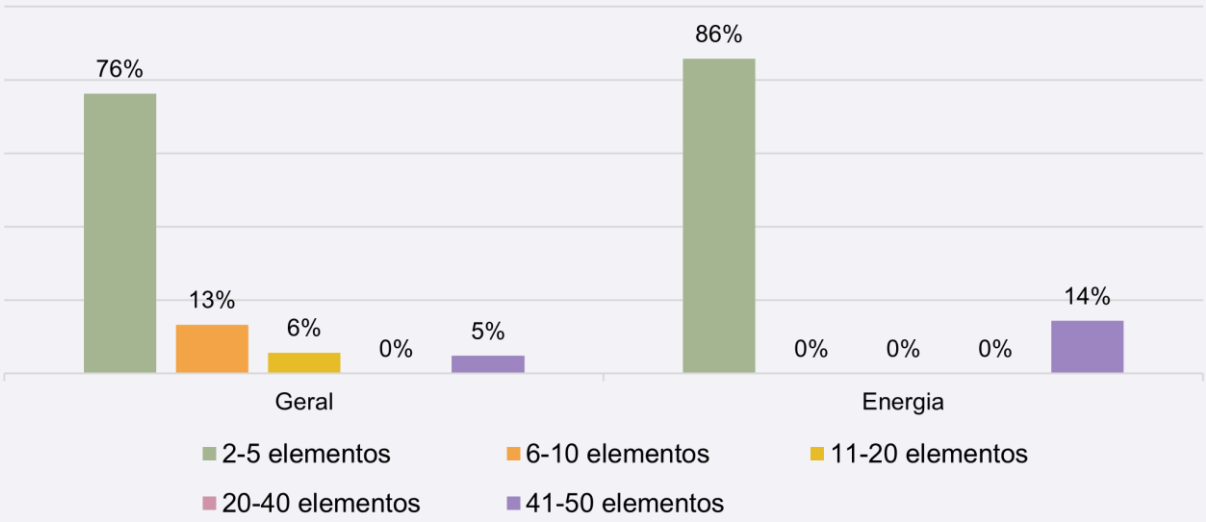



De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

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 Operations Center* (SOC) ou haver uma equipa de uma entidade tutelar a prestar o serviço de *helpdesk*, como no caso dos serviços municipalizados na distribuição de água potável, em que a equipa responsável pertence, por exemplo, à comunidade intermunicipal.

Os operadores do setor energético contam, maioritariamente, com uma ou mais equipas dedicadas (34%) ou com uma única equipa dedicada (33%), verificando-se também o recurso à contratação externa do serviço de *helpdesk* em 22% dos casos.

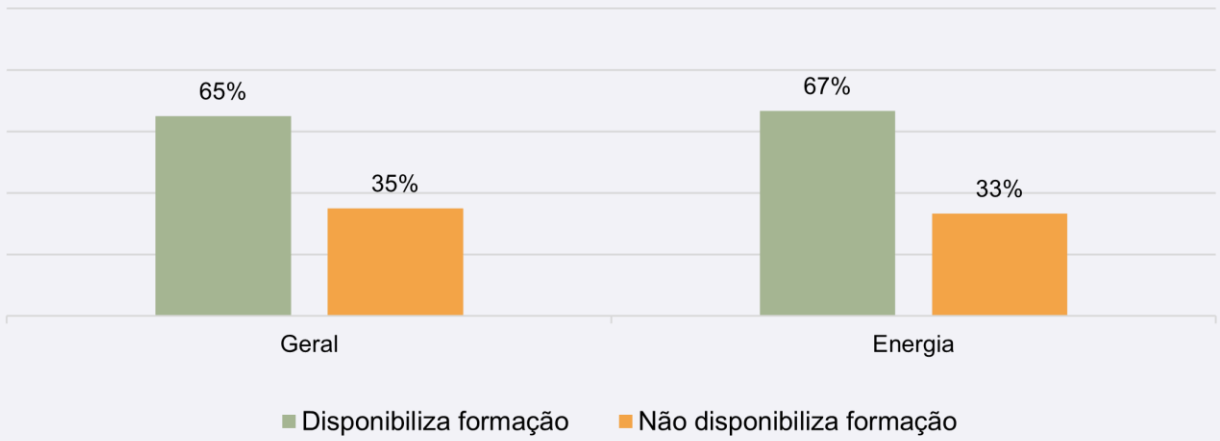
**Gráfico 37 - Composição das equipas de *helpdesk***




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.

No setor da energia 86% das equipas são compostas por 2-5 elementos e apenas 14% por equipas de 41-50 elementos.

**Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores**

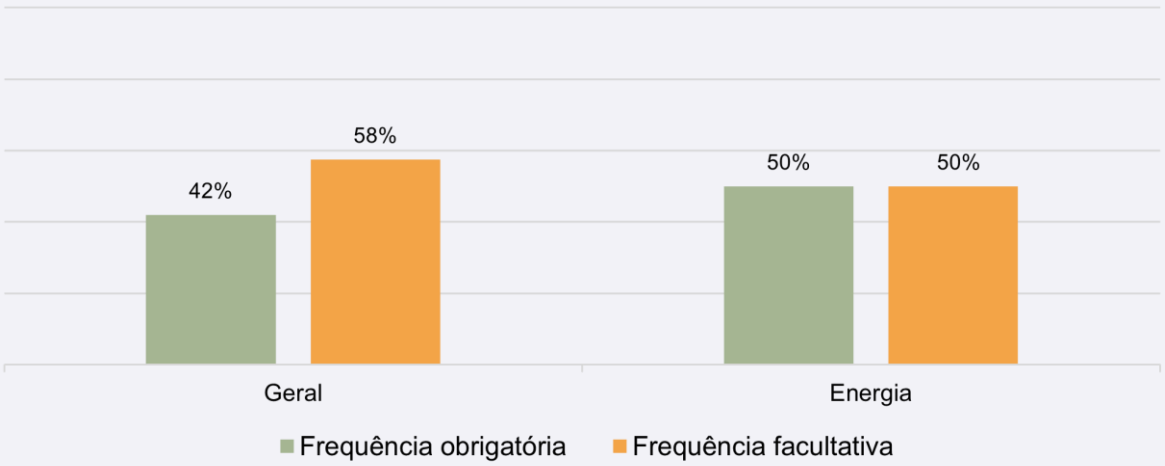



Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. Os operadores do setor da energia mantem a tendência geral.

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[15]. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado "Estado da Cibersegurança em Portugal", indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

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

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

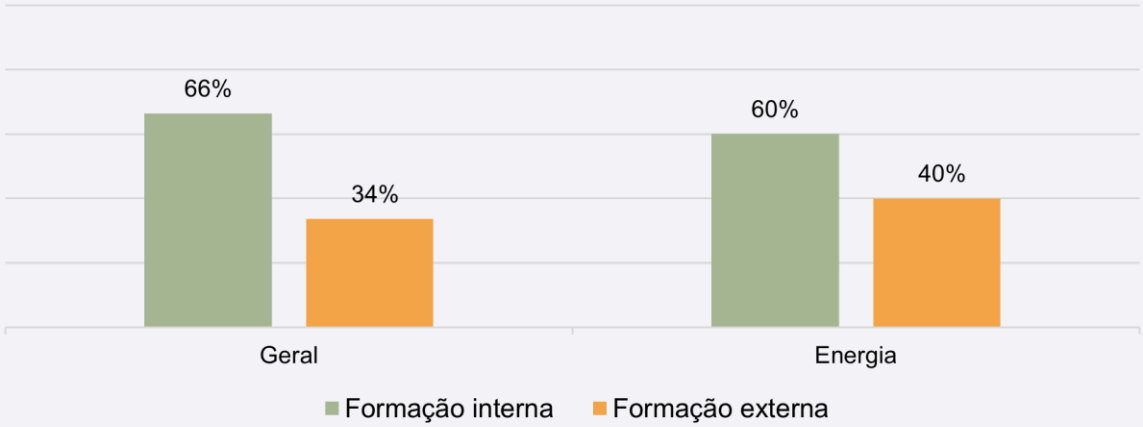



De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. Por exemplo, no setor da energia, há tantos OSE onde a formação é obrigatória como onde é facultativa.

Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre 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[16].

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

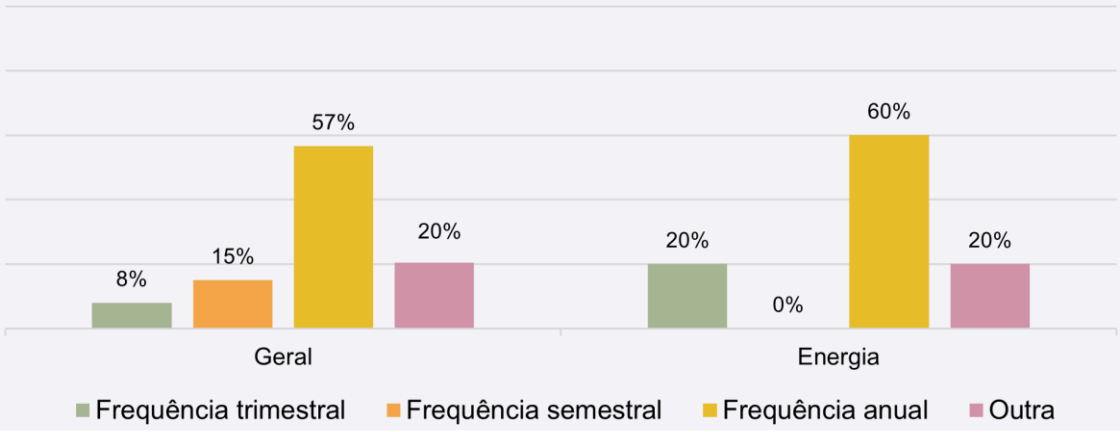
**Gráfico 40 - Caráter das formações disponibilizadas - formação interna ou externa**




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.

Contudo, cerca de um terço dos OSE (34%) recorre a entidades externas para formar os seus colaboradores. Um dos setores onde mais se recorre a entidades externas para ministrar formação é o da energia, com 40% de OSE a optarem por esse método, embora se continue a registar uma maioria de operadores que recorrem aos meios internos para dar formação.

**Gráfico 41 - Frequência média dos momentos de formação**

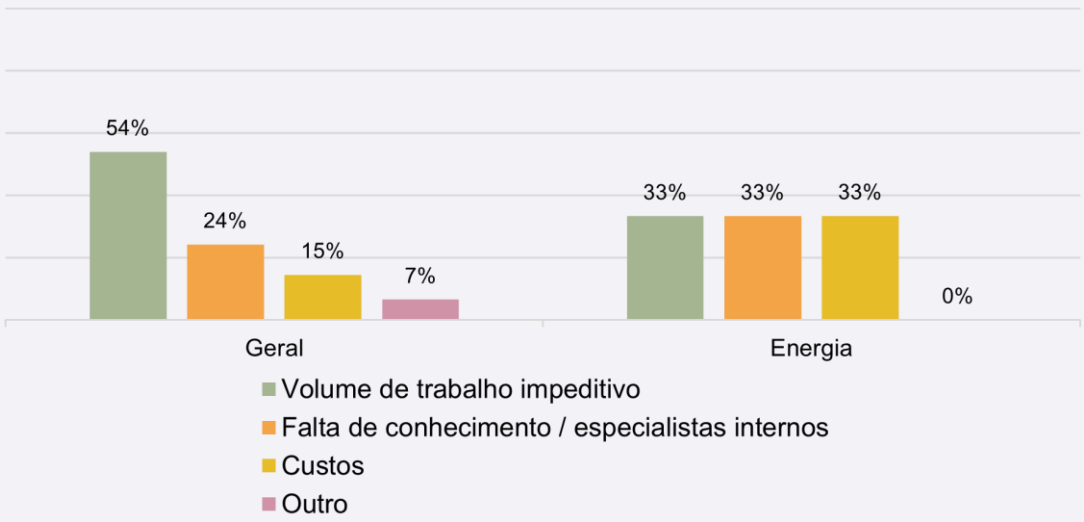



Em termos gerais, a maioria dos OSE que disponibiliza formação (57%) indica que a frequência média dos momentos de formação é anual.

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

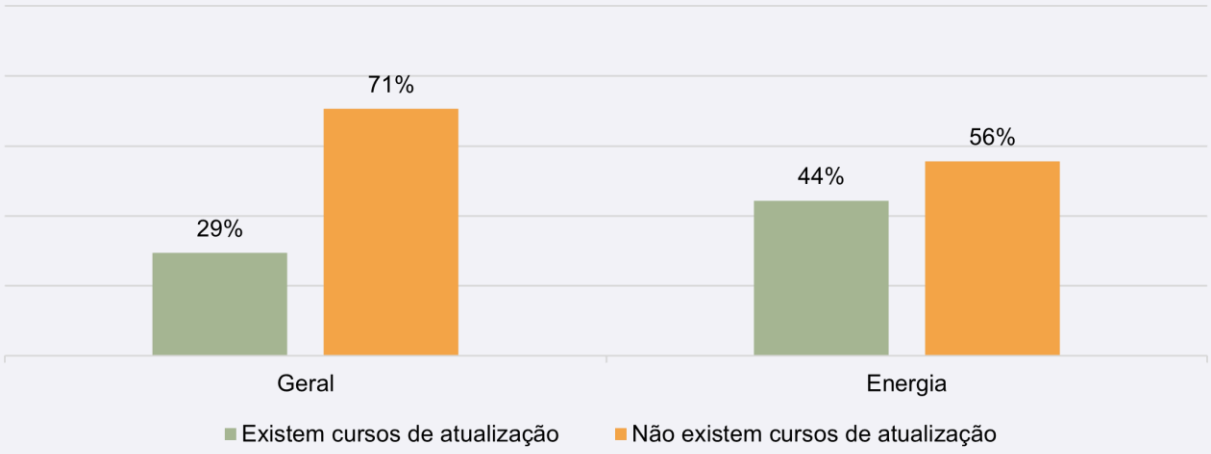
formação sucedem de modo *ad hoc*. No setor da energia predominam as formações com frequência anual, não foram registadas formações com frequência semestral.

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



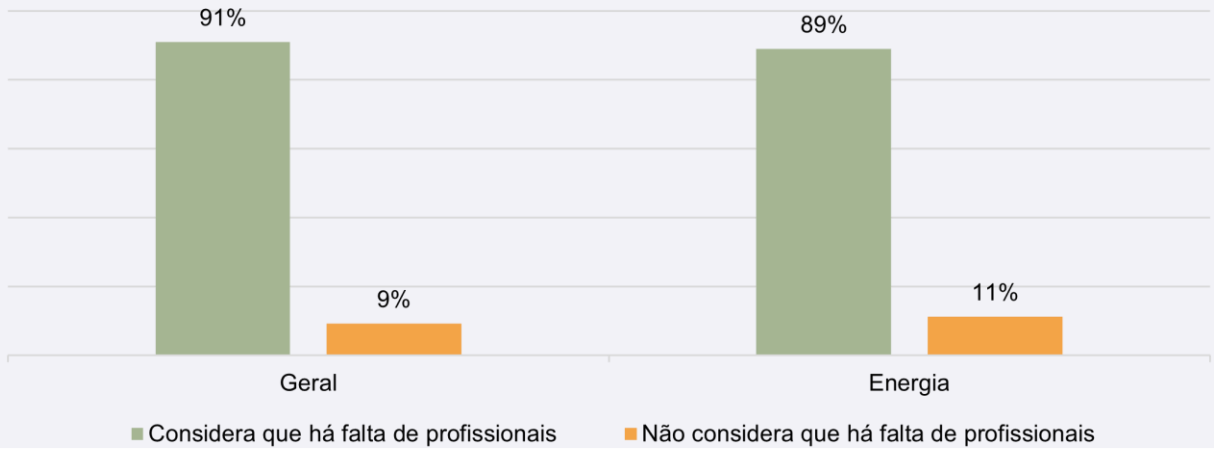

Os motivos para a não disponibilização de formação são na sua maioria atribuídos ao volume de trabalho impeditivo, tendo este motivo sido indicado por 54% dos OSE que afirmaram não disponibilizar formação em cibersegurança aos seus colaboradores. No setor da energia, os motivos para a não disponibilização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

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



A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos. No setor da energia, 44% dos OSE disponibiliza cursos de atualização.

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




A vasta maioria dos OSE inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. No setor da energia, 89% dos OSE considerou haver falta de profissionais de cibersegurança.

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[17] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[18]. 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[19]. De modo a combater esta escassez, organizações como o Fórum Económico Mundial e a ENISA têm feito diversas recomendações, que passam pela contratação de profissionais vindos de outras áreas de formação que não apenas as das TIC, engenharia e matemática, pela admissão de colaboradores menos experientes, ou mesmo sem experiência (sendo esta adquirida ao longo do desempenho das funções pretendidas), a admissão de colaboradores em trabalho totalmente remoto, e pela valorização dos profissionais, não só a nível salarial, mas também a nível das perspetivas de progressão de carreira e até mesmo do respeito pelos profissionais no local de trabalho[20] [21].

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

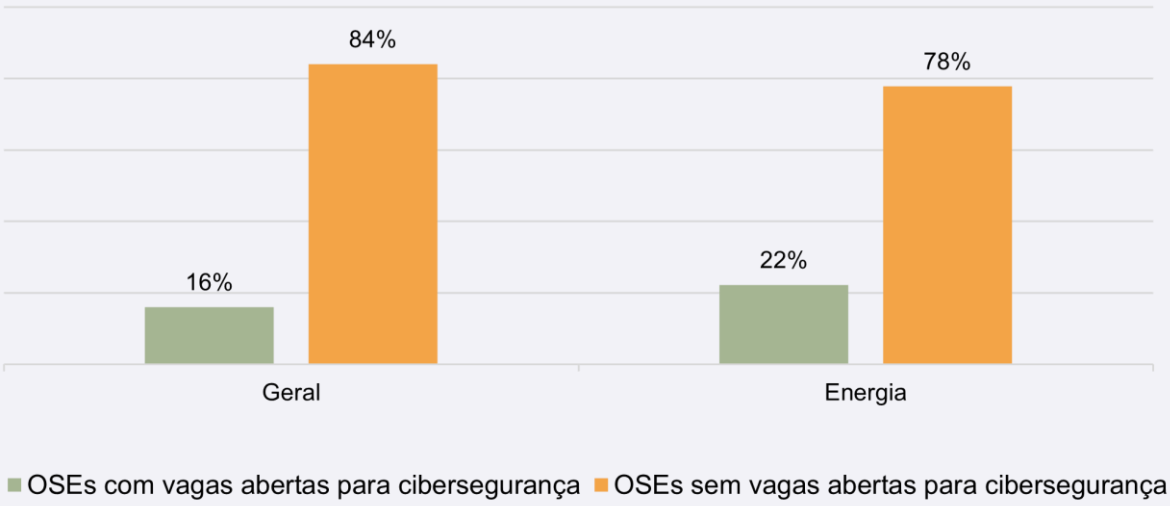
[18] ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU", https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

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

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

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

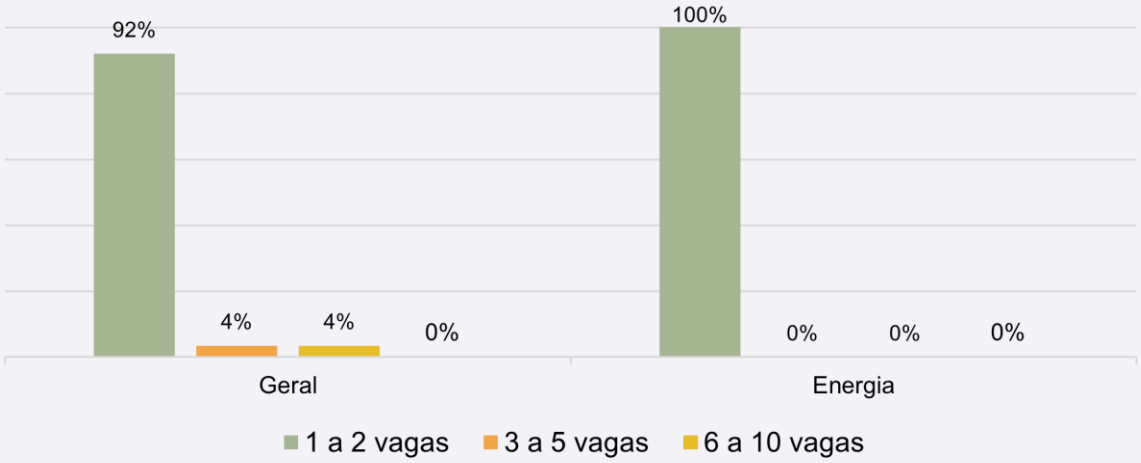
**Gráfico 45 - Vagas abertas para a área de cibersegurança**




À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, na energia, 22% dos operadores apresenta vagas abertas para a cibersegurança, sendo assim superior à generalidade.

Embora não se possa fazer uma associação direta entre vagas para cibersegurança e para pessoal especialista em TIC, os dados do IUTICE de 2022 mostram que, nesse ano, apenas 6,2% das empresas portuguesas tentaram recrutar pessoal especialista em TIC[22].

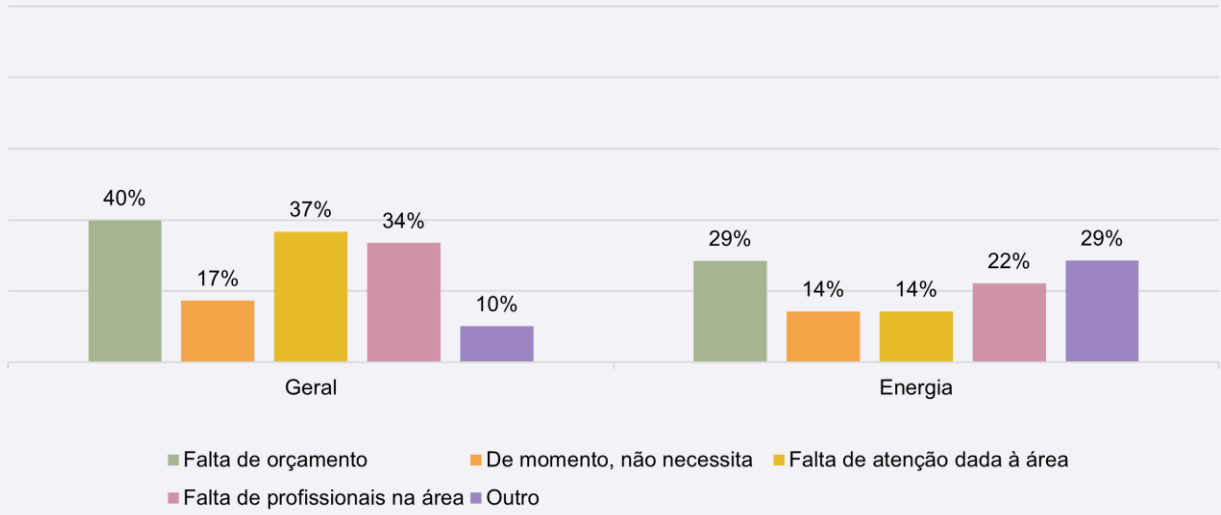
**Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança**




Entre os 16% de OSE que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Tal era o caso para todos os OSE com vagas em aberto nos setores da energia.

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

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




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

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

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[23].

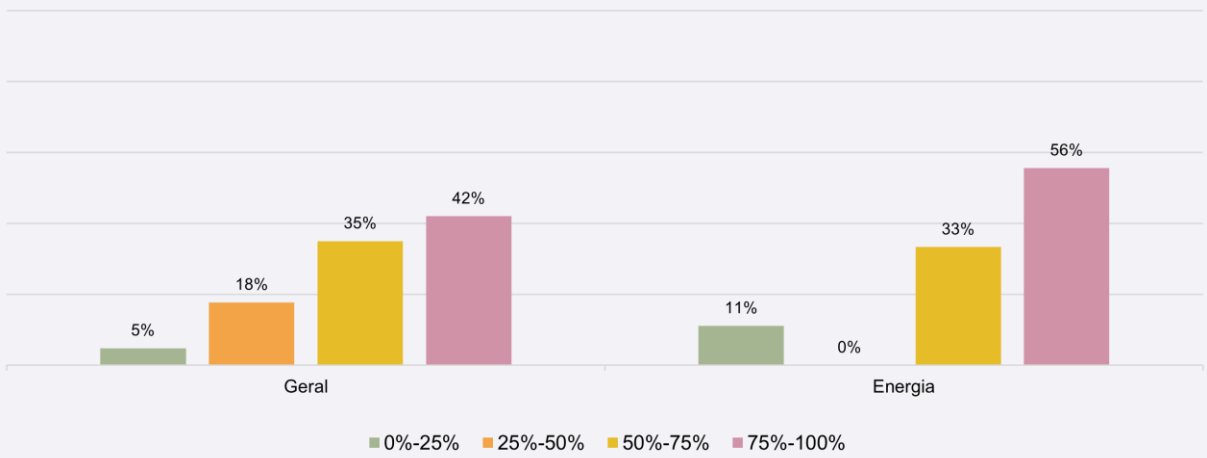
Voltando aos dados obtidos através do questionário realizado, a "falta de atenção dada à área" indicada por 37% dos OSE sem vagas em aberto é um dos aspetos mais preocupantes que surgem na análise. Um dos Objetivos Estratégicos (Objetivo 3) da Estratégia Nacional de Segurança do Ciberespaço 2019-2023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

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

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

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[25].

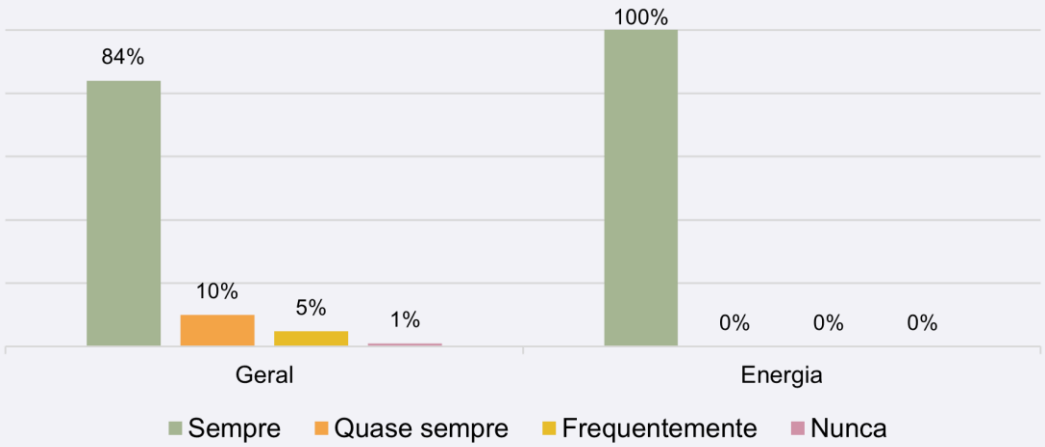
**Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho**




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 há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.
No setor da energia é acompanhada a tendência geral de ter entre 75% a 100% dos colaboradores com acesso a equipamentos digitais.
Segundo dados do IUTICE de 2022, em 2021, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais (+17,2 p.p. face a 2021), abrangendo 28,1% do pessoal ao serviço (+4,2 p.p. que em 2021). Neste ano, 74,7% das empresas tinham pessoal ao serviço com acesso remoto ao sistema de correio eletrónico da empresa[26].

[25] International Organization for Standardization, “International Standard ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements”, 2.
[26] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2022, 4-5.

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



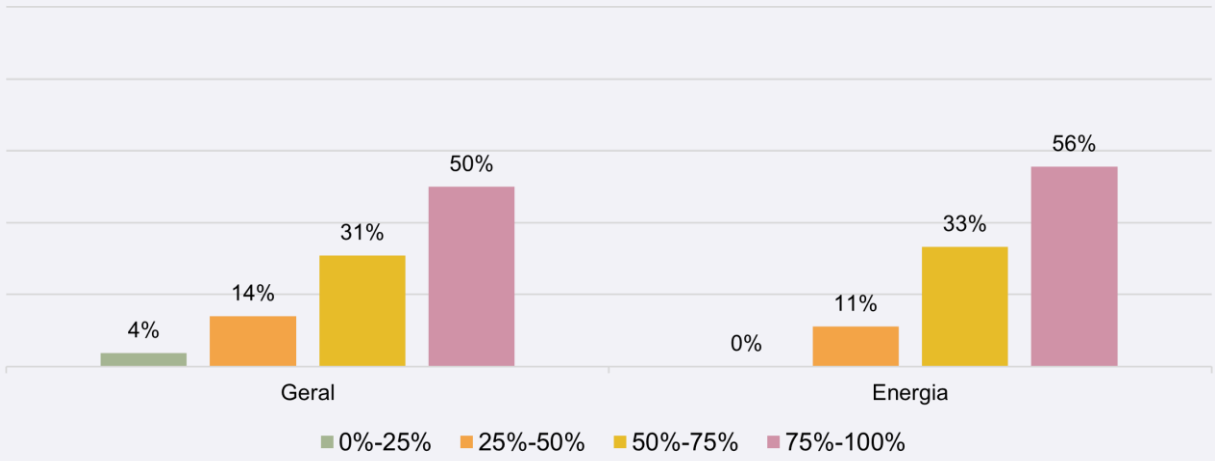

Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos nos setores da energia indicaram ser os próprios a fornecer sempre os equipamentos necessários aos colaboradores.

Contrastando, registam-se alguns OSE onde nem sempre o fornecimento dos equipamentos necessários é feito pelo OSE em questão.

Mais uma vez, 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[27].

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

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

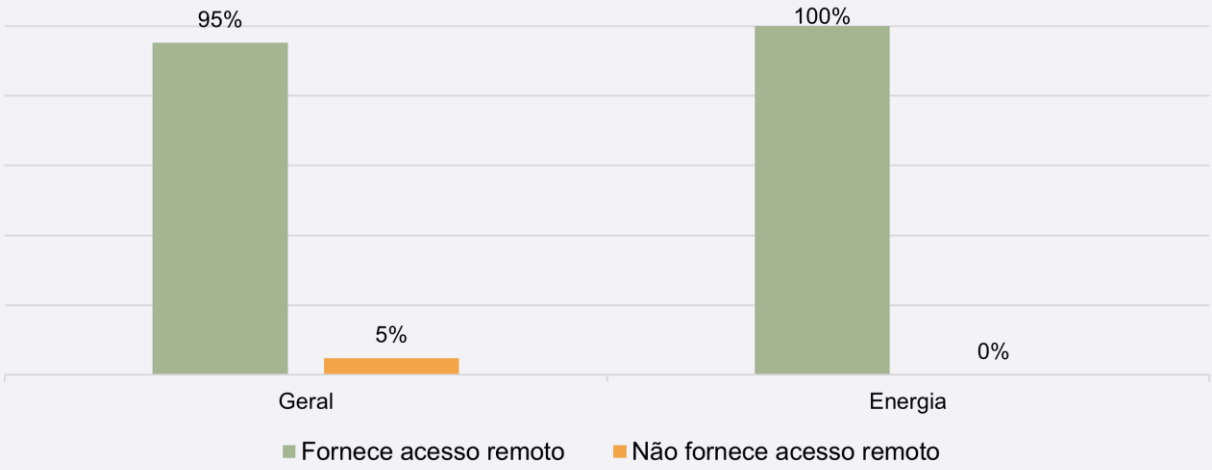



A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.
No setor da energia, a faixa predominante continua a ser aquela em que 75%-100% dos colaboradores tem acesso à Internet no desempenho das suas funções, embora se registem operadores nos quais a percentagem de trabalhadores com acesso à Internet é menor.
Não foram registados operadores no setor da energia na faixa dos 0%-25%.

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[28].

[28] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2023, 3.

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

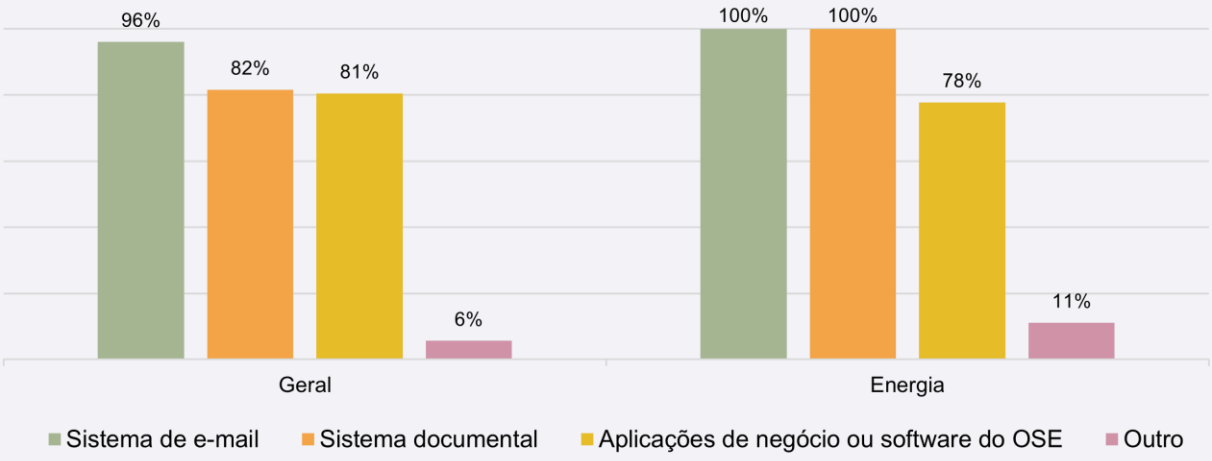



O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). No setor da energia, todos os OSE indicaram permitir o acesso remoto a esses sistemas por parte dos seus colaboradores.

Voltando a comparar com os dados do IUTICE de 2022, há uma maior percentagem de Operadores de Serviços Essenciais a fornecer acesso remoto ao sistema de e-mail do que na generalidade das empresas em Portugal. Enquanto 95% dos OSE indicaram dar esse acesso remoto, no contexto empresarial geral apenas 74,7% das empresas fornecem acesso remoto ao sistema de e-mail[29].

[29] 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**



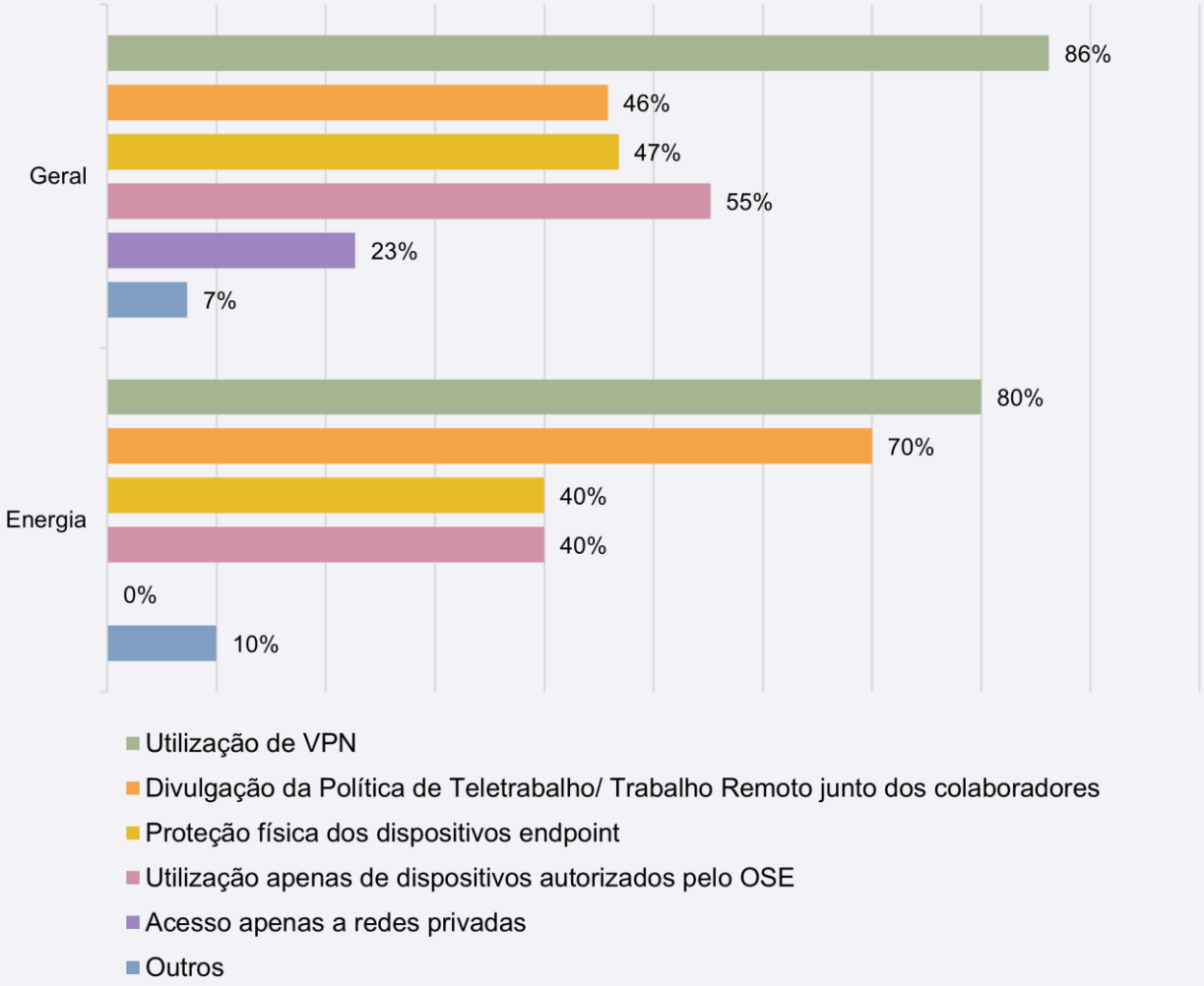

Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

No setor da energia, os sistemas de e-mail e documentais podem ser acedidos remotamente por todos os colaboradores, as aplicações de negócio por 78% e outro tipo de sistemas por 11%.

Comparando novamente com dados do IUTICE de 2022, os OSE continuam a fornecer mais acesso remoto a diferentes sistemas do que a generalidade das empresas portuguesas. Tinha já sido vista a diferença na disponibilização geral de acesso remoto por parte dos colaboradores a sistemas entre OSE (95% a disponibilizar) e empresas (74,7% a disponibilizar). Revisitando essa comparação entre cada sistema, é visível que há mais OSE a dar acesso remoto aos documentos da organização do que empresas em geral (82% de OSE contra 65% de empresas) e também mais OSE a dar acesso remoto a aplicações ou *software* de negócio (81%) do que empresas (63,9%)[30].

[30] 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**

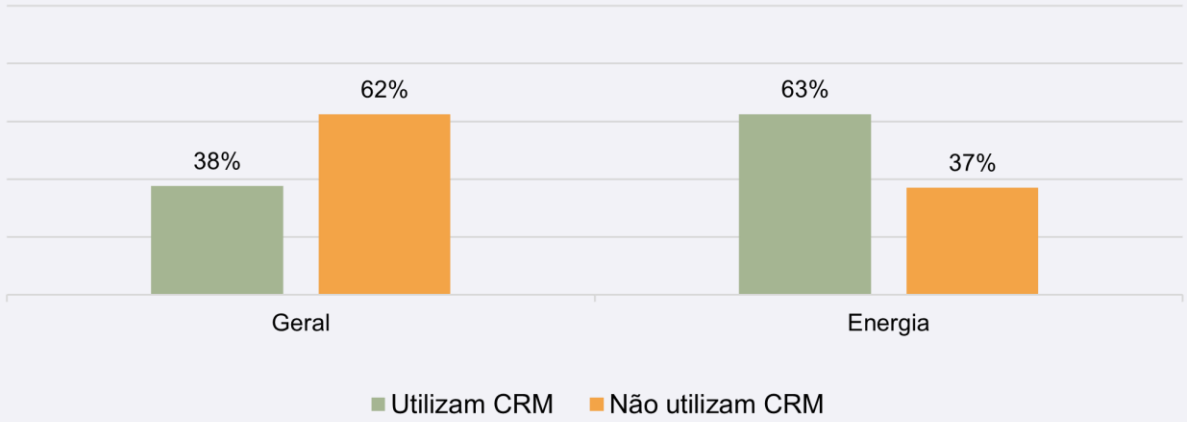



No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança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

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

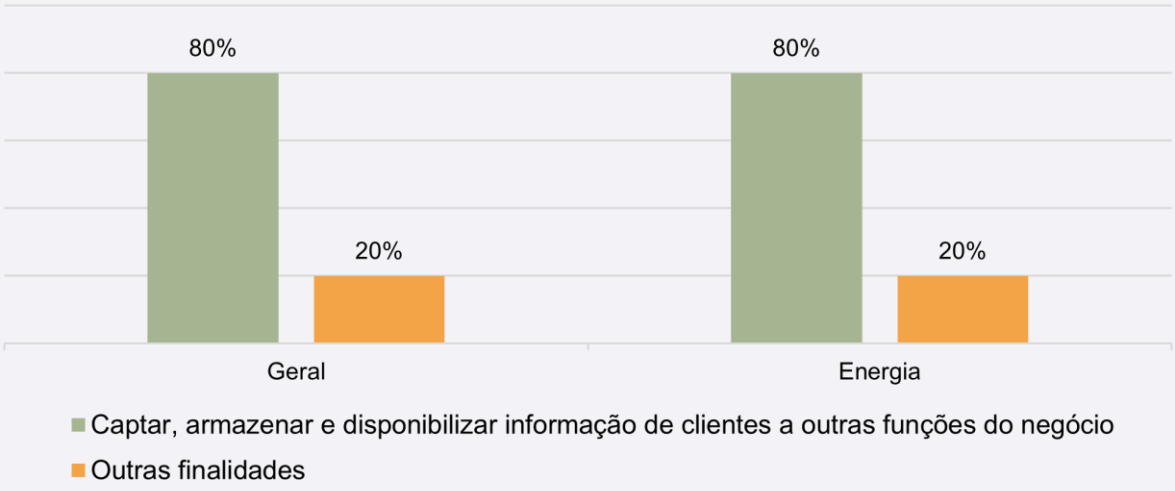
**Gráfico 54 - OSE que utilizam *Customer Relationship Management software* (*CRM*)**




São mais os operadores que não utilizam *software* de *Customer Relationship Management* (*CRM*)[31] - 62% - do que aqueles que utilizam - 38%. No setor de energia, a maioria dos operadores (63%) já utiliza esse tipo de *software*.

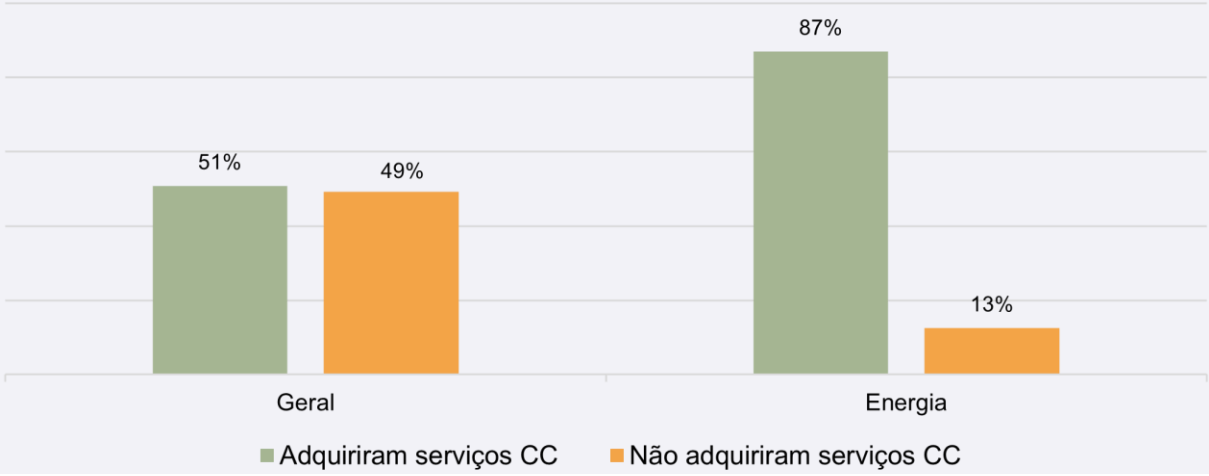
[31] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

**Gráfico 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 da energia espelha na sua totalidade a generalidade.

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



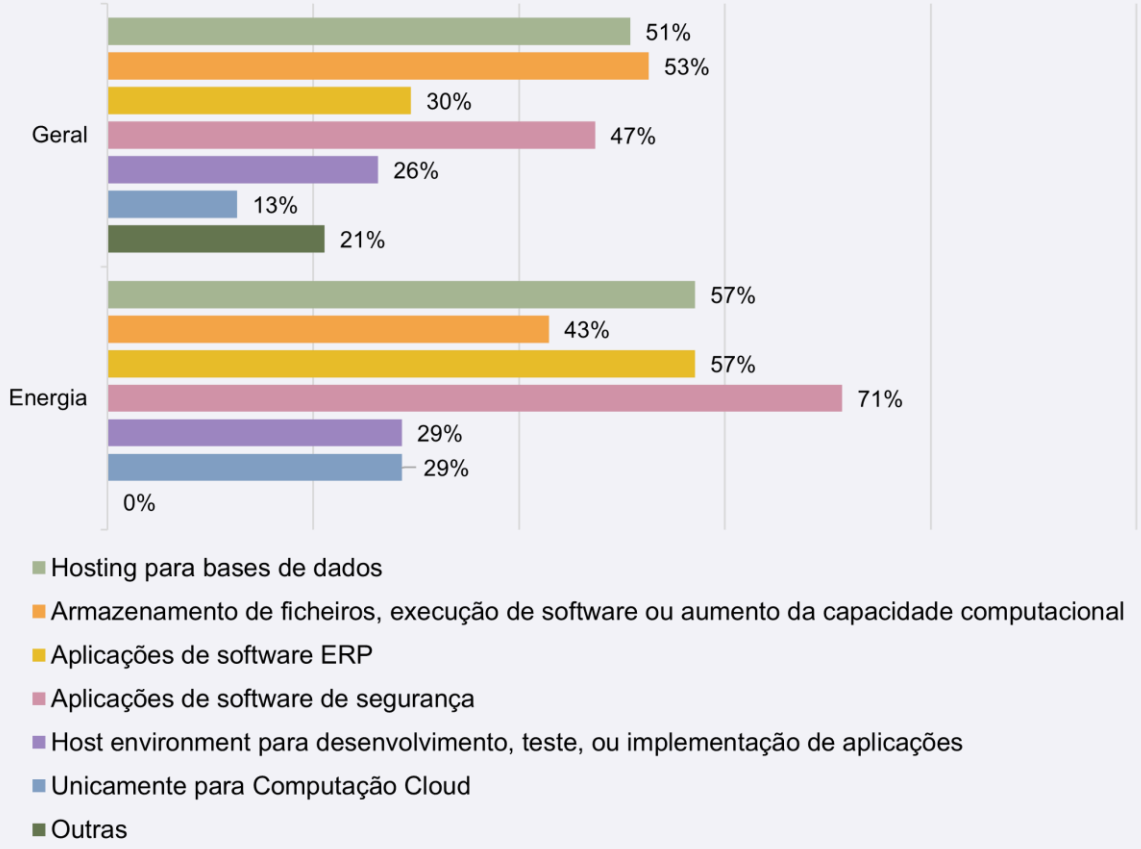

À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização. O setor da energia, é um dos setores que mais procuraram este tipo de serviços (87%).

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[32]. Em 2023, este tipo de serviços continuou a ser uma das áreas onde os OSE

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

mais aumentaram o seu investimento (49% dos OSE inquiridos pela ENISA em 2023 indicaram ter aumentado os seus investimentos em plataformas *cloud*)[33]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[34].

**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[35] 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.

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

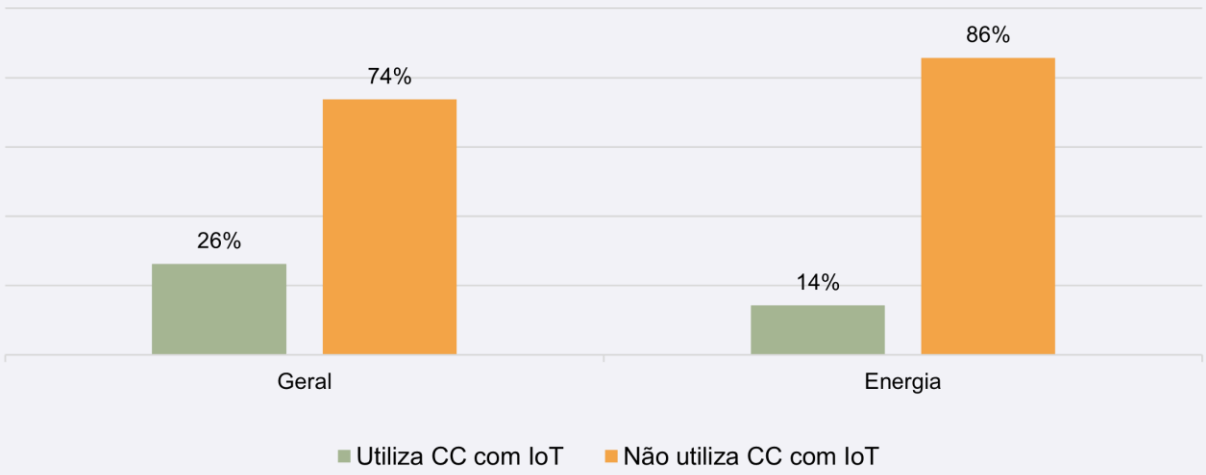
[34] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

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

A nível setorial, torna-se evidente que no setor da energia, a computação *cloud* é mais utilizada em aplicações de software de segurança (71%), seguido de hosting para base de dados e aplicações de software ERP (57% para ambas).

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

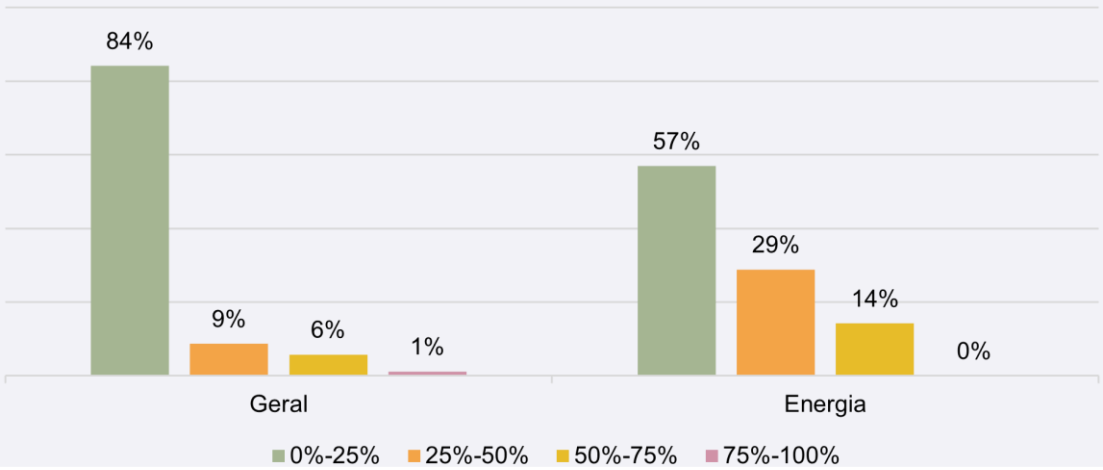
**Gráfico 58 - Utilização de serviços de CC em conjunto com Internet of Things (IoT)**




De modo geral, não é frequente, entre os OSE, a utilização de serviços de Computação *Cloud* (CC) em conjunto com a *Internet of Things* (IoT), embora alguns operadores o façam (26%). Especificamente, o setor da energia fica aquém do limiar dos 15% de utilização de CC com IOT.

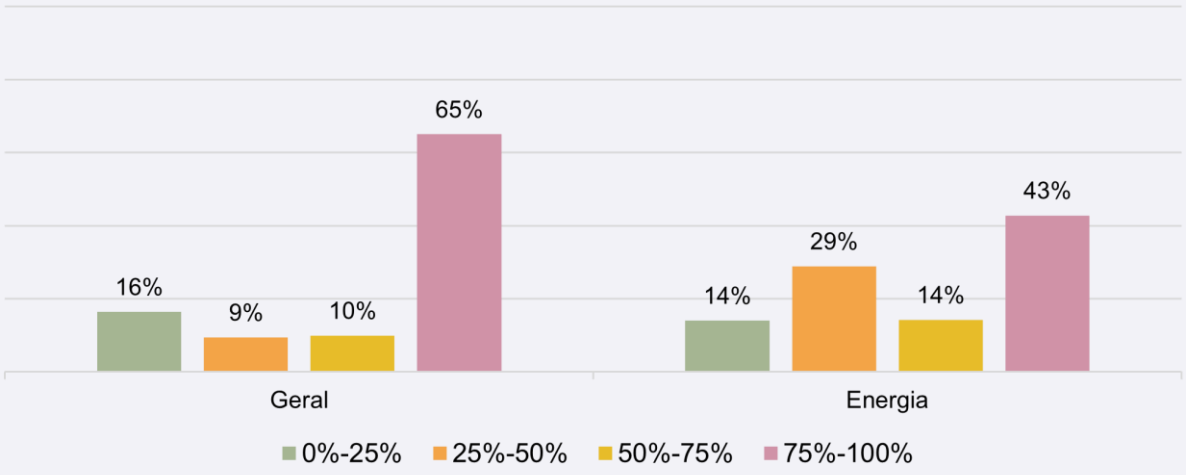
[36] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

**Gráfico 59 - Percentagem de sistemas *core* em *cloud***



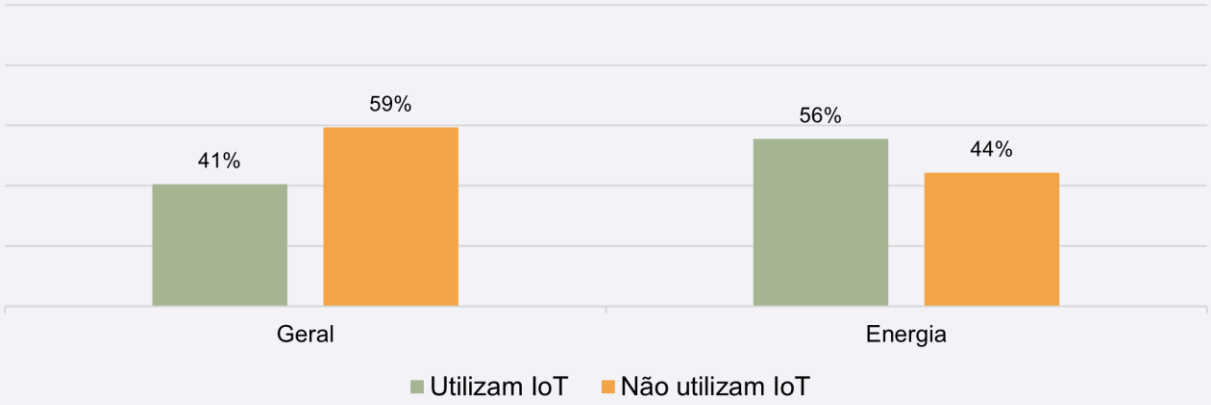

Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos. Há, no entanto, exceções. Por exemplo, no setor da energia, registam-se OSE cuja percentagem de sistemas *core*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

**Gráfico 60 - Percentagem de sistemas *core on-perm***




Contrastando com o gráfico anterior, aqui se mostra a tendência dos operadores em manter os seus sistemas core no próprio ambiente da organização (*on-prem*) e não na *cloud*. De um modo geral, cerca de 60% dos operadores inquiridos referem que mantêm entre 75% a 100% de sistemas principais dentro do ambiente de TI da sua organização. No setor da energia, prevalece a faixa de 75 a 100%, ainda assim as percentagens são bastante distribuídas, apresentando pouca diferença percentual entre as diferentes faixas.

**Gráfico 61 - Utilização de IoT pelos OSE**

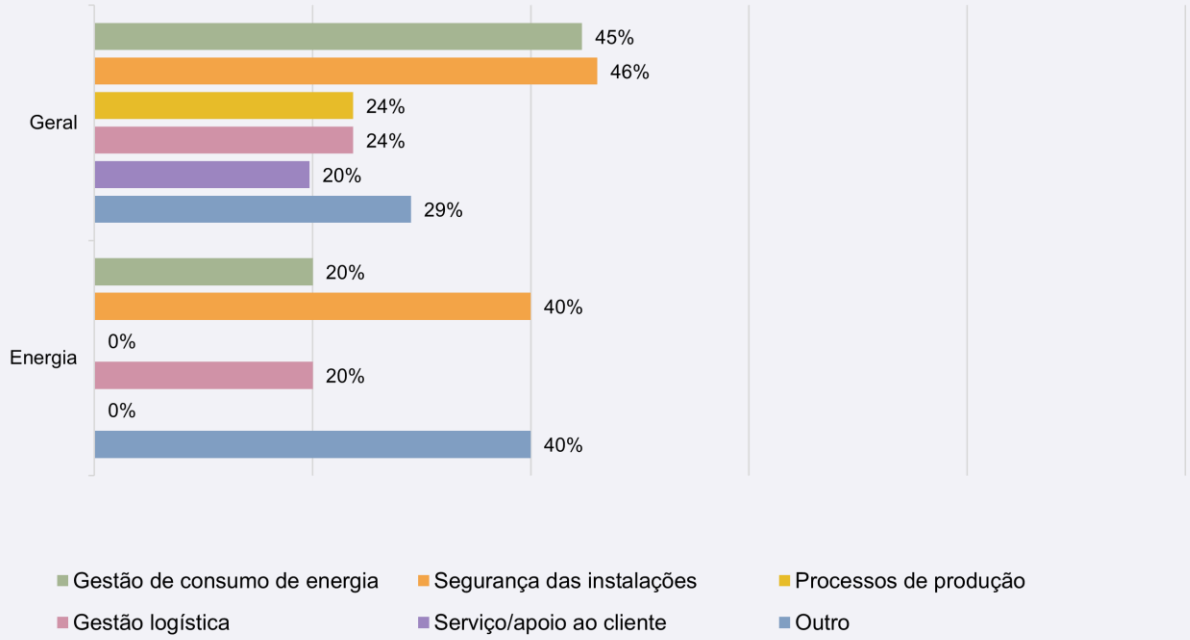



A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. No setor da energia, são mais os operadores que utilizam IoT do que aqueles que não utilizam, embora essa seja uma maioria ligeira, pouco acima dos 50%.

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

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

**Gráfico 62 - Contextos de utilização de IoT**




De maneira geral, a utilização de IoT é mais comum nos contextos de gestão do consumo de energia e de segurança das instalações, respondido por cerca de 45% dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. Contudo, no setor da energia, o uso de IoT para a segurança das instalações. Neste setor, a opção "Outro" contempla a utilização de IoT para fins de manutenção preditiva e de telemetria.

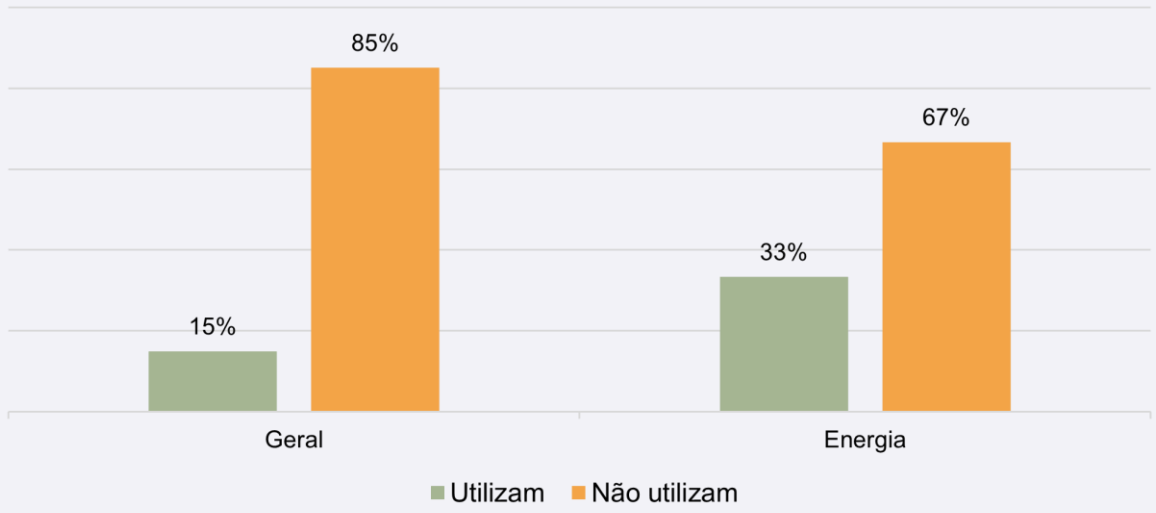
O mesmo estudo da ANACOM mencionado no gráfico anterior indica que "os equipamentos IoT foram sobretudo utilizados para segurança das instalações (86%), gestão do consumo de energia (32%), gestão logística (21%), processos de produção (19%), monitorização das necessidades de manutenção (18%) e serviço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

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

**Gráfico 63 - Motivos pelos quais não utilizam IoT**


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

**Gráfico 64 - OSE que utilizam processos que recorrem a IA**




A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.
Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. Contudo, é de salientar o setor da energia, no qual já se registam mais de 30% dos operadores a recorrer a Inteligência Artificial.

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

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

**Gráfico 65 - Funções para as quais utilizam IA**

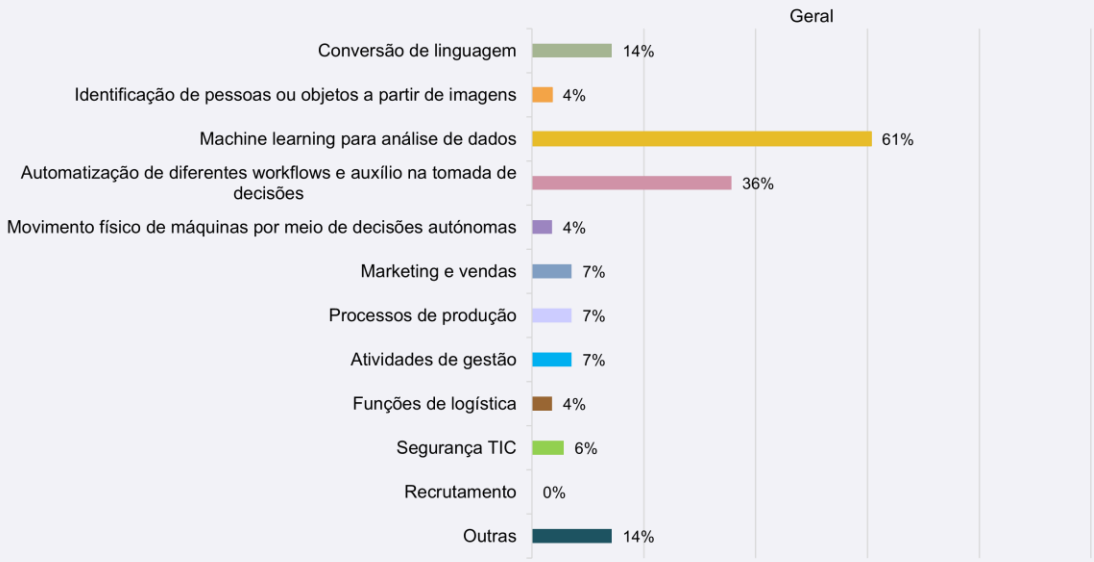
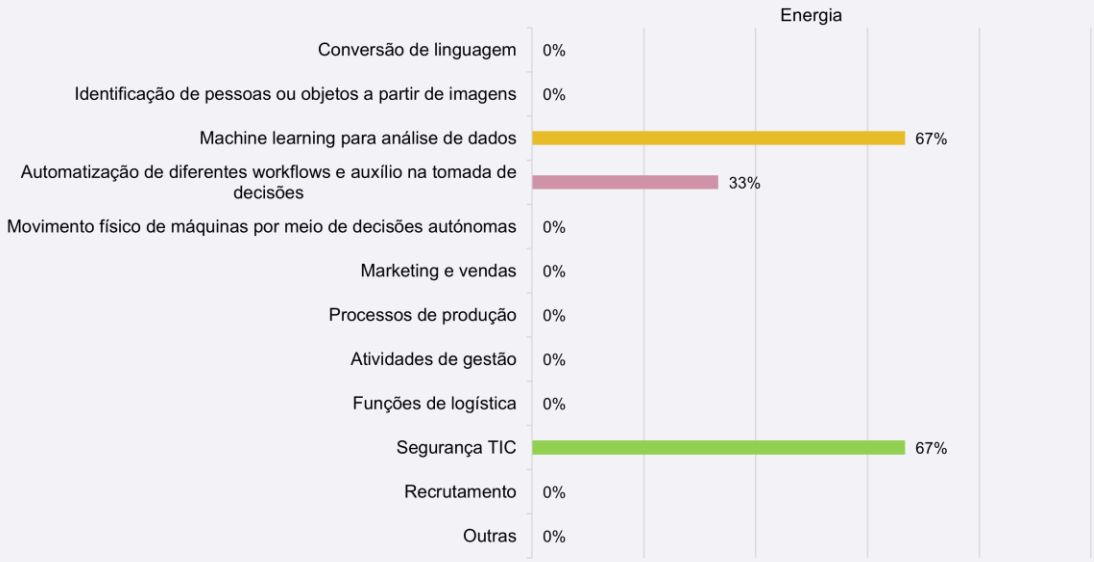



**Gráfico 65.1 - Funções para as quais utilizam IA**




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

indicada por 35% dos OSE que fazem uso de IA. As restantes funções surgem de forma mais residual, sendo indicadas por apenas 15% ou menos dos OSE que já recorrem a IA. Curiosamente, não se registou o recurso a Inteligência Artificial em processos de recrutamento entre os OSE inquiridos.
No setor da energia utilizam IA em *machine learning* para análise de dados, automatização de fluxos de trabalho e auxílio na tomada de decisões e em segurança TIC.

De acordo com os dados do IUTICE de 2023, entre as empresas que utilizam tecnologia de IA, 44,7% delas utilizam-na para identificar objetos ou pessoas através de imagens. Em seguida, 40,8% das empresas utilizam tecnologias que automatizam fluxos de trabalho ou auxiliam na tomada de decisão. Tecnologias para análise de linguagem escrita são utilizadas por 35% das empresas, apresentando um ligeiro. Já as tecnologias de aprendizagem automática para análise de dados, incluindo *deep learning*, são adotadas por 26,2% das empresas. A tecnologia de IA menos utilizada pelas empresas é a que permite a movimentação física de máquinas através de decisões autónomas baseadas na observação do meio ambiente, com apenas 8,3% de adoção. No entanto, no setor da Indústria e Energia, essa tecnologia é mais prevalente, sendo utilizada por 15,3% das empresas que empregam IA[41].

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

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

**Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança**

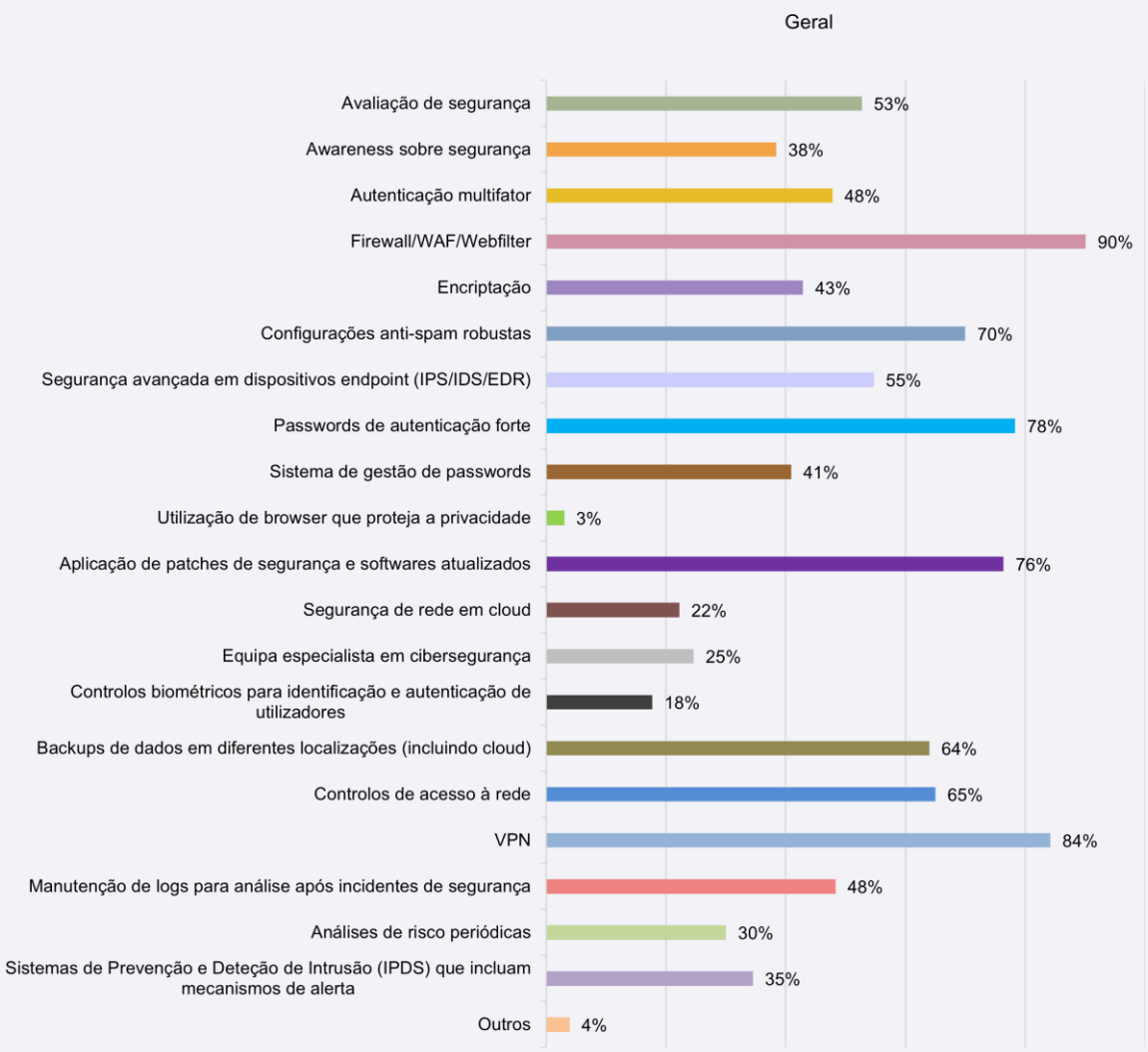


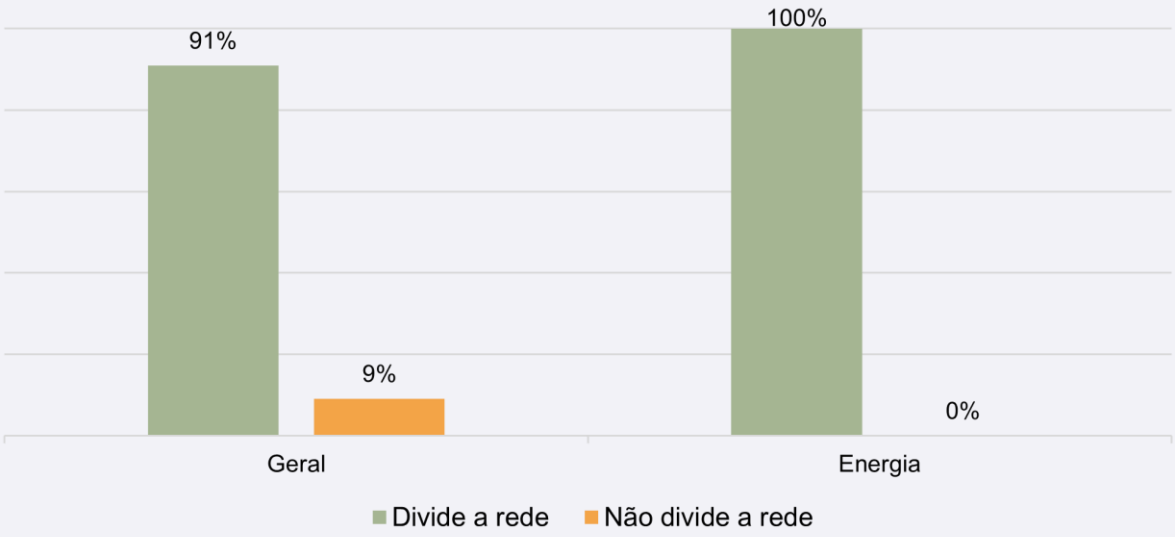
**Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança**


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%[44].

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

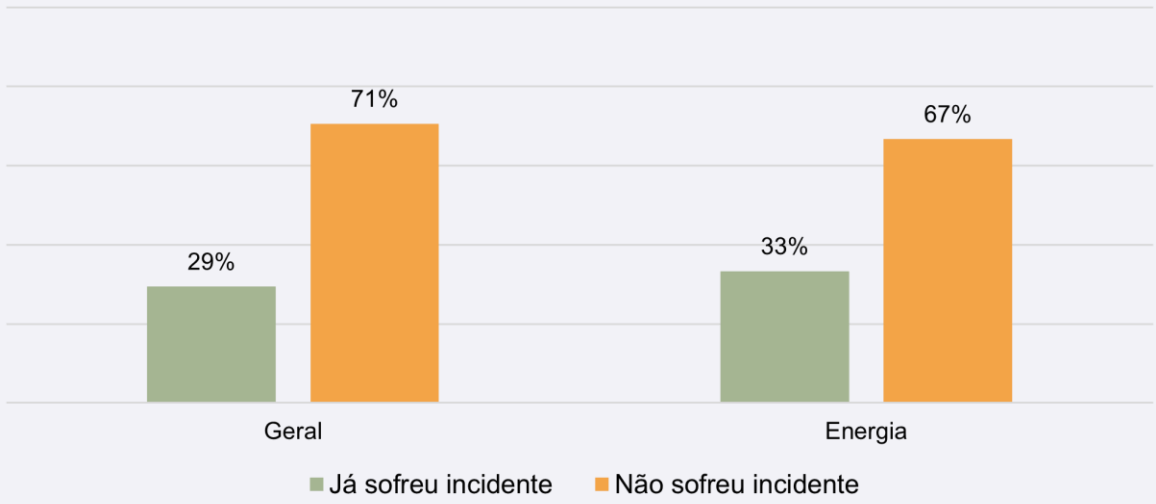
**Gráfico 67 - Divisão entre rede dos colaboradores e rede para guests**




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

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

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



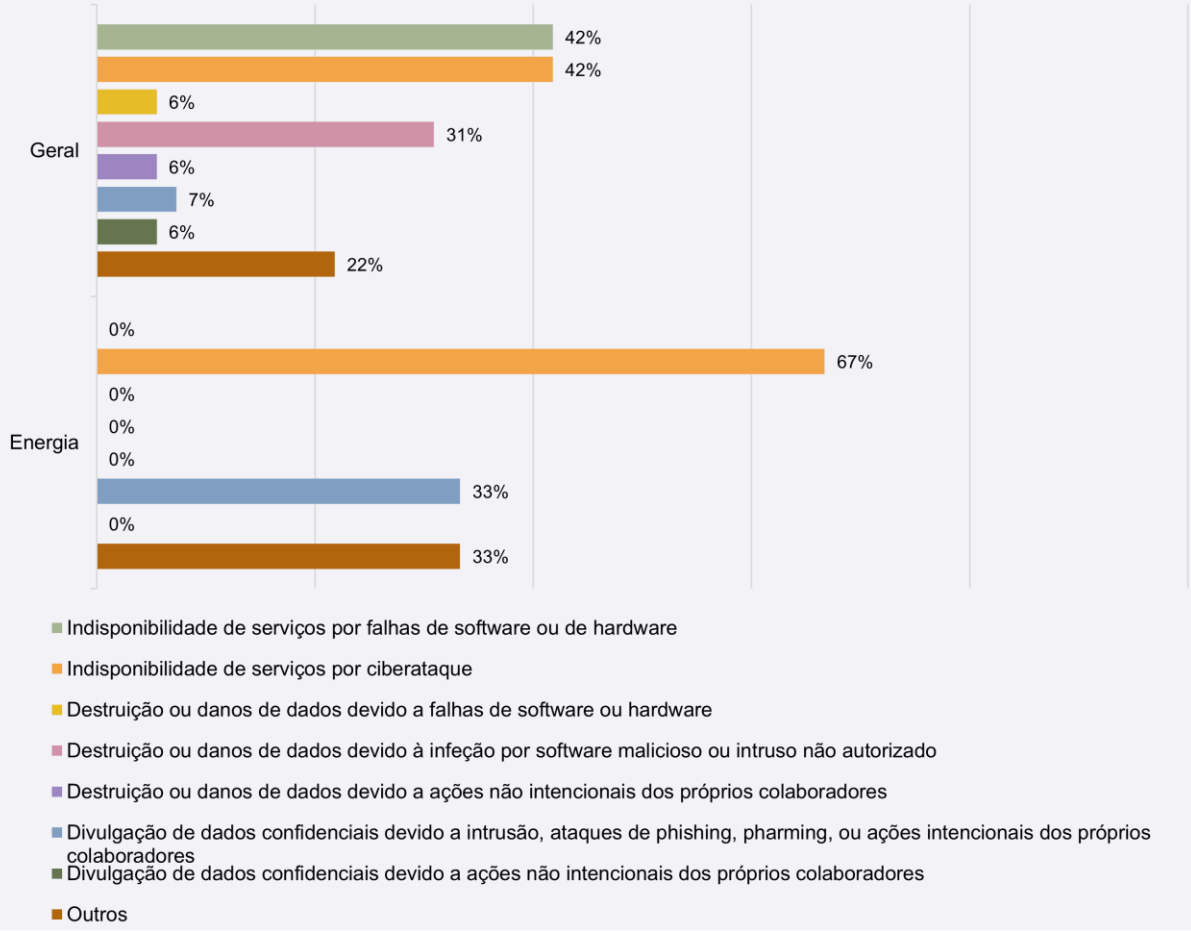

Em contexto TIC, pelo observado no gráfico, conclui-se que a maioria dos OSE inquiridos (71%) não sofreu incidentes neste contexto. O setor da energia segue a tendência geral, onde 33% referiram já ter sofrido incidentes de segurança.

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

O Fórum Económico Mundial (FEM) publicou um inquérito em janeiro de 2024, no qual contou com 199 empresas de 49 países. Neste inquérito, cerca de 29% das organizações reportaram que foram afetadas materialmente por um incidente de cibersegurança nos últimos 12 meses. Destas empresas, cerca de 41% afirmaram que o incidente ou incidentes foram causados por terceiros[47].

[46] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.
[47] 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. Destaca-se o setor da energia pela prevalência de incidentes que resultaram na indisponibilidade de serviços devido a ciberataque (67%).

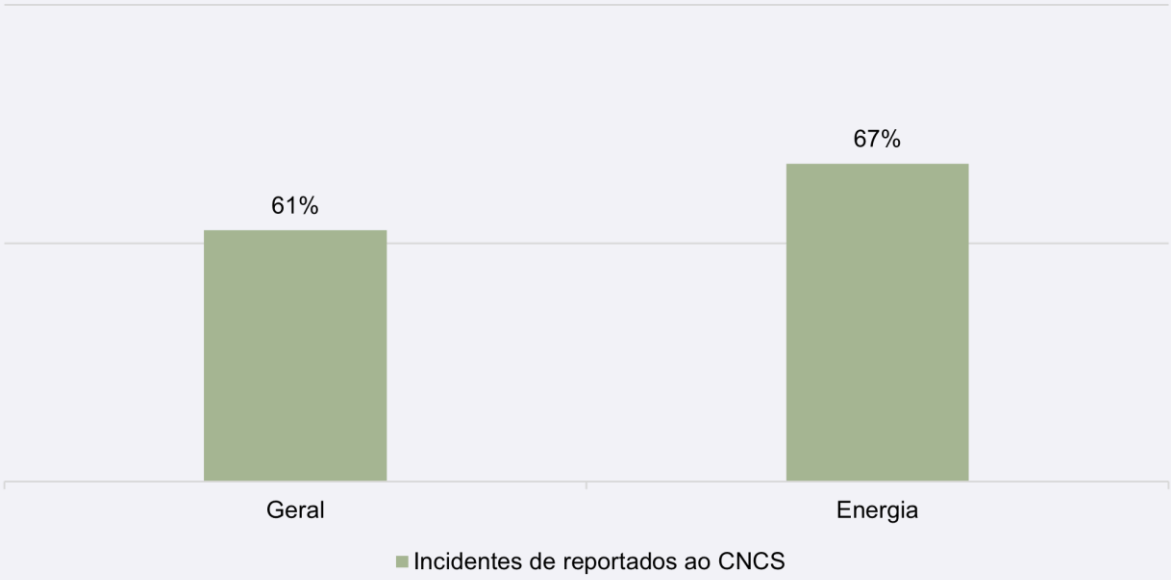
Nos “outros” incidentes ocorridos, referidos por os inquiridos que já sofreram incidentes, foram mencionados um acesso indevido a um computador empresarial na rede *guest*, fraude e compromisso dos prestadores de serviço, *DDoS* ou causados por terceiros bem como indisponibilidade de serviços por ataque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

Segundo dados do IUTICE de 2022, em 2021, 11,5% das empresas experienciaram pelo menos um problema, seja de indisponibilidade de serviços TIC, de destruição ou corrupção de dados, ou

de divulgação de dados confidenciais, devido a um incidente de segurança relacionado com as TIC. As consequências mais referidas destes incidentes foram a indisponibilidade de serviços TIC devido a falhas de *hardware* ou *software* e a ataques do exterior (8,3% e 2,5%, respetivamente), seguindo-se a destruição ou corrupção de dados devido a infeção de *software* malicioso ou intrusão não autorizada e devido a falhas de *hardware* ou *software* (2,1% e 1,8%, respetivamente)[48].

Segundo o estudo da Microsoft sobre o estado da cibersegurança em Portugal publicado em 2023, 70% dos inquiridos destaca o *phishing*, 63% dos inquiridos destaca os *softwares* maliciosos com cifragem de dados e pedido de resgate, 29% dos inquiridos destaca os ataques de negação de serviço *DDoS* pela sua capacidade de explorar vulnerabilidades nas redes e dispositivos programáveis da organização e, desta forma, perturbar os serviços e recursos das aplicações[49].

**Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS**

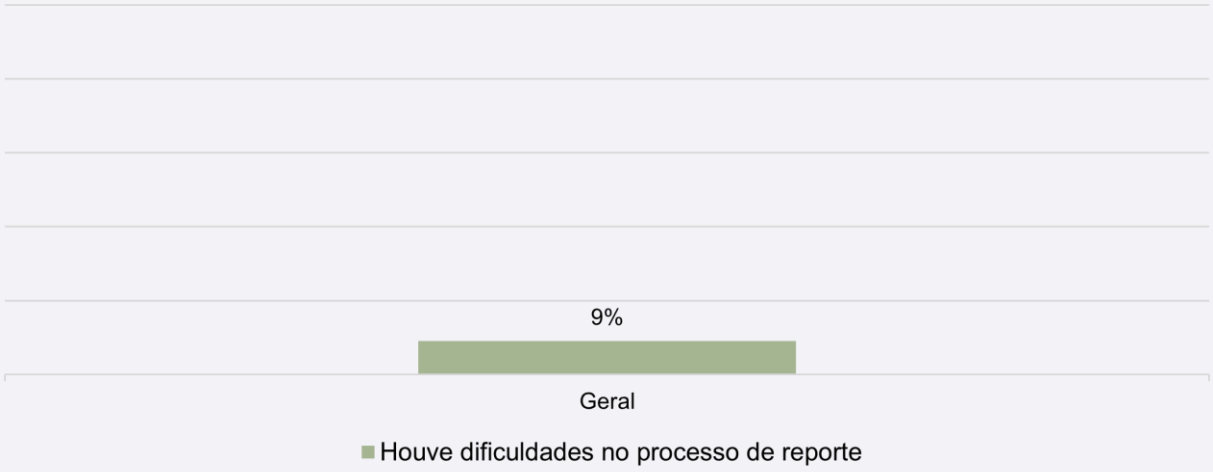



De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSE estão apenas obrigados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

No setor de energia, observa-se mais reportes de incidentes que na generalidade, onde mais de 67% 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.

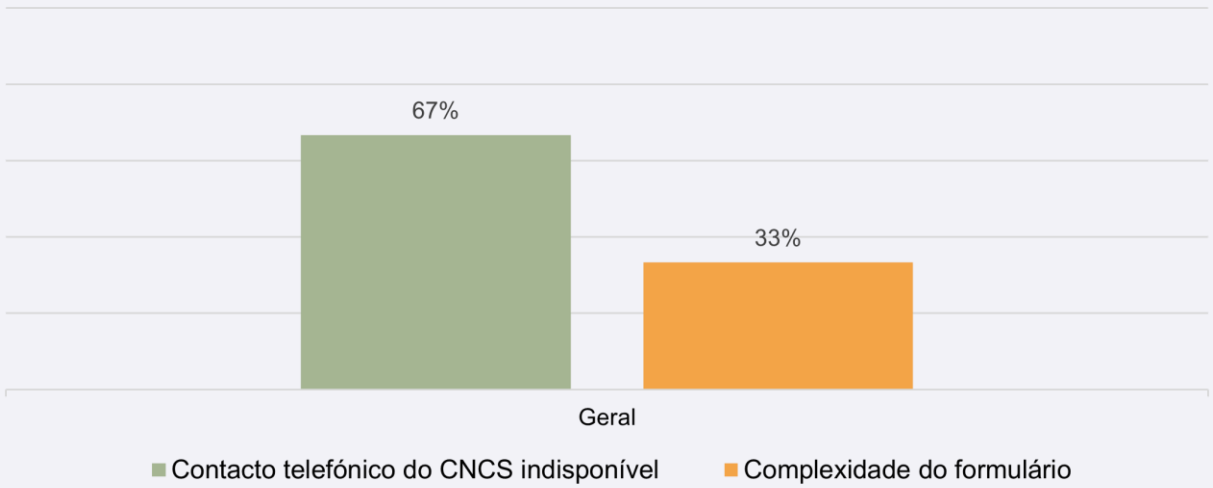
[48] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 20.
[49] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 6.

**Gráfico 71 - Dificuldades no processo de notificação ao CNCS**



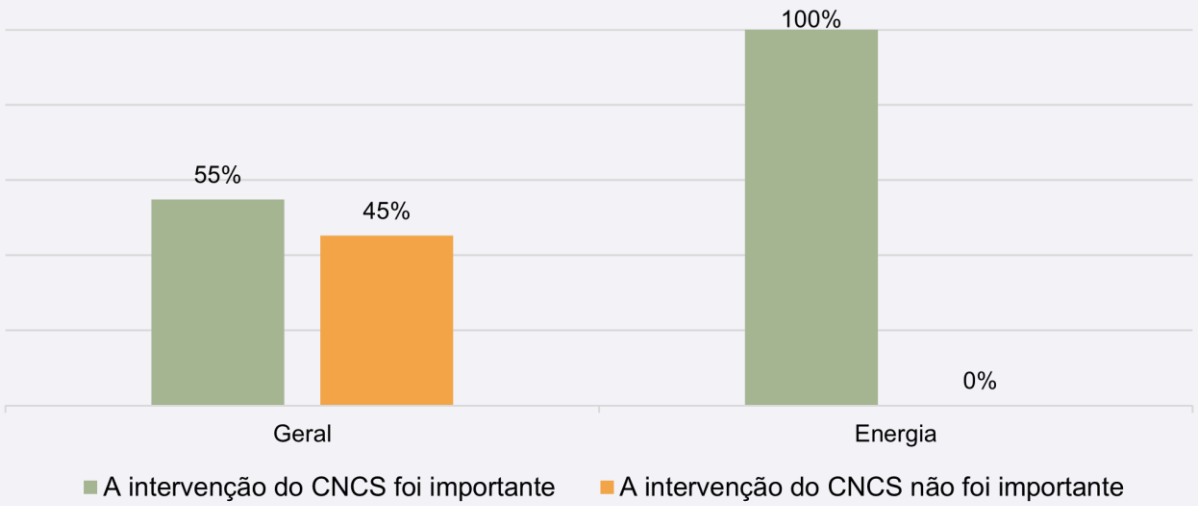

De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação. No setor da energia não existiram dificuldades no processo de notificação ao CNCS.

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



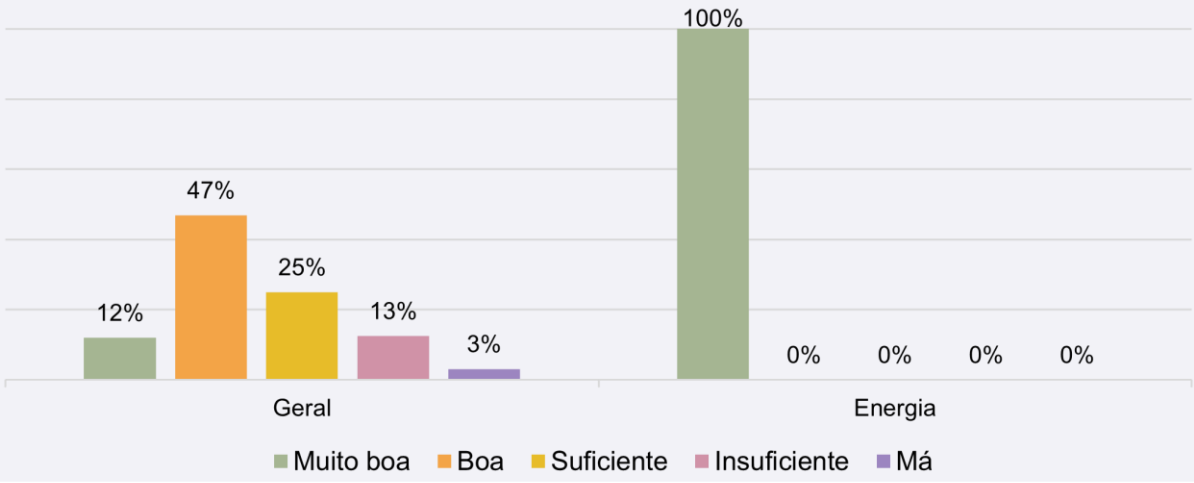

Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, dois referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico e um atribuiu a principal dificuldade à complexidade do formulário de notificação.
O setor de energia 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%). No setor da energia, é unânime, a totalidade dos operadores informou que a intervenção do CNCS foi importante na resolução do incidente notificado.

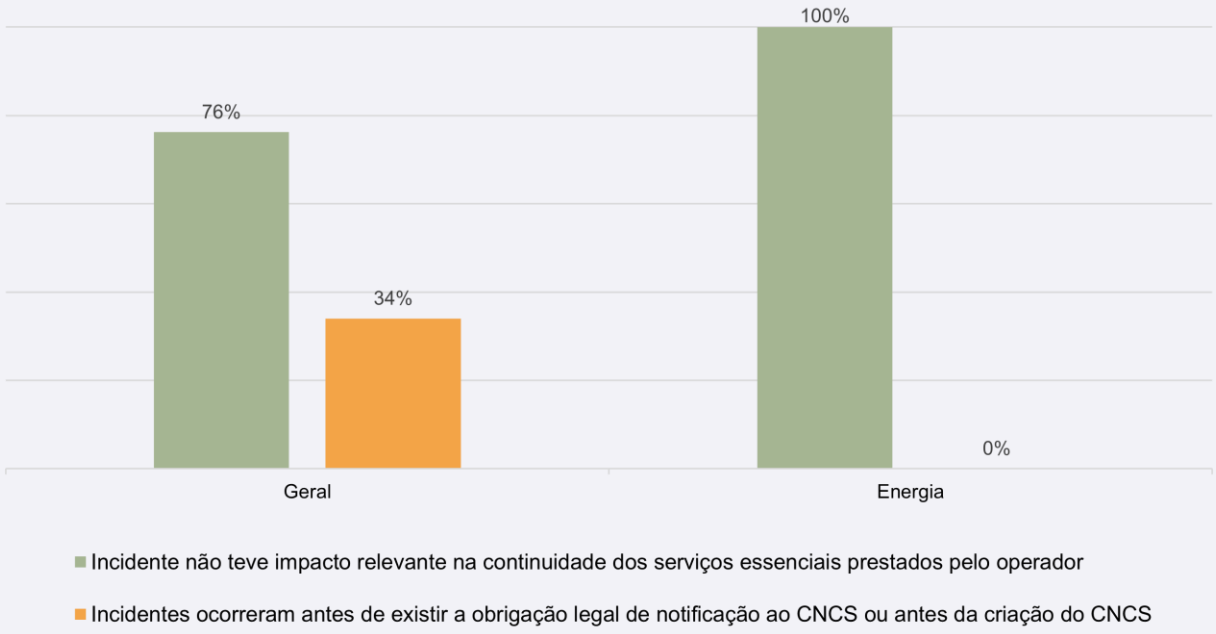
**Gráfico 74 - Avaliação da resposta dada pelo CNCS**




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

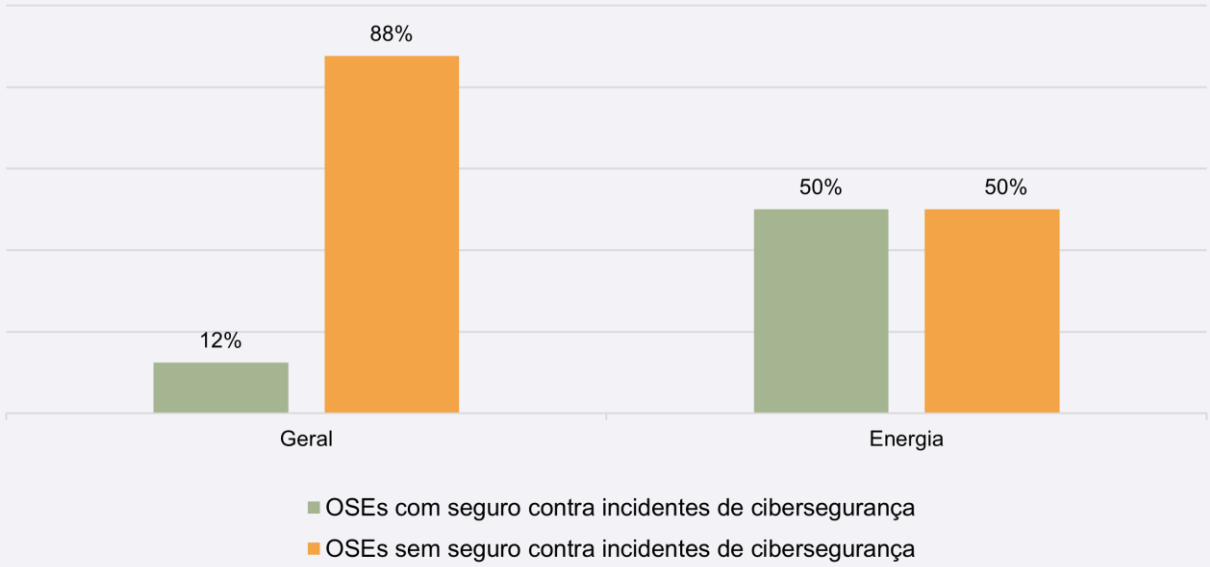
No setor de energia, 100% dos colaboradores inquiridos consideram que a resposta dada por parte do CNCS foi muito boa.

**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. Novamente, no setor da energia, a totalidade dos operadores referiu que o incidente não teve impacto relevante.

**Gráfico 76 - Seguro contra incidentes de cibersegurança**



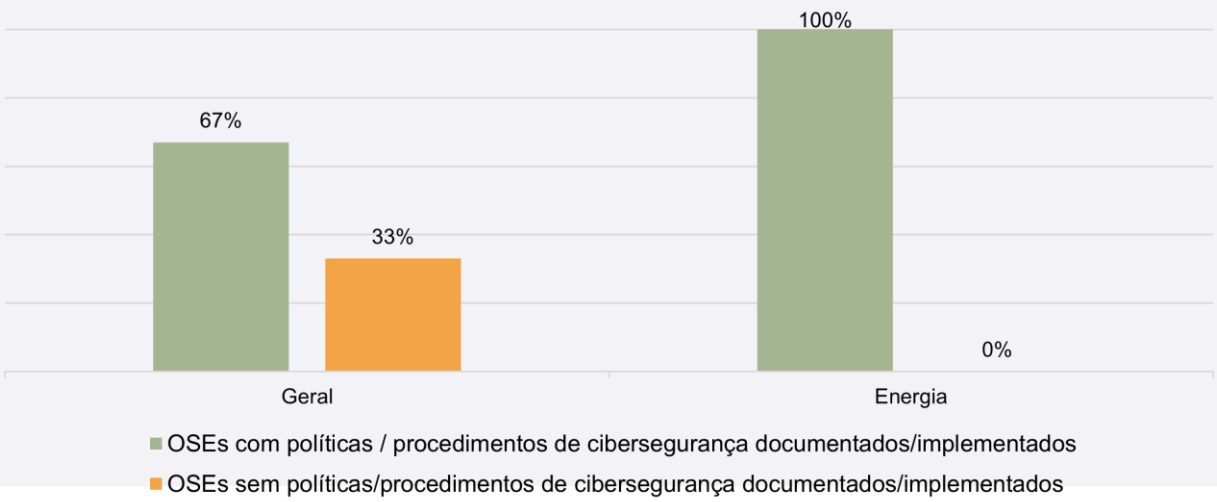

Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. O setor da energia é o setor onde mais operadores têm seguro contra incidentes de cibersegurança, chegando aos 50% de operadores com seguro.

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[50].

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[51].

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

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

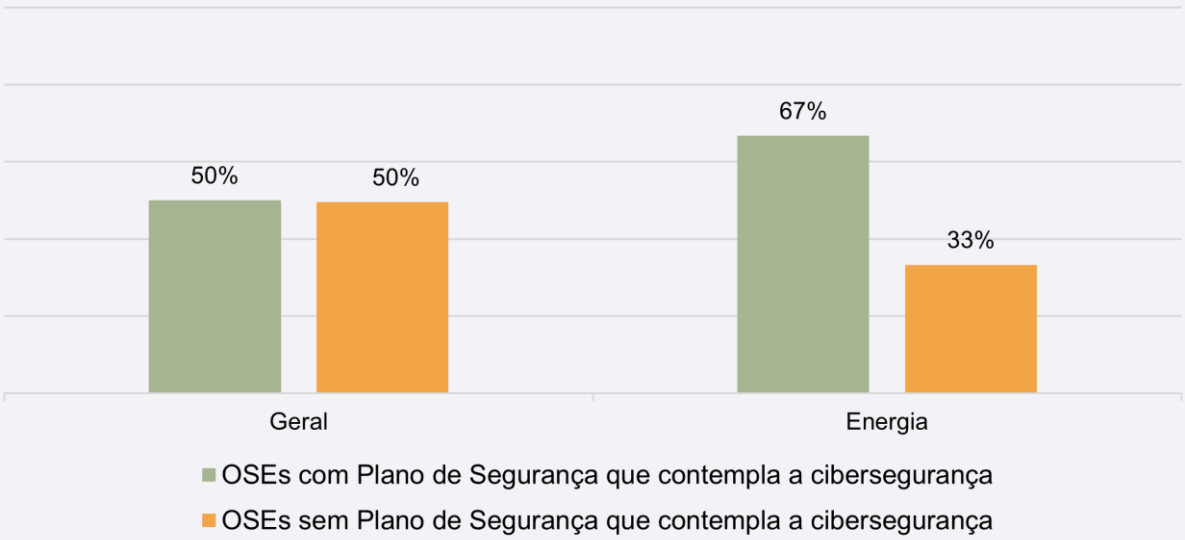



Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados. No setor da energia, todos os operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados.

Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança[52].

[52] 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 da energia, a maior parte dos operadores já tem um plano de segurança que contemple a área da cibersegurança (67%).

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[53].

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

**Gráfico 79 - Políticas incluídas no Plano de Segurança**

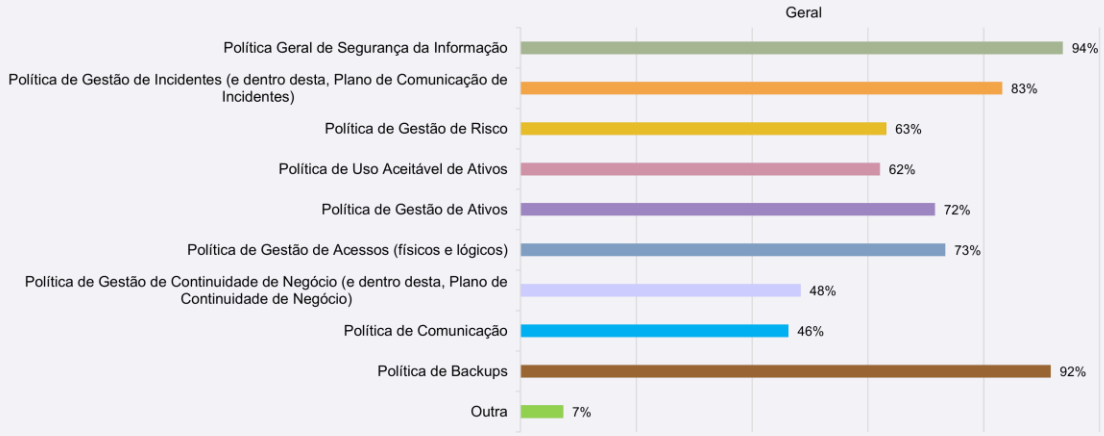
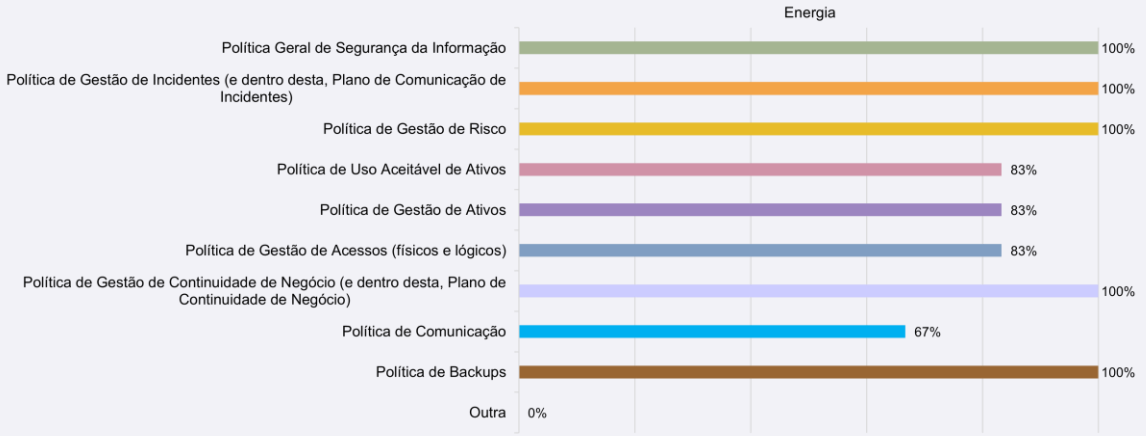



**Gráfico 79.1 - Políticas incluídas no Plano de Segurança**

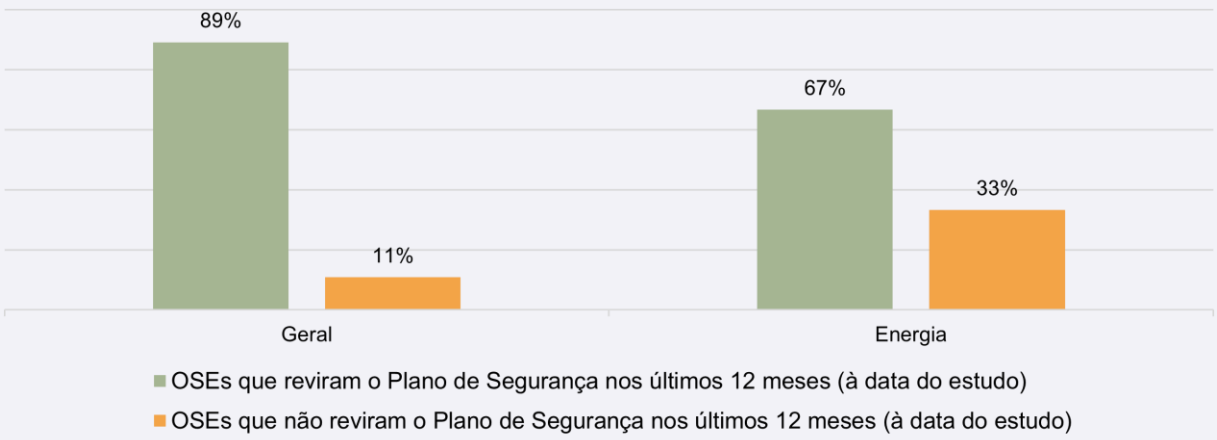



Os gráficos acima representam a percentagem de operadores com plano de segurança que tem as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.

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

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

**Gráfico 80 - Revisão do Plano de Segurança**




Cerca de 89% dos operadores com plano de segurança fizeram a revisão anual do mesmo nos últimos 12 meses, à data do estudo, seguindo as exigências do artigo 7º do decreto-lei nº 65/2021. Apenas em dois setores, sendo um deles o da energia, os resultados estão abaixo dos 80% de operadores que reviram o plano de segurança nos últimos 12 meses, à data do estudo.

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

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[54].

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


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

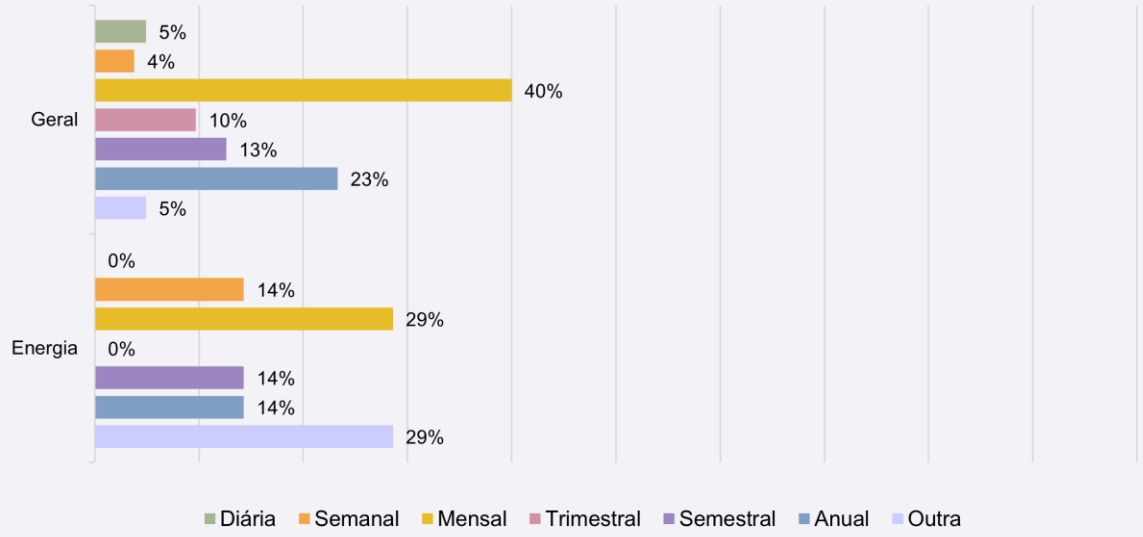
Mais de 60% dos operadores inquiridos dos diferentes setores referem realizar procedimentos de deteção e gestão de vulnerabilidades.
No setor da energia, a percentagem de operadores que realiza estes procedimentos fixa-se nos 78%.

**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 da energia, todos os operadores que já realizavam procedimentos de deteção e gestão de vulnerabilidades, fazem também a análise das mesmas.

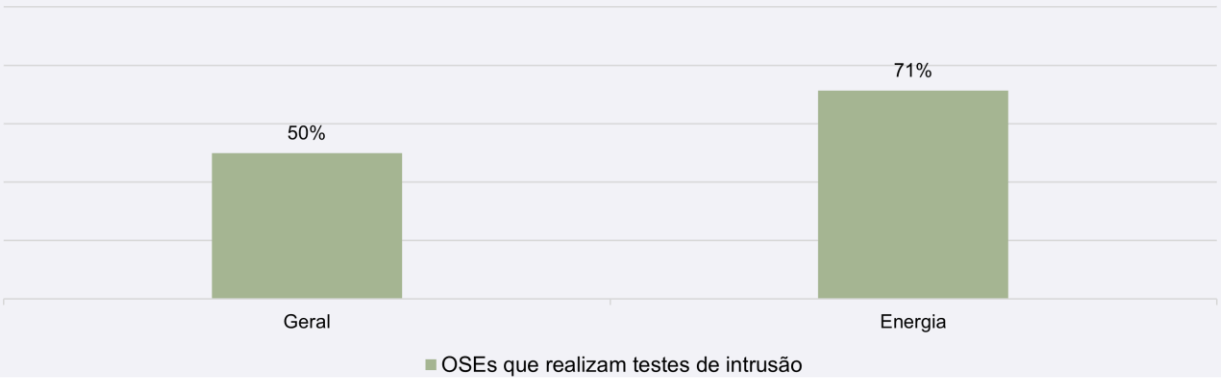
**Gráfico 83 - Frequência da análise de vulnerabilidades**




A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
A frequência semanal é a menos observada, não tendo sido indicada por qualquer operador de quatro setores.
Há ainda operadores, embora poucos, que realizam análise de vulnerabilidades diariamente.

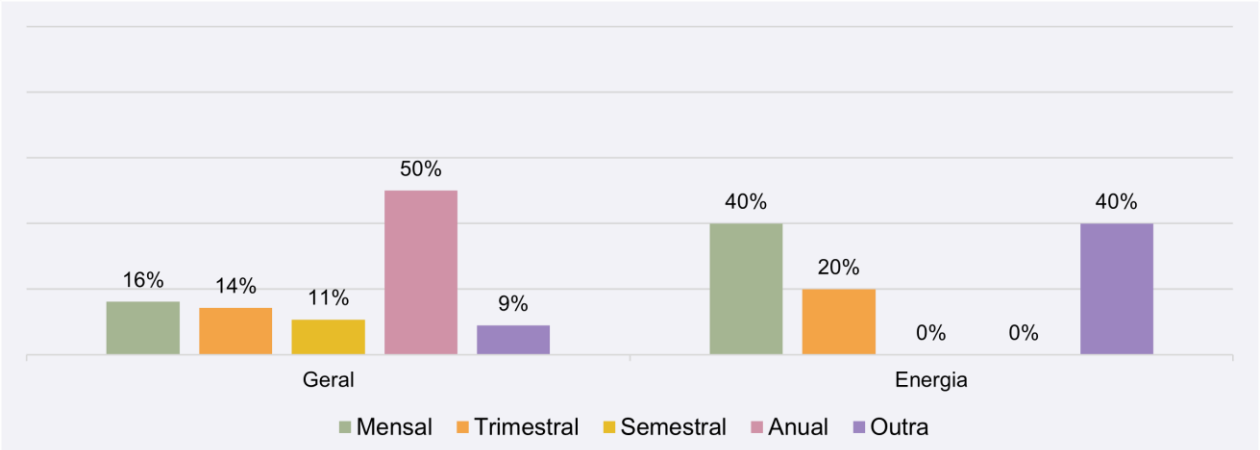
No setor da energia, existe alguma discrepância no tipo de frequência de análise de vulnerabilidades entre os operadores. Neste setor, as frequências mensal ou contínua são as que se verificam mais frequentemente. Nenhum operador referiu realizar análises de vulnerabilidades de frequência diária ou trimestral.

**Gráfico 84 - Realização de testes de intrusão**



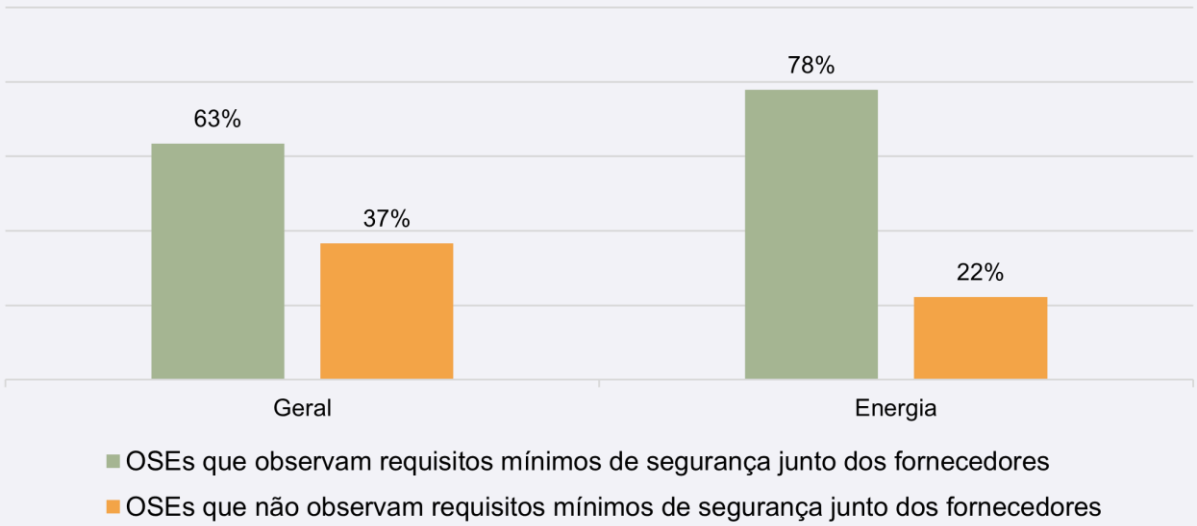

Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
É de salientar, o setor da energia, onde 71% dos operadores, respetivamente, realizam testes de intrusão.

**Gráfico 85 - Frequência de testes de intrusão**



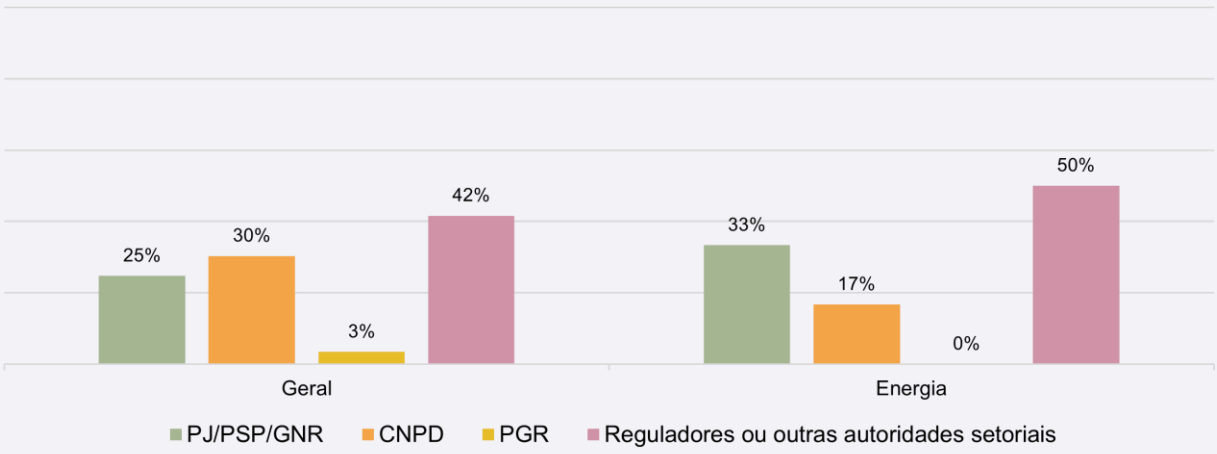

Com exceção dos operadores de serviços essenciais do setor da energia, os operadores dos setores tendem a realizar testes de intrusão anualmente.
A exceção verificada no setor da energia prende-se com o facto de todos os operadores realizarem esses testes com uma frequência superior à anual e semestral.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

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




Na generalidade, e também em cada setor, a maioria dos operadores (mais de 60%) procura que os seus fornecedores estejam alinhados com os requisitos mínimos de segurança por si exigidos. Sectorialmente, na energia, a observação dos requisitos de segurança por parte dos fornecedores ocorre em 78% dos operadores.

**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.

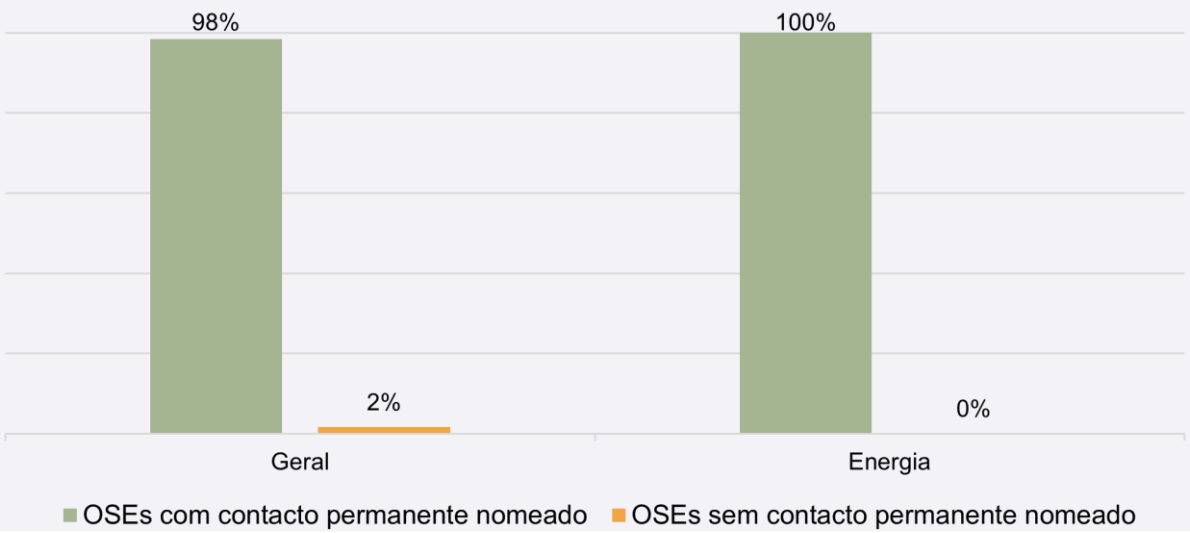
Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).

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.

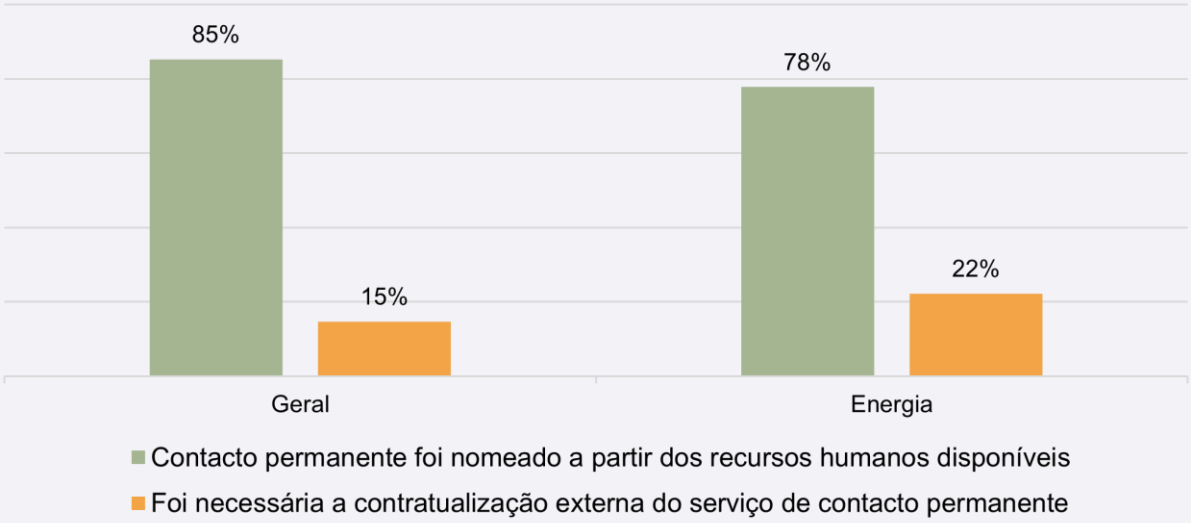
O setor da energia privilegia a notificação ao regulador ou outras entidades setoriais em caso de ciberataque ou incidentes. Depois destas entidades encontra-se a PJ/PSP/GNR e por último a CNPD.

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



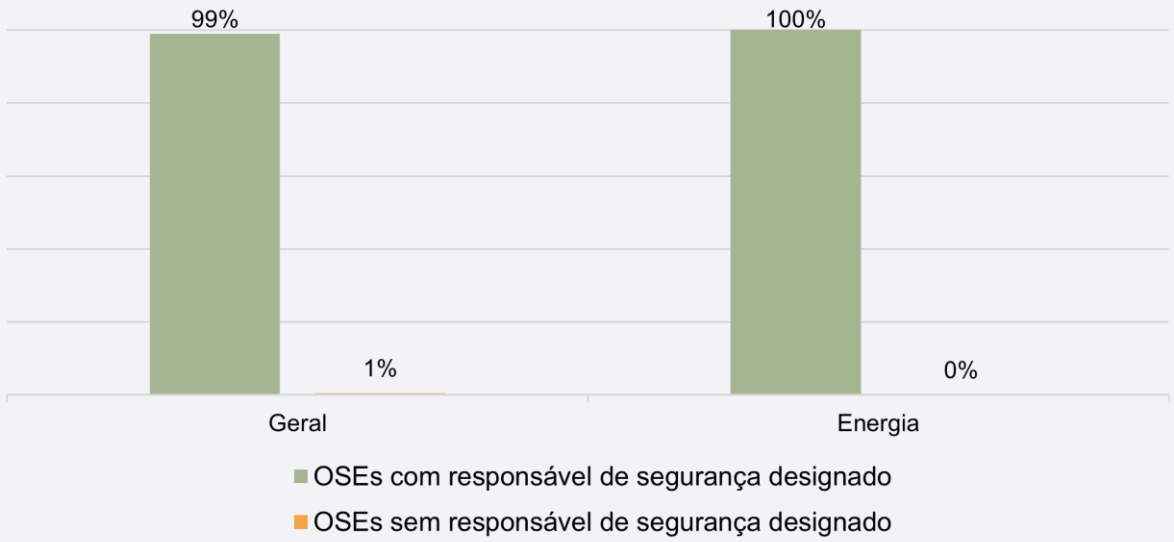

98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado.
Em apenas dois setores houve uma entidade inquirida que ainda não tinha nomeado o contacto permanente.

**Gráfico 89 - Designação do contacto permanente**



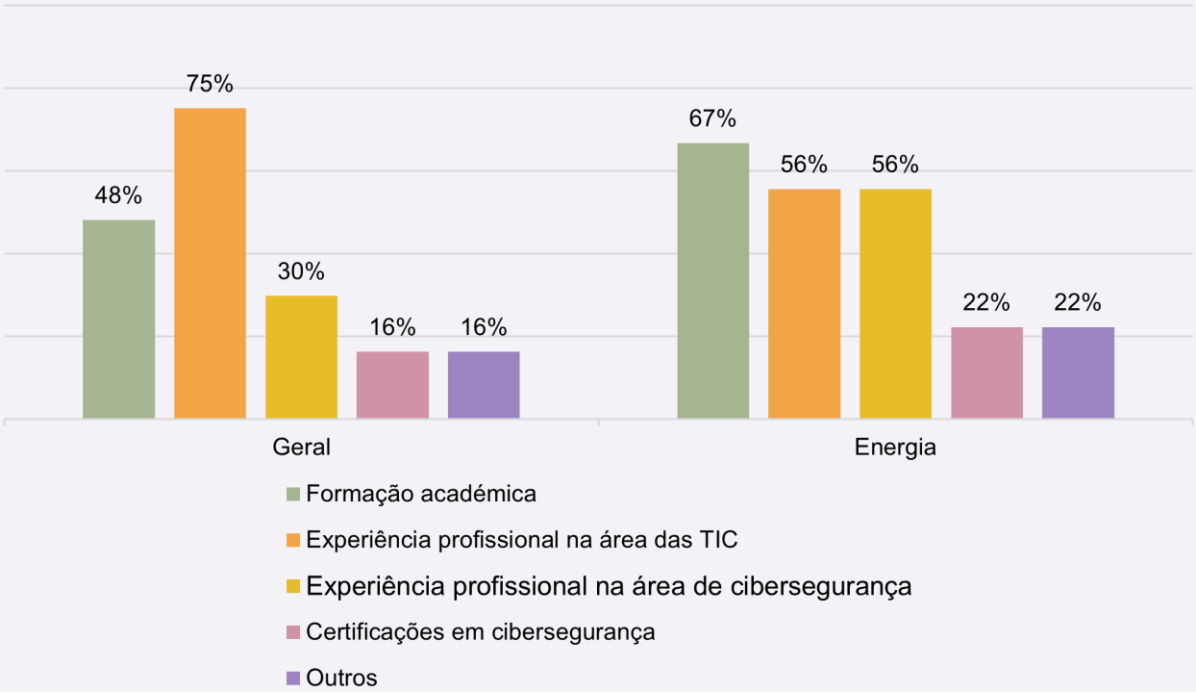

A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente, com particular destaque para o setor da energia, no qual a percentagem de operadores que necessitou de contratualizar o serviço foi de 22%.

**Gráfico 90 - Designação do responsável de segurança**




Tal como no requisito da nomeação do contacto permanente, também o requisito de ter designado um responsável de segurança é amplamente cumprido pelos OSE. Entre todos os inquiridos, apenas em um 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**

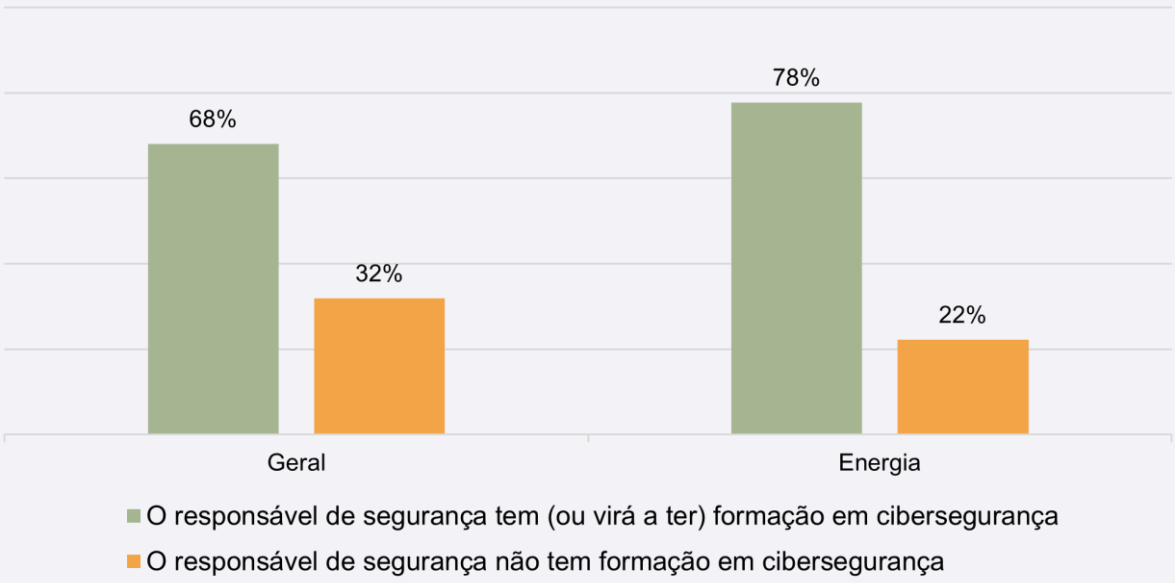



A formação académica e a experiência profissional na área das TIC e na área de cibersegurança foram os critérios mais importantes para a designação do responsável de segurança dos operadores. Na generalidade, a experiência profissional nas TIC foi um critério em 75% dos casos, a formação académica foi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

Verifica-se, contudo, duas exceções, sendo uma no setor da energia, onde o critério mais aplicado foi a formação académica, ao contrário do que é possível observar nos outros setores.

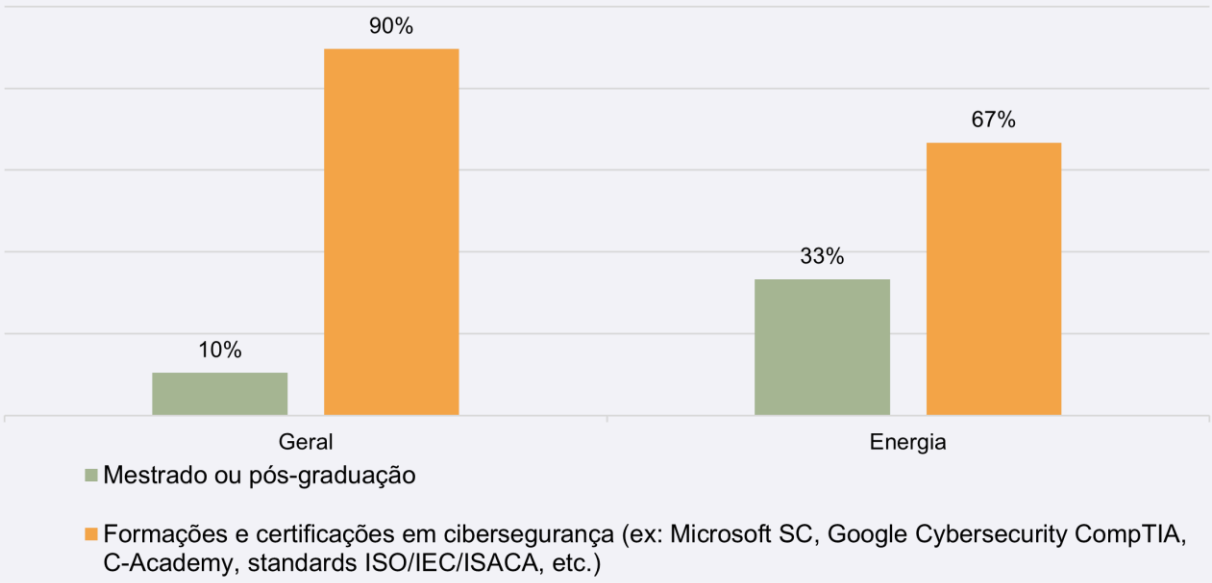
É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de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

**Gráfico 92 - Formação específica de cibersegurança do responsável de segurança**




Em cerca de 70% dos casos, o responsável de segurança tem ou virá a ter formação específica em cibersegurança. No setor da energia, a maioria dos operadores (78%), refere que o responsável de segurança tem (ou virá a ter) formação em cibersegurança.

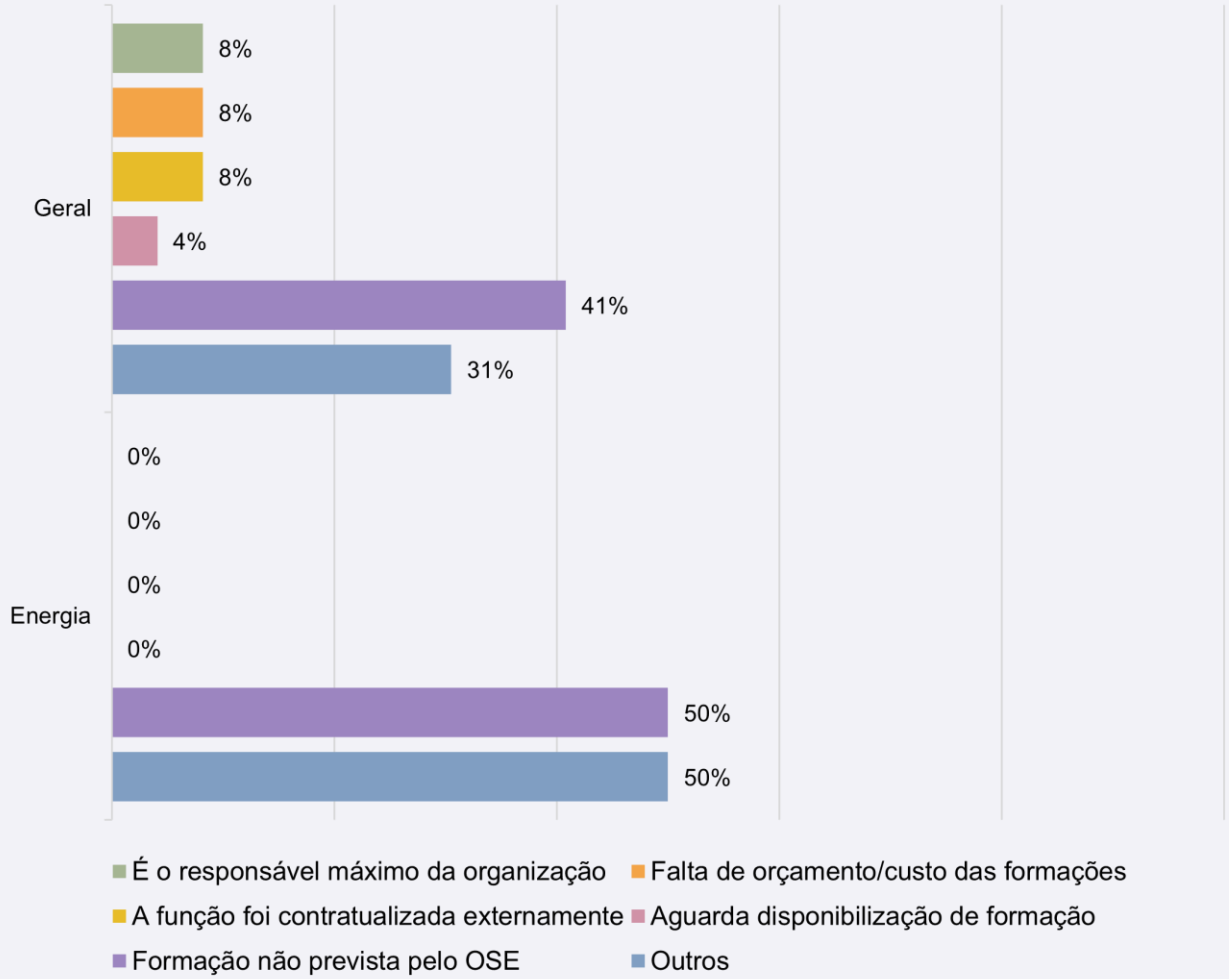
**Gráfico 93 - Tipo de formação específica em cibersegurança**




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

cibersegurança. Cerca de 90% dos responsáveis de segurança tem uma mais das formações do primeiro tipo.
O setor onde se verifica mais responsáveis de segurança com o grau de mestre ou de pós-graduado é o da energia, com mais de 30% dos responsáveis a terem este nível de qualificação.

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

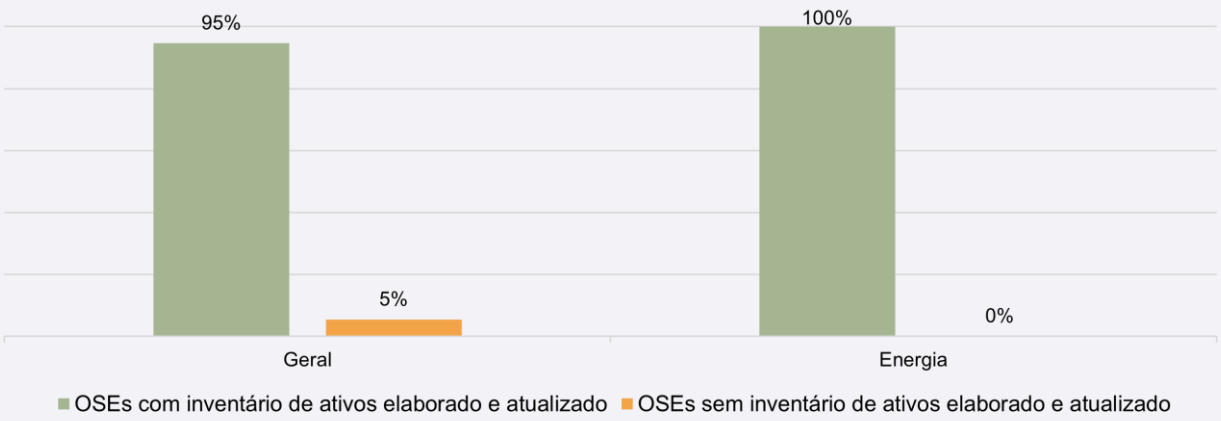



Os motivos pelos quais um responsável de segurança de um operador não tem formação específica em cibersegurança são diversificados. Na generalidade, o motivo mais vezes observado, em cerca de 40% dos operadores onde o responsável não tem formação na área, é o facto de essa formação não estar prevista 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 energia, a principal motivação para que o responsável de segurança não tenha formação específica em cibersegurança é maioritariamente o facto de a formação não estar prevista ou ainda estarem a analisar a possibilidade de integrar um CISO.

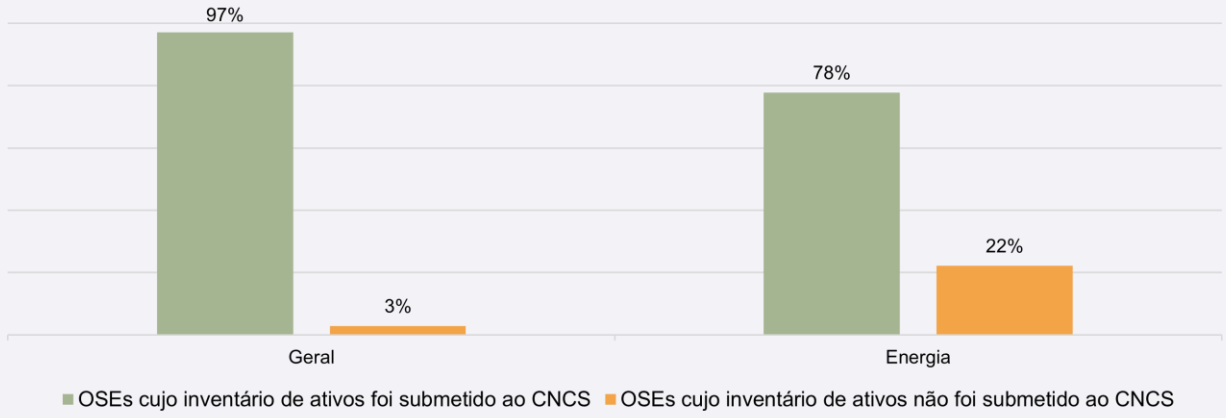
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado "Compromisso C-Academy" que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança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



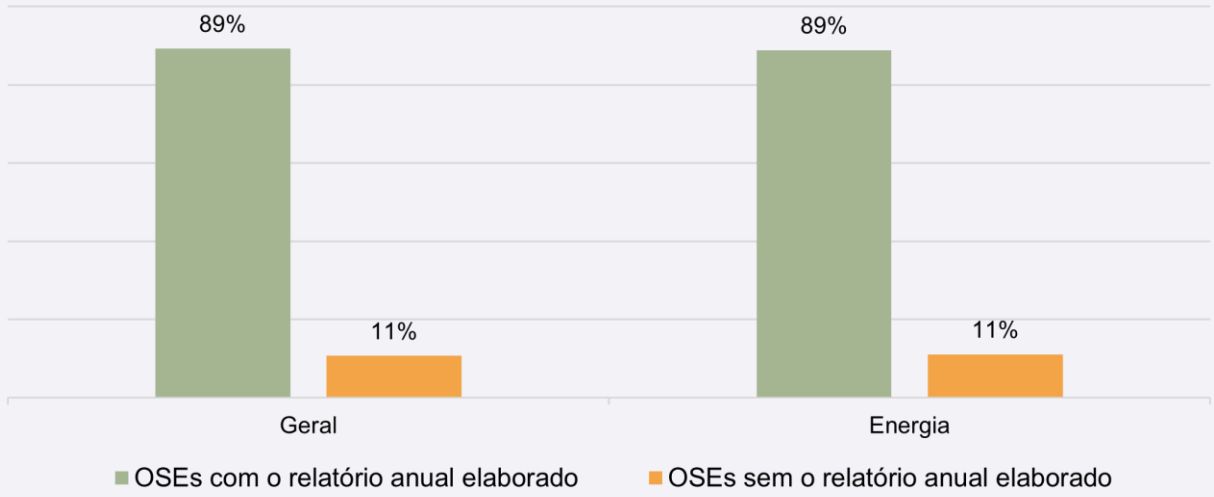

A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. Destaca-se o setor da energia, onde todos os operadores têm o seu inventário elaborado e atualizado.

**Gráfico 96 - Submissão do inventário de ativos ao CNCS**



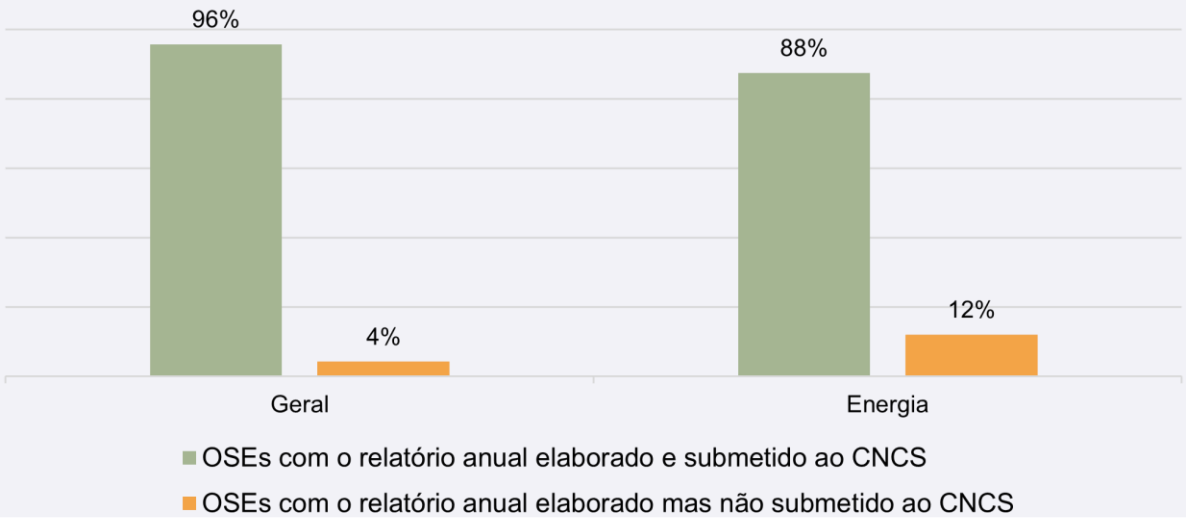

Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. As exceções são observadas no setor da energia (o único em que se ultrapassam os 20% de operadores que não submeteram o inventário).

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



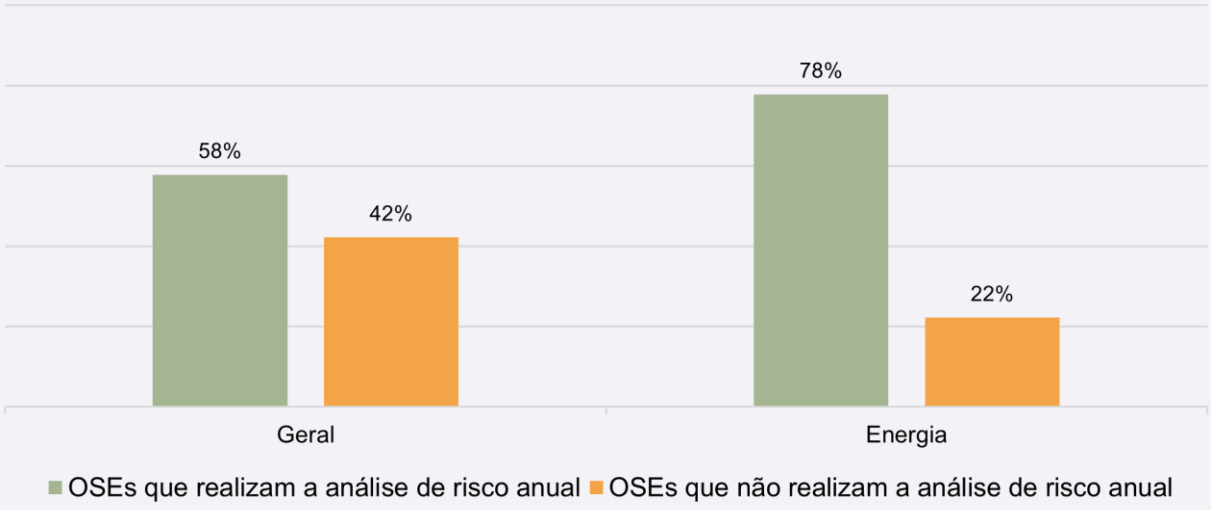

Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. O setor da energia espelha a generalidade.

**Gráfico 98 - Submissão do relatório anual ao CNCS**



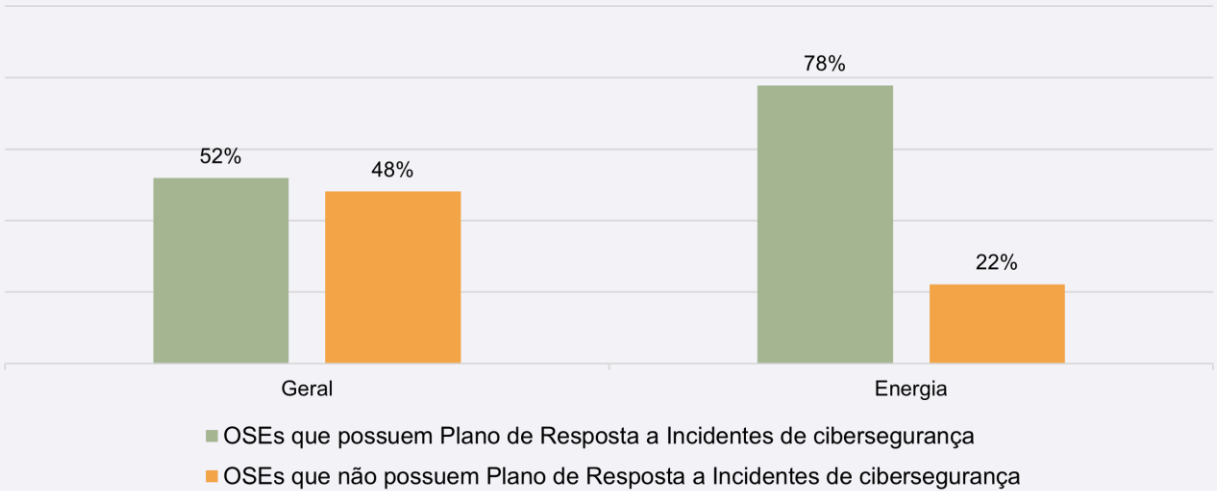

Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. Os casos em que tal não se verificou, ou seja, em que o relatório foi elaborado, mas não submetido, ocorreram em operadores do setor energético (12,5%).

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



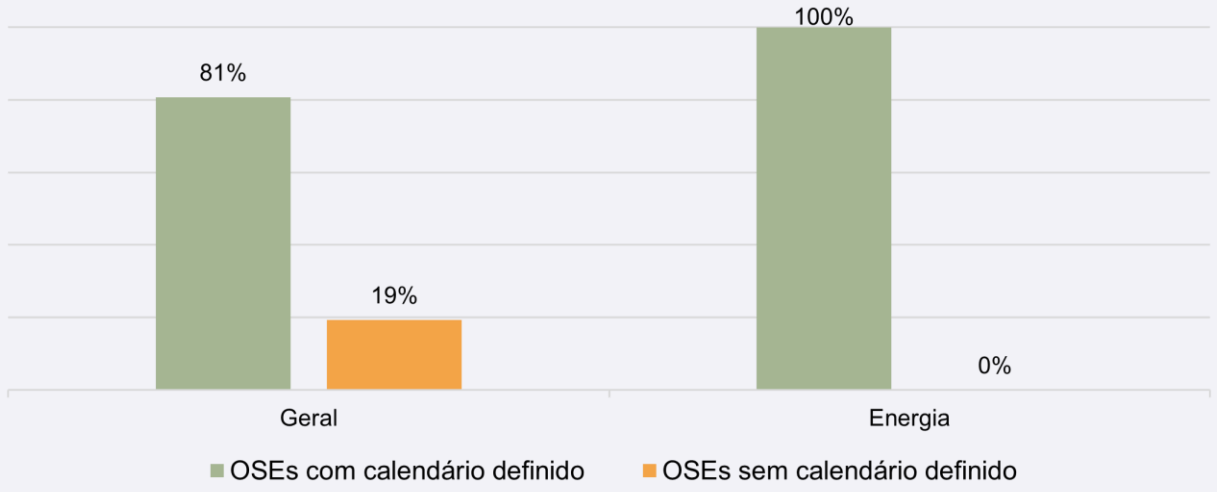

A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. O setor da energia é um dos setores nos quais maior percentagem dos operadores realiza esta análise (78%).

**Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança**



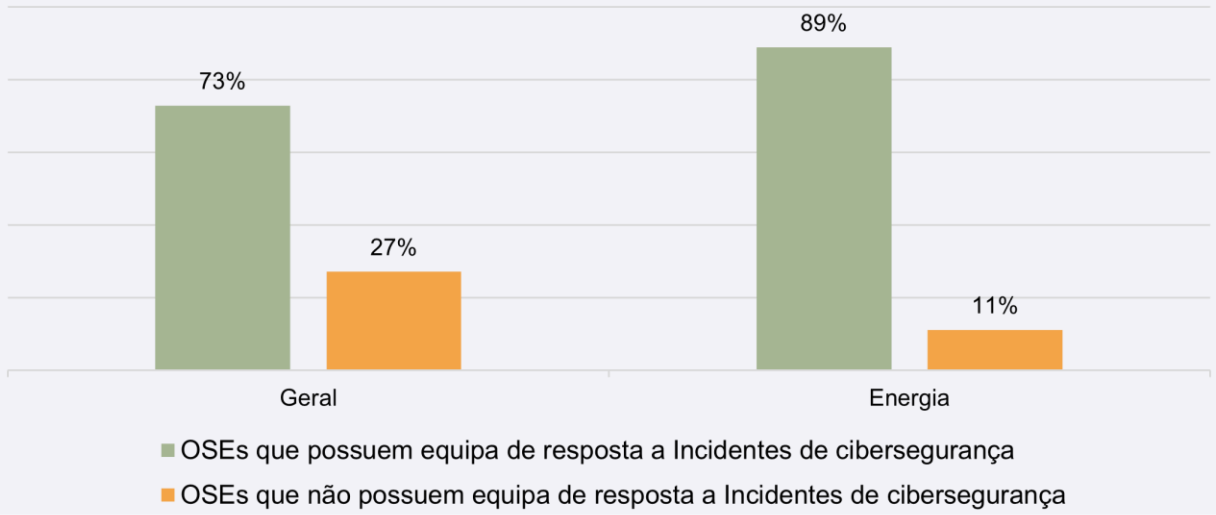

Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. O setor da energia apresenta o segundo resultado mais elevado, atingindo os 78%.

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



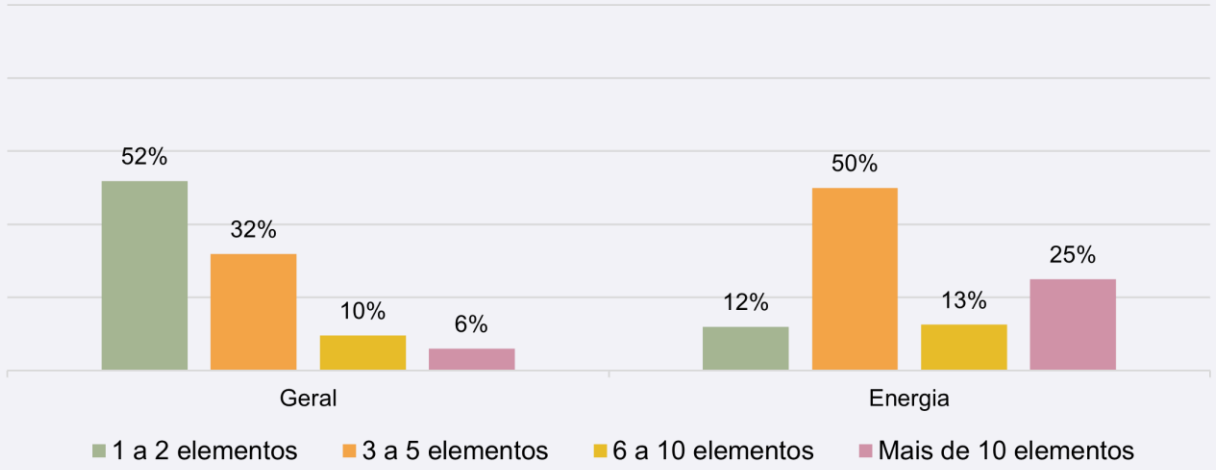

A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. O setor da energia indica ter tal calendário definido. Há que salientar ainda que, tal como revelam os gráficos anteriores, mesmo com calendário definido,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

**Gráfico 102 - Equipa de resposta a incidentes de cibersegurança**



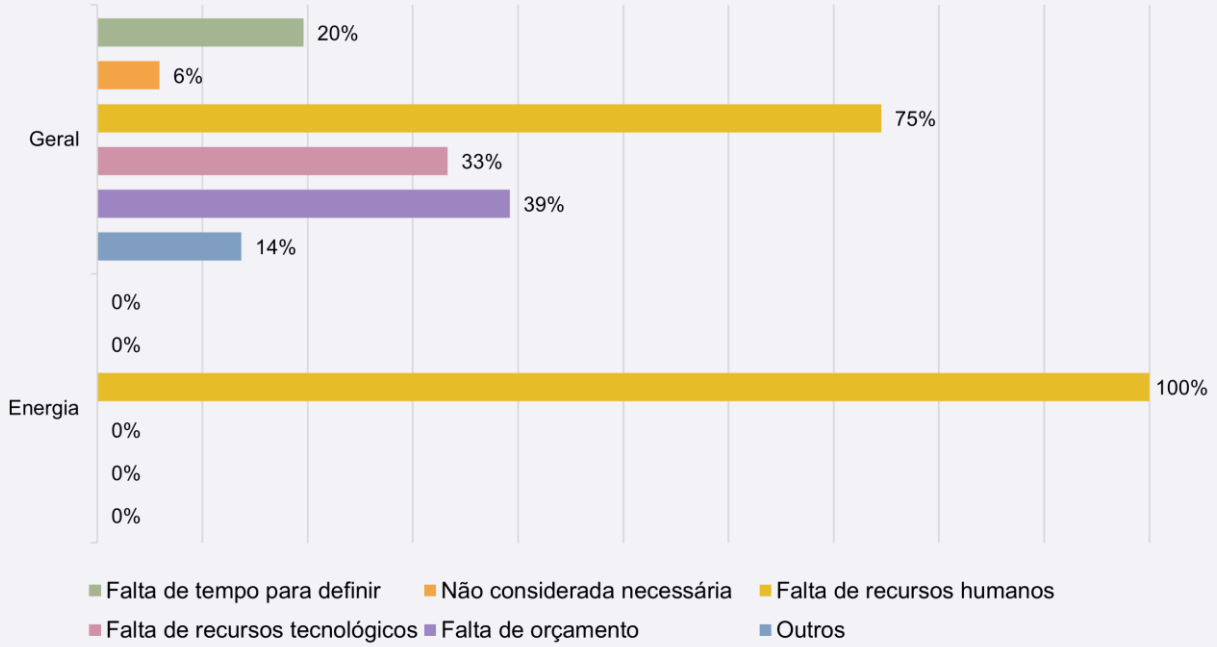

A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. O setor da energia apresenta elevadas percentagens de operadores com equipas de resposta a incidentes, nomeadamente 89%.

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



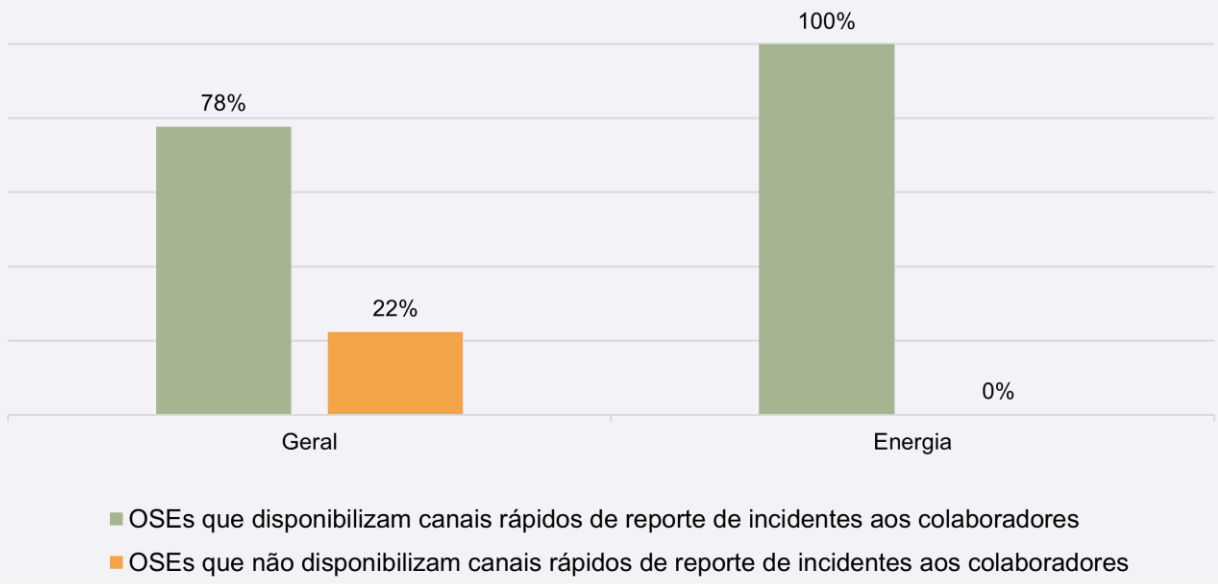

Na visão geral, 55% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, na energia, a composição de equipas de 3 a 5 elementos verifica-se em 50% dos operadores com equipa definida. Ressalva-se ainda que embora equipas com 6 ou mais elementos se verifiquem menos vezes, estas chegam a verificar-se em até 40% dos operadores com equipa de resposta a incidentes, sobretudo quando se atenta a setores como o da energia.
Em resumo, a composição das equipas de resposta a incidentes de cibersegurança tende a ser maioritariamente pequena.

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



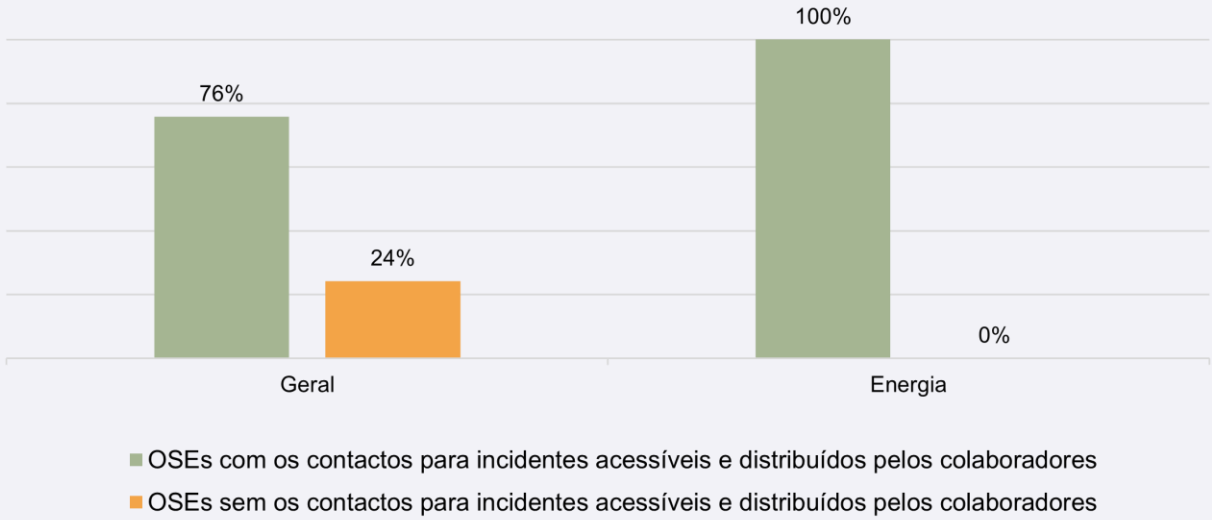

O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. No caso dos operadores do setor da energia, esse é mesmo o único motivo indicado. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores sem equipa de resposta a incidentes. A falta de tempo para definir a equipa surge com menos expressividade, sendo indicada por 20% dos operadores sem equipa. Os operadores que não consideram necessária uma equipa de resposta a incidentes necessária são, no cômputo geral, menos de 10%. Os operadores que selecionaram a opção “outros” (14%) indicaram motivos tais como estar a ser planeada a criação da equipa, a equipa estar a receber formação, ou mesmo o descuido para com a área de cibersegurança.

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



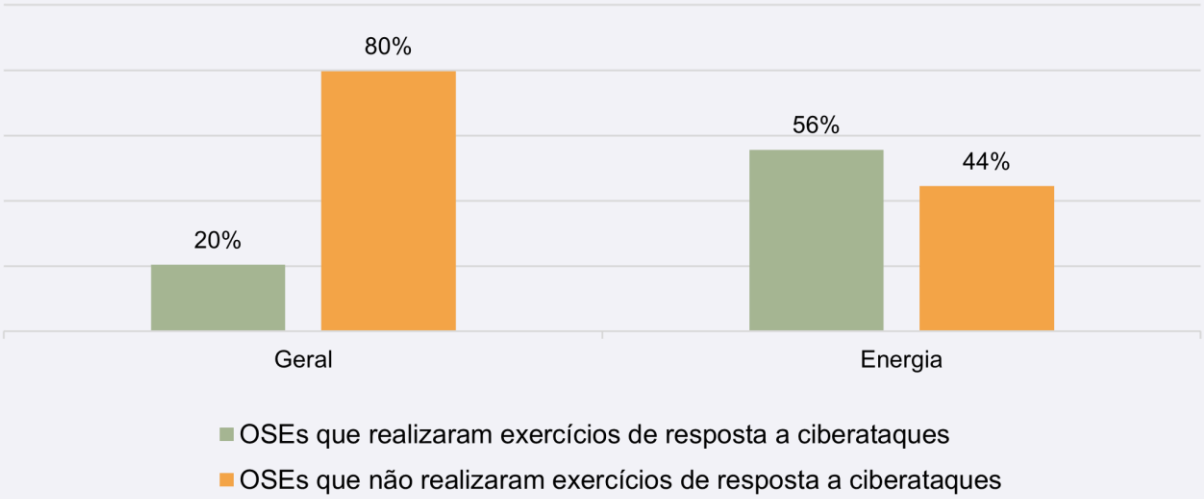

No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. Destaca-se o setor da energia, no qual todos os operadores inquiridos disponibilizam tais canais aos seus colaboradores.

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



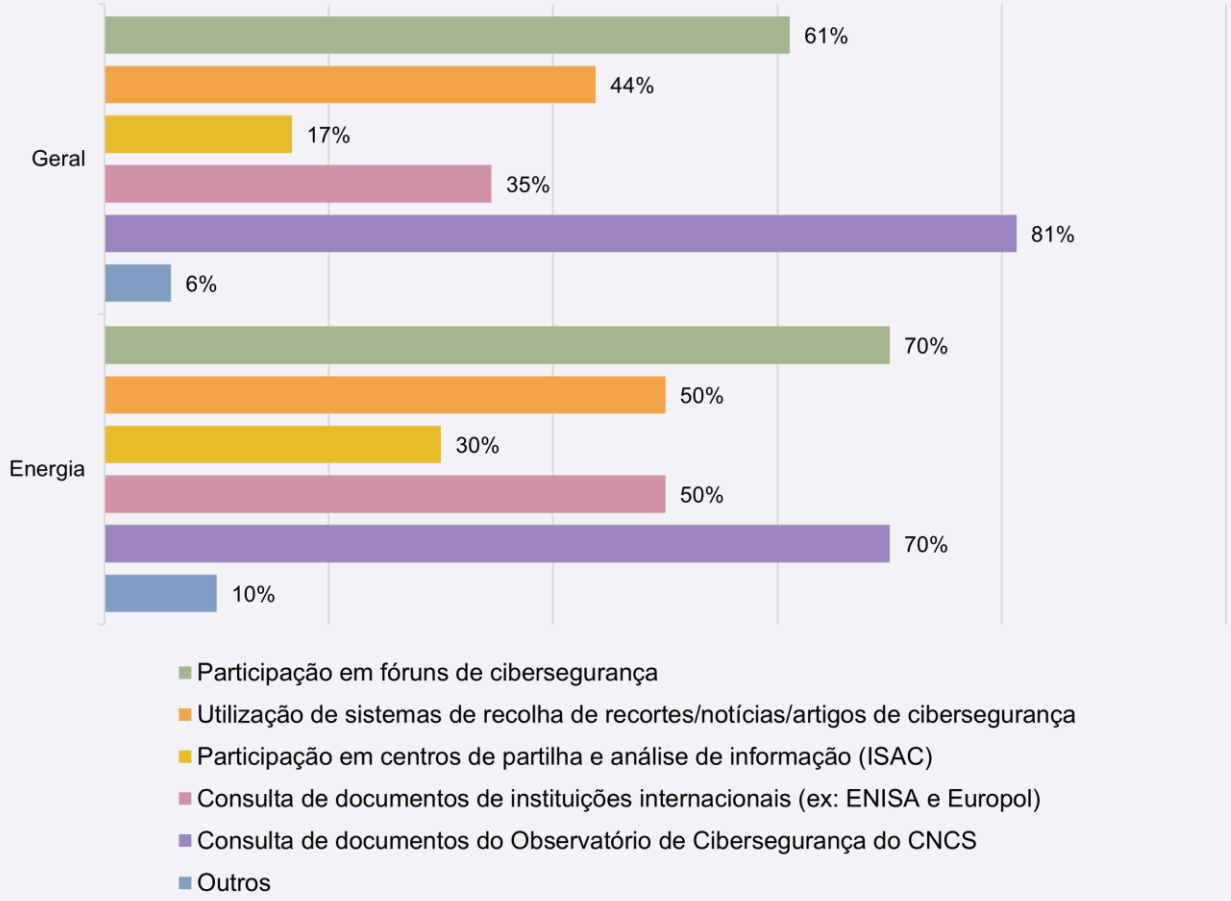

Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. Destaca-se, mais uma vez, o setor da energia, no qual todos os inquiridos responderam positivamente a esta questão.

**Gráfico 107 - Realização de exercícios de resposta a ciberataques**




De acordo com as respostas obtidas, apenas 20% dos operadores inquiridos realizam exercícios de resposta a ciberataques. No setor da energia, 56% dos inquiridos respondeu de forma positiva.

**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[55].

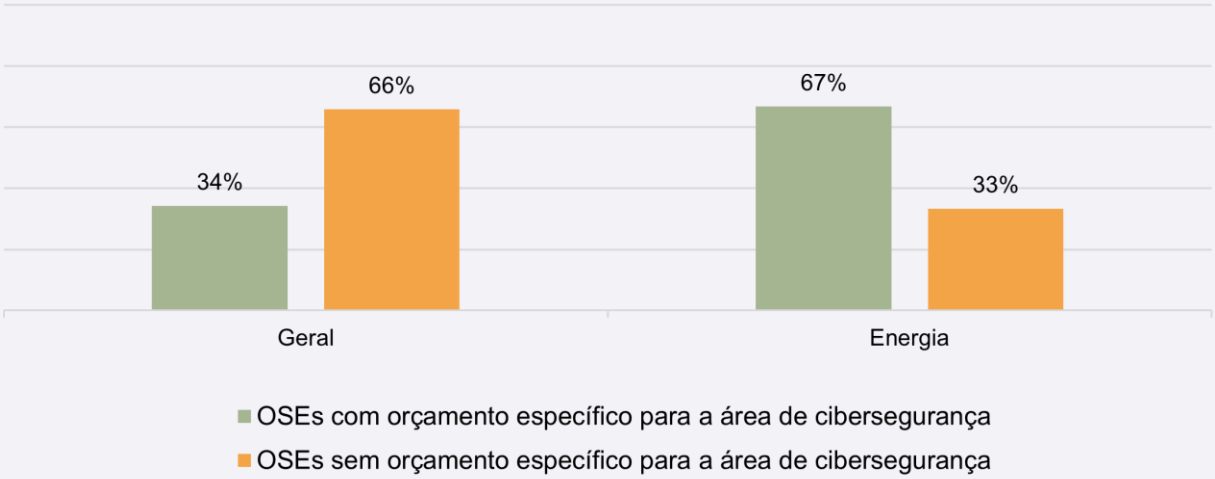
[55] ENISA, "NIS Investments 2023", 59-61.

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"[56]. O próprio CNCS dinamiza seis ISACs, nomeadamente nos seguintes setores: energia, águas, portos marítimos; *media*; retalho e distribuição; e saúde. O CNCS dinamiza também um ISAC regional na Região Autónoma dos Açores. Há ainda um outro ISAC do setor financeiro, do qual o CNCS é membro, mas não promotor[57].

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[58]. A par destes, existem ainda outros ISACs europeus que não são específicos dos setores em análise, mas que se dedicam à recolha e análise de informações no âmbito dos sistemas de controlo industrial (ICS) e dos sistemas de supervisão e aquisição de dados (SCADA), e até mesmo no âmbito das cidades e órgãos de administração pública nelas presentes. Estes ISACs realizam um extenso trabalho de recolha e análise de informação no domínio da cibersegurança, reunindo os contributos de diversas entidades, produzindo, entre vários documentos, guias úteis a diversos níveis, como o da gestão do risco, do tratamento e resposta a incidentes, da gestão de informações sobre ameaças (*threat intelligence management*)[59]. Estes ISACs acabam também por fazer uma importante articulação entre os vários elementos dos diversos setores e a Comissão Europeia, sobretudo quando esta procura obter a análise e os contributos daqueles a quem nova legislação europeia será aplicável[60].

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

**Gráfico 109 - Orçamento específico para a área de cibersegurança**




Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. Contudo, no setor da energia, são mais os operadores que possuem orçamento específico (67%) para essa área do que aqueles que não (33%).

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[61], próximo dos 33% registados pelo CNCS. O mesmo relatório indica que a maioria dos OSE aloca fundos à cibersegurança a partir do orçamento dedicado à parte informática.

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSE a ter orçamentos específicos para cibersegurança. No entanto, um estudo da Comissão Europeia e do Banco Europeu de Investimento (BEI) sobre a criação de uma plataforma de investimento em cibersegurança constatou que as ausências desses orçamentos específicos dificultam grandemente a análise do investimento realizado nesta área. Segundo o mesmo estudo, a própria UE não tinha, no ano de 2022, um orçamento dedicado ao financiamento da sua estratégia de cibersegurança[62]. 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[63]. 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[64].

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

**Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança**

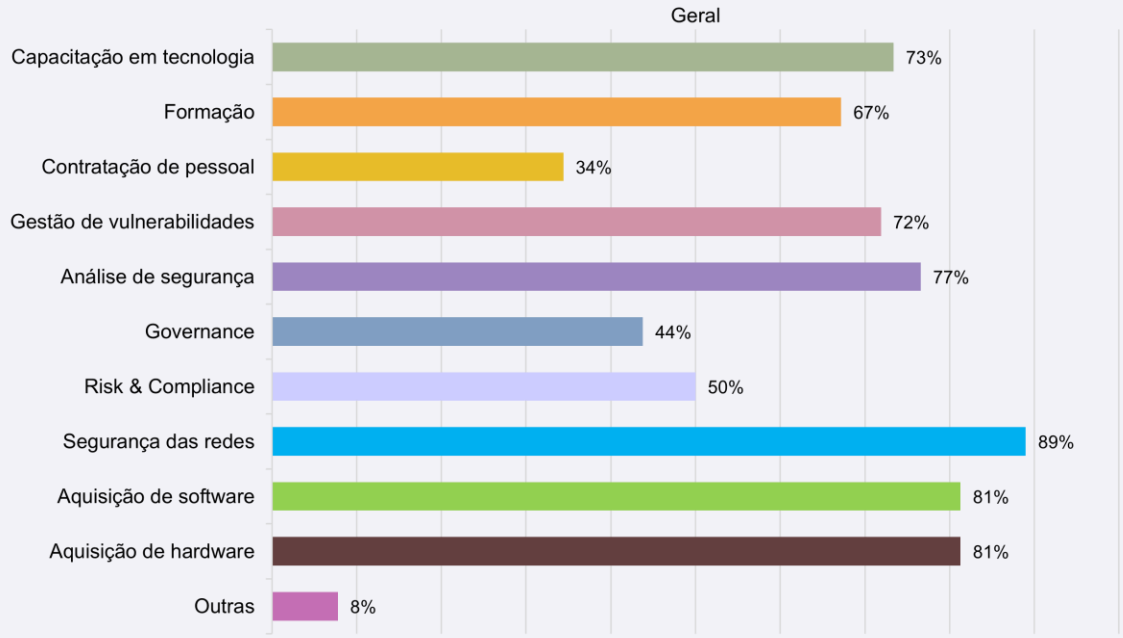
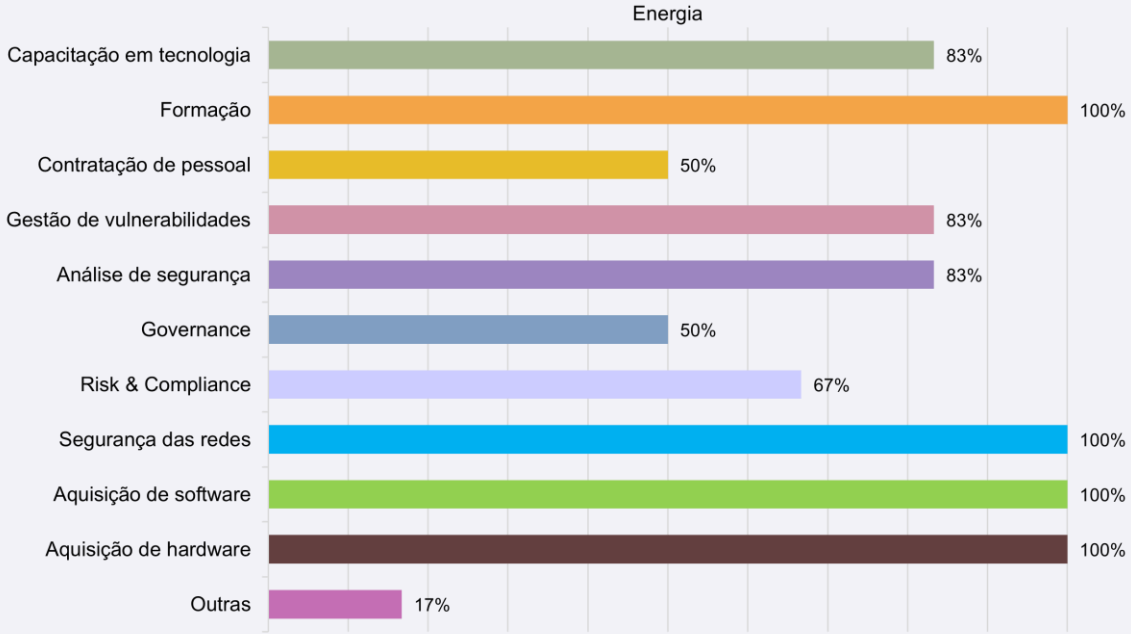



**Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança**




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

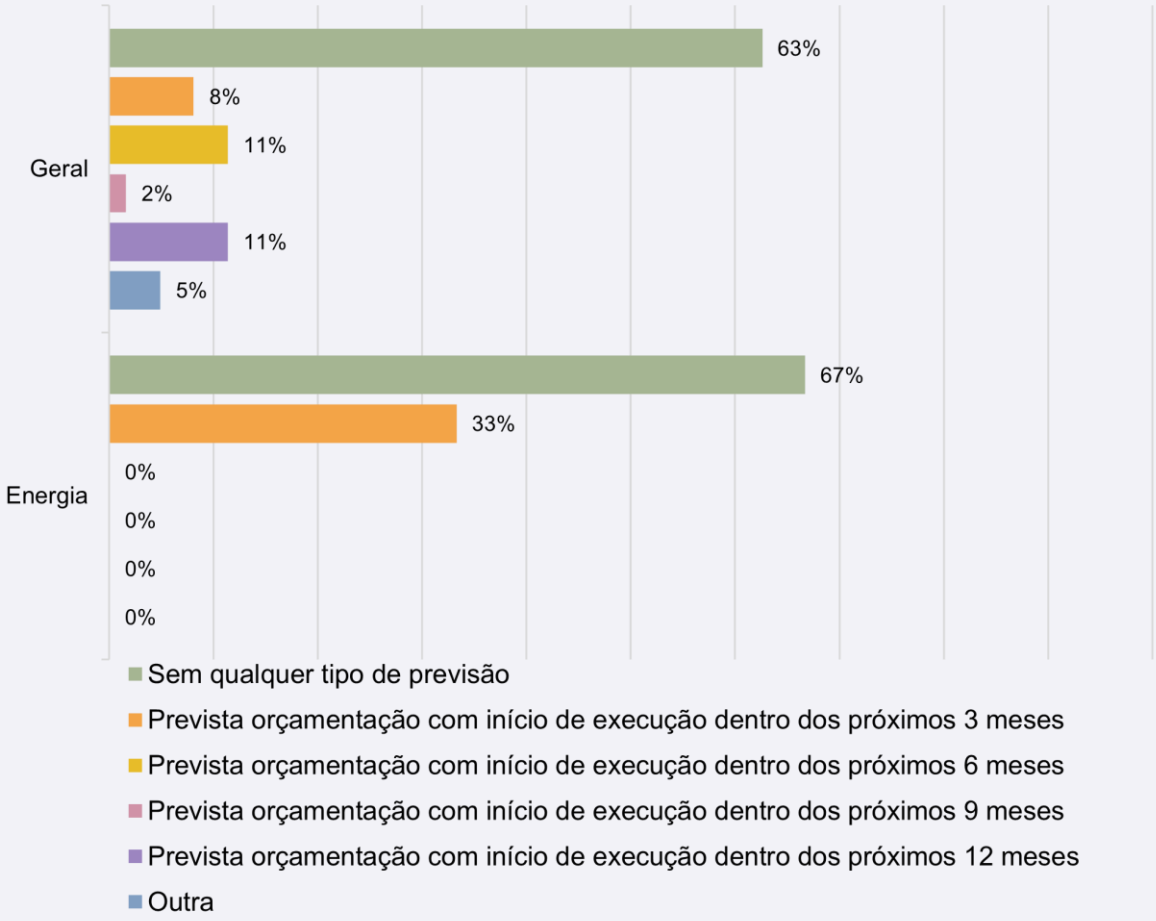
pessoal (34%) e *Governance* (44%). Nas "outras" áreas, surgem sobretudo a contratação de serviços externos para a área de cibersegurança, processos de implementação de normas (*standards*) como a NIST e a aquisição de serviços *cloud*.

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[65]. De acordo com um estudo da NIS de 2023, a média de impacto anual dos incidentes informáticos foi de 365 mil euros e a mediana de 250 mil euros, tendo sido estes dados recolhidos de 38 entidades[66].

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

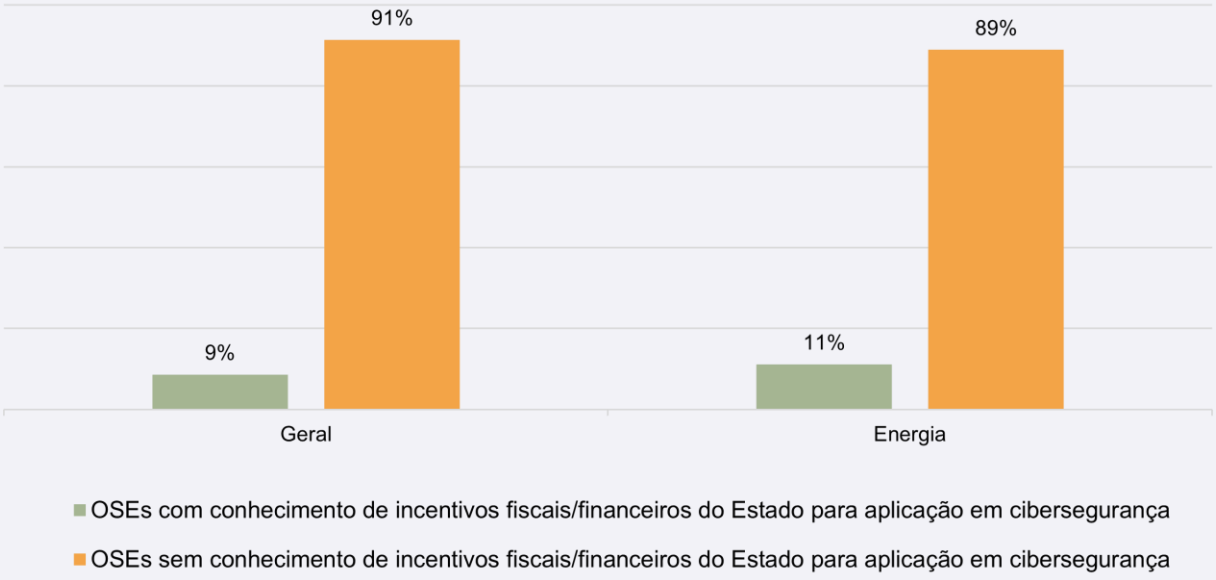
[66] ENISA, "NIS Investments", 2023

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




Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento. Apesar deste panorama, no setor da energia previa-se que um terço dos operadores sem orçamento viria ainda a iniciar a execução de um durante o último trimestre de 2023. Quanto às "outras" respostas, estas corresponderam globalmente a situações em que os orçamentos atribuídos à cibersegurança se incluem ou decalcam dos orçamentos dedicados à área de informática.

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

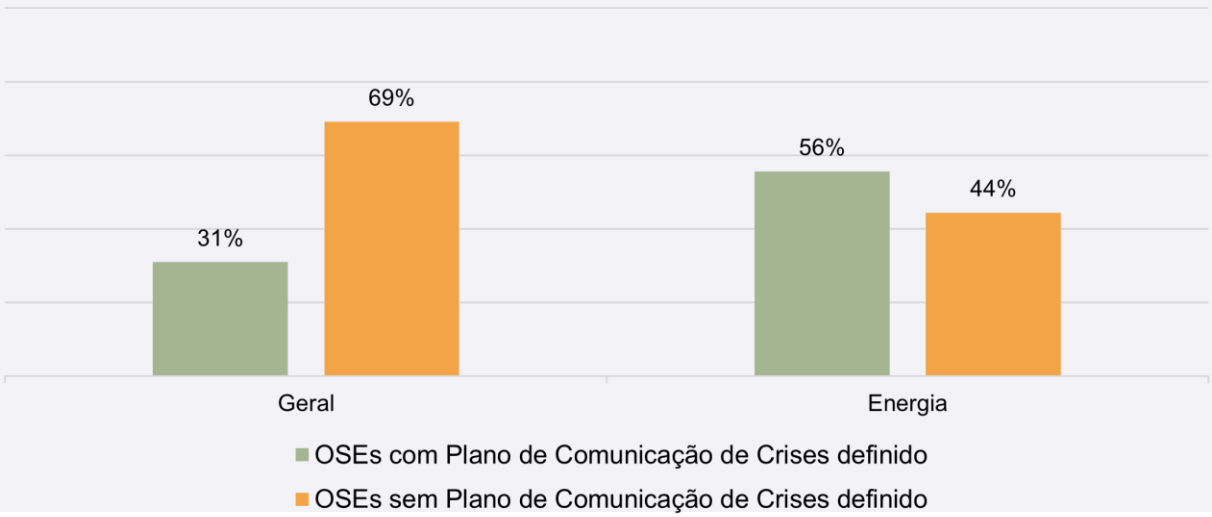



Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No entanto, havia ainda alguns operadores nos setores da energia com conhecimento sobre tais incentivos. A percentagem de operadores com esse conhecimento é de 11%.

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[67].

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

**Gráfico 113 - Plano de Comunicação de Crises**




Muitos dos operadores de serviços essenciais não têm definido um plano de comunicação de crises. Apenas 31% dos inquiridos referiram ter tal plano definido. Há que destacar setores como o da energia onde 56% dos operadores tem plano de comunicação de crises definido.

**Gráfico 114 - Secções definidas no Plano de Comunicação de Crises**

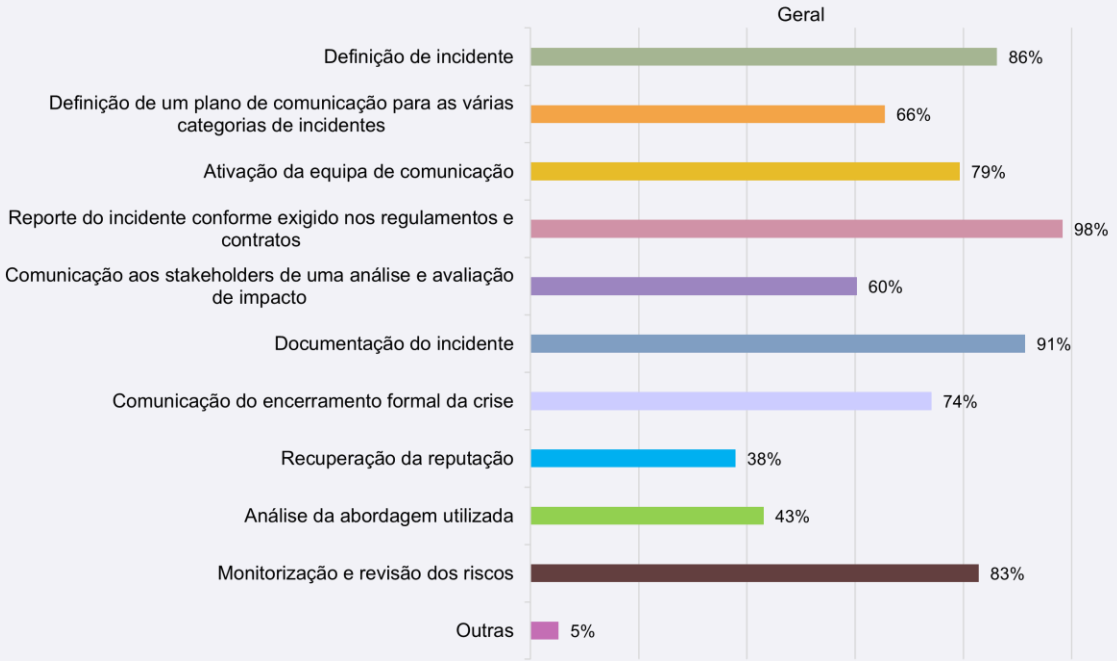
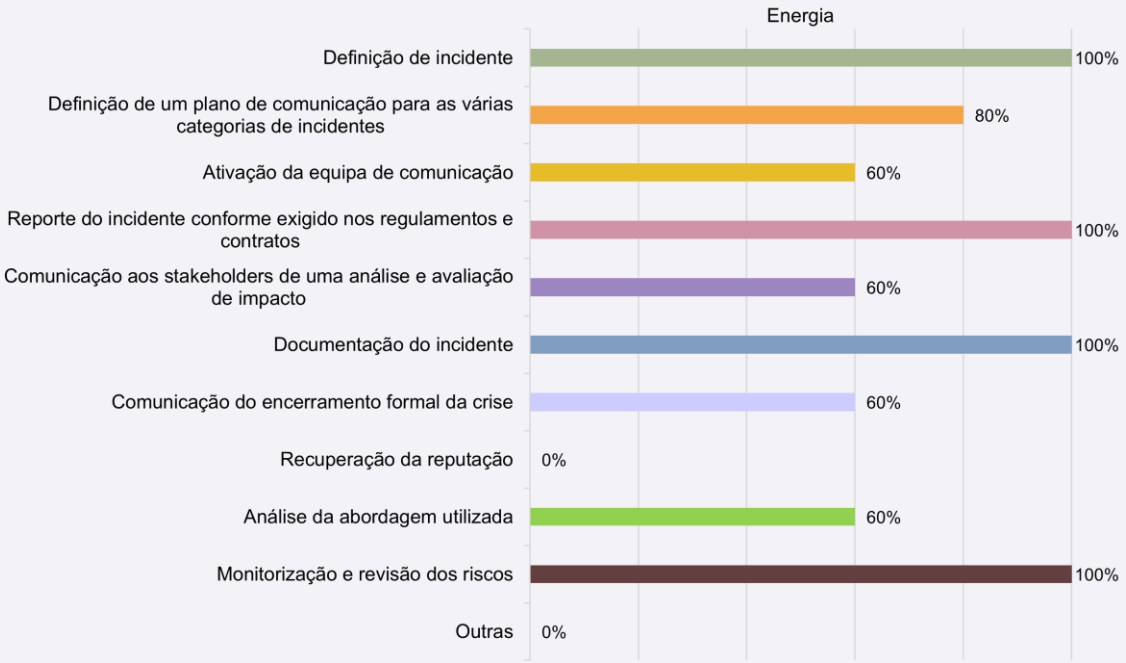


**Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises**

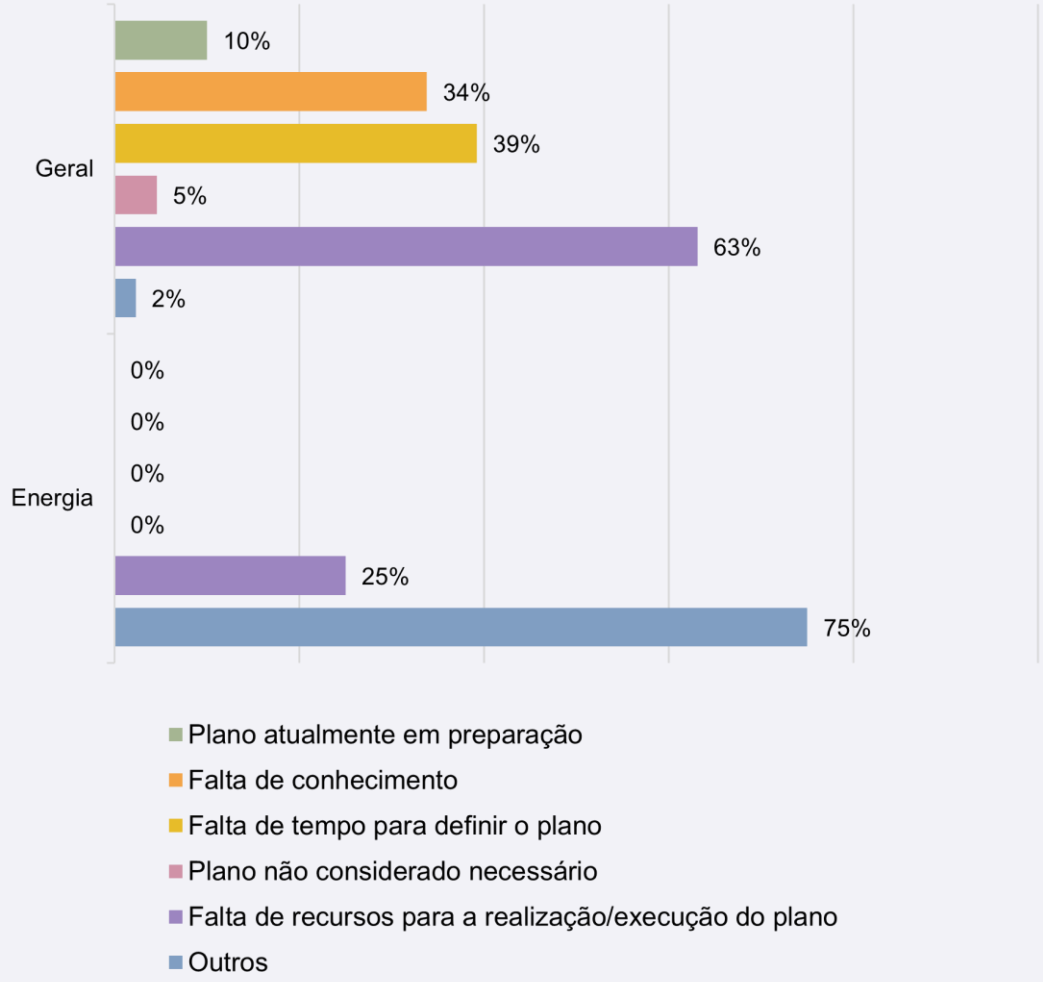



Na análise das secções incluídas nos planos de comunicação de crises, foram incluídas dez secções. Verifica-se que sete destas secções estão incluídas em pelo menos 60% dos planos já definidos. As sete secções mais presentes são a definição de incidente, a definição de um plano de comunicação para várias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

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

A nível setorial, destaca-se o setor da energia, por ser um dos setores onde mais planos incluem as secções elencadas.

**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, mencionado por 75% dos inquiridos do setor da energia.

# Análise Setorial

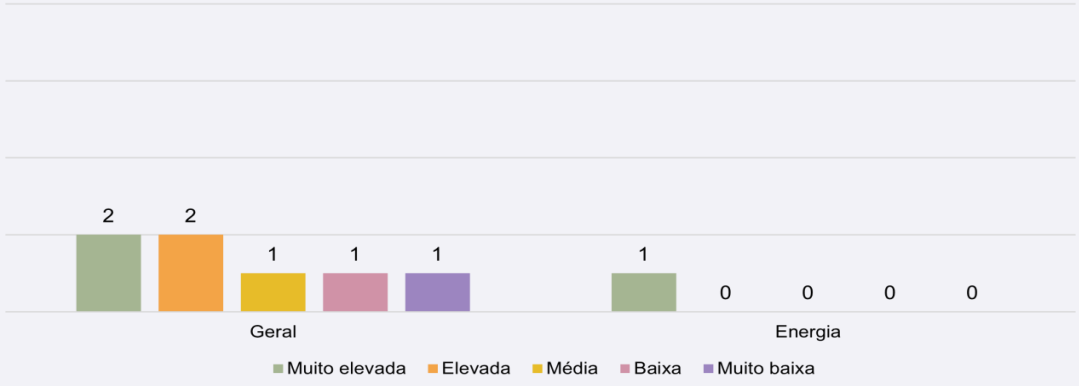
## 1. Energia

### 1.1. Contextualização setorial

No âmbito da Diretiva 2016/1148[68], também conhecida como Diretiva NIS, e Lei n.º 46/2018[69], que transpõe a Diretiva e estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC), o setor da energia abrange três subsetores: o da eletricidade, o do petróleo e o do gás. Embora estas formas de energia sejam conhecidas há mais tempo (por exemplo, há evidências da utilização de petróleo e de gás natural que datam de 4.000 a 6.000 anos a.C.), a sua difusão ocorreria nos finais do século XIX, fruto da Revolução Industrial, substituindo gradualmente o carvão, que era a principal fonte de energia nos vários ramos industriais, bem como no transporte ferroviário.

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

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

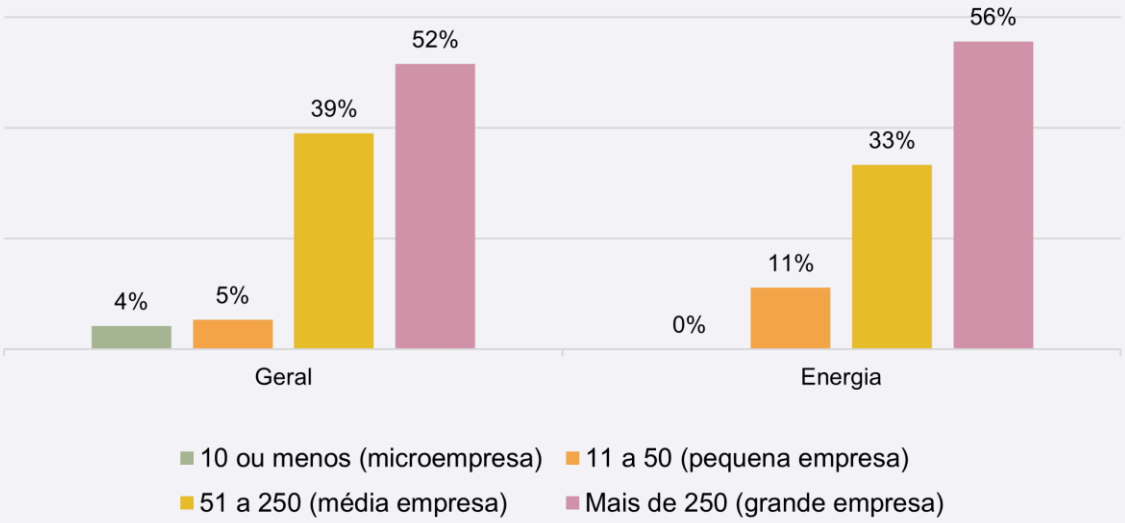



[68] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, Anexo I, *Jornal Oficial da União Europeia*, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.

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

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

**Gráfico 30 - Número de colaboradores na organização**



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

**Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores**

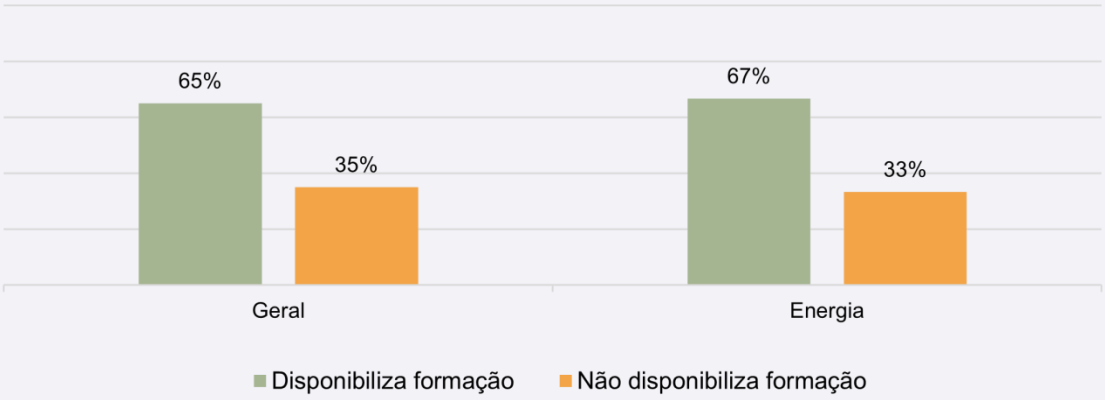
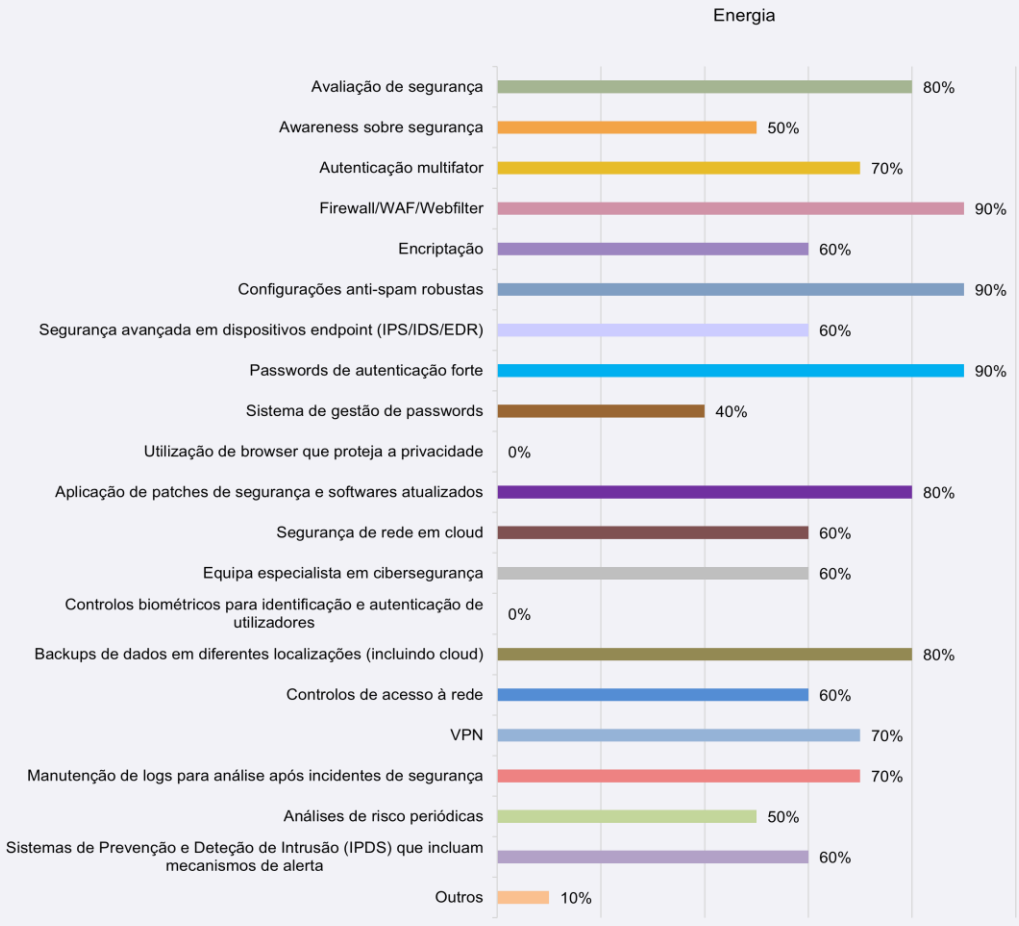
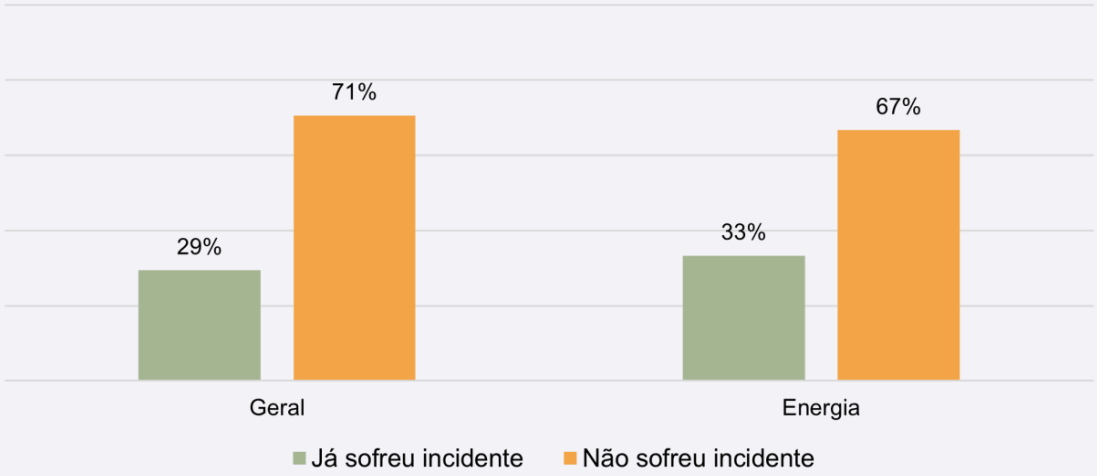



**Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança**



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

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



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

**Gráfico 79.1 - Políticas incluídas no Plano de Segurança**

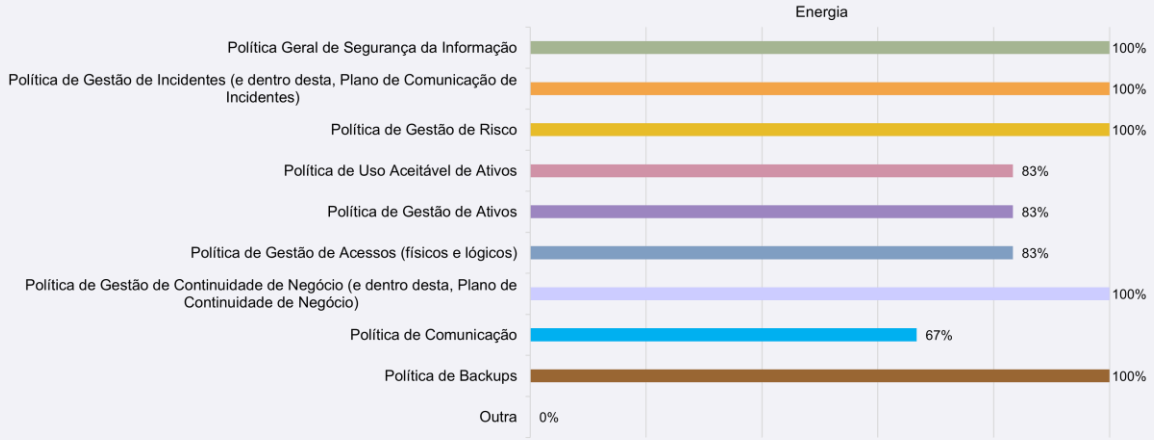
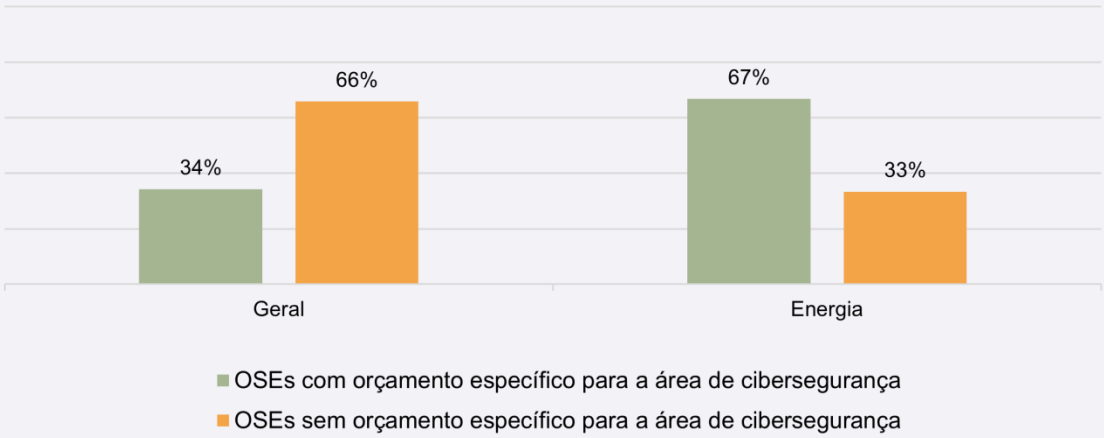



**Gráfico 109 - Orçamento específico para a área de cibersegurança**




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

**Subsetor da Eletricidade**

A história da eletrificação em Portugal iniciou-se em finais do século XIX e ficou marcada por diversos avanços e recuos. O primeiro passo no processo de eletrificação do país iniciou-se com a iluminação pública. A primeira experiência elétrica de que há notícia deu-se a 28 de setembro de 1878, por ocasião do 15.º aniversário do ainda príncipe D. Carlos, no qual se acenderam candeeiros elétricos na esplanada da Cidadela de Cascais[70]. O evento real marcou o início da eletrificação em Portugal. Eram até feitas excursões de famílias a Lisboa para ver os novos candeeiros elétricos, que já não deixavam o cheiro do petróleo pelo ar[71].

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

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

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

Apesar de marcante, o processo de eletrificação foi lento. Foi impulsionado pelo Estado Novo, através da Lei da Eletrificação, publicada em 1944, que estabeleceu como prioridade o desenvolvimento das centrais hidroelétricas. Na década de 50, a construção de barragens era parte integrante do quadro de industrialização do país e, nas regiões onde as barragens eram construídas, eram sinónimo de desenvolvimento económico e social para as populações. Durante a mesma década, o Estado aplicou uma política de apoio económico à eletrificação. Municípios, federações de municípios e concessionários privados podiam recorrer às comparticipações, e através destas foram construídas pequenas centrais térmicas, redes de transporte e distribuição de energia e redes de pequena distribuição rural e urbana[72].

A década seguinte foi a década da consolidação de infraestruturas, da atualização do inventário dos recursos nacionais de produção hídrica e térmica e de definir o seu aproveitamento. Enquanto o processo de eletrificação do país parecia estar próximo da sua conclusão nas zonas urbanas, havia ainda muitas freguesias rurais onde não chegava eletricidade. Assim o Estado teve de alargar os apoios à eletrificação rural de forma a conseguir chegar a estas[73].

No final da década, o Estado determinou a fusão de 14 empresas concessionárias de aproveitamentos hidroelétricos, de empreendimentos termoelétricos e de transporte de energia. Esta concessão unificada foi atribuída à Companhia Portuguesa de Eletricidade, que ficou responsável por 95% da energia elétrica produzida no país e que foi a antecessora da atual Energias de Portugal (EDP), constituída em 1976[74].

[70] EDP, "Uma história de dois séculos: Portugal acende a primeira lâmpada", *Histórias EDP,* 14 de agosto de 2019, https://www.edp.com/pt-pt/historias-edp/uma-historia-de-dois-seculos-portugal-acende-a-primeira-lampada.
[71] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.
[72] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.
[73] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.
[74] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.

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

Ainda assim, a EDP tinha três grandes objetivos: a eletrificação total do território, a melhoria da qualidade dos serviços prestados e a uniformização tarifária[76]. A uniformização tarifária foi o primeiro a ser cumprido, em 1980. A eletrificação total do território foi concluída na década de 90. A melhoria da qualidade dos serviços foi sendo feita à medida que o território era eletrificado e que a capacidade de produção de energia era aumentada. Mais energia produzida significa menos interrupções de serviços e mais circuitos instalados significam mais circuitos alternativos em caso de interrupção no fornecimento de energia[77].

O subsetor da eletricidade tem também sido caracterizado por uma forte aposta na produção de energia elétrica a partir de fontes renováveis. Segundo dados da REN, a produção renovável abasteceu 61% do consumo de energia elétrica em Portugal em 2023, num total de 31,2 TWh, o valor mais elevado de sempre no sistema nacional. A energia eólica abasteceu 25% do consumo em Portugal, a hidroelétrica 23%, a fotovoltaica 7% e a biomassa 6%[78]. Estes valores colocam Portugal entre os países da UE que mais energia elétrica produzem a partir de fontes renováveis, junto da Áustria, Dinamarca, Finlândia e Suécia[79].

### Subsetor do Petróleo

O petróleo tem uma história muito mais longa do que a eletricidade. A utilização do petróleo pelo Homem remonta a 4.000 a.C., época em que povos do Médio Oriente já utilizavam betume na pavimentação de estradas, na calafetação de grandes construções e no aquecimento e na iluminação de casas. No entanto, o petróleo apenas passou a ser considerado valioso em meados do século XIX, com o desenvolvimento de técnicas de destilação na separação de querosene do crude e com a crescente necessidade destes produtos devido à Revolução Industrial. Foram estes produtos refinados que vieram substituir o óleo e o carvão e que ainda hoje abastecem viaturas, aviões, unidades de produção de energia e aquecimento doméstico[80].

Em Portugal, a história da exploração petrolífera remonta ao século XIX, com o início das atividades de pesquisa e exploração datando do ano de 1844, através da concessão relativa à mina de asfalto do "Canto do Azeche", localizada em Nossa Senhora da Vitória, no concelho de Alcobaça[81].

---

[75] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.

[76] EDP, "Uma história de dois séculos", *Histórias EDP,* 14 de agosto de 2019.

[77] Francisco de la Fuente Sanchéz, entrevistado por Jorge Branco em "Eletrificação total do território", ISCTE, 2013, 838.

[78] "Produção de energia renovável bate recorde em 2023", REN, 2 de janeiro de 2024, https://www.ren.pt/pt-pt/media/noticias/producao-de-energia-renovavel-bate-recorde-em-2023.

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

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

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

No entanto, a real evolução do setor só aconteceria já no Estado Novo. Em 1936 foi realizado um concurso público para a concessão de uma área destinada à pesquisa de hidrocarbonetos em regime de exclusividade. O alvará de concessão n.º 2138 foi concedido a dois cidadãos ingleses, conforme aprovado pelo Decreto 28575, de 7 de abril de 1938. Estes cidadãos ingleses viriam a transmitir os direitos e obrigações à empresa *Anglo Portuguese Oil Company Ltd*., que desenvolveu a atividade até 1941, sendo interrompida pela segunda guerra mundial[82].

Esta primeira fase incidiu na região de Torres Vedras, havendo duas sondagens com indícios de petróleo. No entanto, na época, a falta de recursos adequados impediu a realização de testes de produção. Uma segunda fase de pesquisa ocorreu entre 1946 e 1969, durante a qual foram encontrados sinais promissores de petróleo e gás. Contudo, os testes de produção realizados demonstraram que as quantidades não eram viáveis para a comercialização[83].

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

Apesar da presença de companhias estrangeiras no mercado português, este era de pequena dimensão na escala europeia. Em 1938, o consumo total nacional rondava as 200 mil toneladas por ano, enquanto em Itália este rondava os 2 milhões de toneladas e em França os 6 milhões. Tal correspondia a um consumo por habitante em Portugal a cerca de 60% do consumo médio de um habitante italiano e a 20% do consumo médio de um habitante francês[85].

Ainda assim, o mercado do petróleo foi crescendo gradualmente em Portugal, e, à medida que iam surgindo novas necessidades de consumo, surgiam também novas necessidades de produção. As medidas protecionistas do Estado Novo foram também limitando a entrada de outros intervenientes no mercado, pelo que o mercado petrolífero se encontrava essencialmente nas mãos de quatro grandes operadores em meados da década de 70. Eram estes a Sacor, a Sonap, a Cidla e a Petrosul. Com a Revolução de Abril, estas viriam depois a ser nacionalizadas (1975) e a constituir a Petrogal em 1976[86], que adotaria no mesmo ano o nome comercial Galp[87].

Atualmente, a Galp continua a ser uma das maiores empresas petrolíferas do país, controlando cerca de 50% do comércio de combustíveis e a totalidade da capacidade refinadora de Portugal[88].

---

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

[83] Direção-Geral de Energia e Geologia, "História da Prospeção e Pesquisa".

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

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

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

[87] "As nossas raízes: cronologia ilustrada", Galp, https://www.galp.com/corp/pt/sobre-nos/a-galp/as-nossas-raizes.

[88] "Cotação Galp Energia", Rankia, https://www.rankia.pt/cotacoe/galp-energia/.

**Subsetor do Gás**

O gás natural foi descoberto na Pérsia entre 6000 a.C. e 2000 a.C., na China, é conhecido desde 900 a.C., mas o conhecimento da primeira utilização do gás natural data de 347 a.C., com um manuscrito desse período a descrever um "ar de fogo" que podia ser usado para iluminação[89].

Na Europa, o gás natural foi descoberto no século XVII, embora não tenha despertado grande interesse. O gás de iluminação pública na Europa era produzido a partir do carvão. Em 1778, Alessandro Volta descobriu o potencial energético do gás natural quando verificou que o gás capturado nas bolhas emergentes da água, no lago Maggiore, ardia com uma chama azulada. Volta ficaria conhecido por ter sido quem isolou pela primeira vez o gás metano[90]. Os gases butano e propano (aqueles que se veem comercializados em botijas) viriam a ser obtidos com o desenvolvimento das técnicas de destilação e refinação do petróleo desenvolvidas a partir de meados do século XIX, bem como através da captura de gases durante o processo de extração do gás natural[91].

Em 1807 são acesos, pela primeira vez no mundo, candeeiros a gás na Rua Pall Mall em Londes. Por sua vez, em 1846, é atribuída uma concessão de iluminação pública de Lisboa à CLIG e, esta, arranca com o sistema de gás iluminante[92]. Em 1857 surgia o primeiro fogão a gás e, em 1885, com a invenção do bico de Bunsen, que permitia a queima segura de gás natural sem que esta se propagasse pelo tubo, foram compreendidas as vantagens deste gás como fonte de energia para o aquecimento ambiente, aquecimento de água e utilização na cozinha[93]. No ano de 1899 a rede de gás canalizado estende-se até Cascais, Oeiras e Sintra. É inaugurada, em 1944, a fábrica de gás da Matinha, em Lisboa, com uma capacidade de produção diárias de 75 000 $m^3$ e dez anos depois é iniciada a produção de Gases de Petróleo Liquefeito (GPL)[94].

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

Em 2000 são iniciados os trabalhos de preparação do terreno para as obras de implantação do terminal de Gás Natural Líquido (GNL) em Sines e dois anos depois é iniciada a construção do gasoduto entre Setúbal e Sines. No ano de 2012 ocorrem as obras de ampliação do Terminal de GNL de Sines[96].

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

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

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

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

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

94 Fundação Galp Energia, "Gás A História Natural", 4.

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

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

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

Embora as principais linhas de distribuição de gás natural se estendam atualmente por praticamente todo o país, o gás natural não chega a todos. Um estudo da Marktest, quantificava, em 2018, que o número de indivíduos em Portugal com gás canalizado em casa era aproximadamente 3,9 milhões, o que corresponderia a cerca 45,3% dos residentes com 15 ou mais anos no continente[98].

### 1.1.1. Impacto socioeconómico

O setor energético exerce um papel fundamental na economia e na sociedade. É este setor que permite, nas casas e empresas, que as luzes, os eletrodomésticos, as máquinas, grandes e pequenas, e os transportes, privados ou públicos, funcionem. É um dos setores essenciais que mais dependências provoca nos restantes - sem energia, todos os outros ficam comprometidos. A maior dependência energética verifica-se nos setores dos transportes, da indústria, da agricultura e da pecuária que, segundo o Banco de Portugal (BdP), são os que mais intensamente consomem energia no país[99].

É também um setor que move muitos milhões de euros. Para que se tenha uma ideia, o volume de negócios (VVN) da maior empresa do subsetor da eletricidade em 2022 foi de, pelo menos, 12,7 mil milhões de euros. Somando os volumes de negócio das principais empresas dos setores do petróleo (14,9 mil milhões) e do gás (4,5 mil milhões), ultrapassam-se os 32 mil milhões de euros, o que corresponde a quase 13% do PIB português em 2022[100].

[97] ERSE, “Caracterização do Sector do Gás”, 5.

[98] “Gás canalizado: penetração aumenta mas não chega à maioria da população”, Marktest, 11 de dezembro de 2018, https://www.marktest.com/wap/a/n/id~2470.aspx.

[99] Banco de Portugal, “Economia numa imagem”, março de 2022, https://www.bportugal.pt/page/economia-numa-imagem-148-0.

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

Concomitantemente, é um setor gerador de empregos. Segundo dados da PORDATA, os setores da eletricidade, gás e água empregavam, em 2023, 56,9 mil colaboradores[101]. No subsetor do petróleo, estima-se que haja também cerca de 53 mil colaboradores[102]. Retirando os quase 10 mil colaboradores que trabalham no setor da água, o setor energético será responsável por cerca de 100 mil empregos em Portugal. Além dos 100 mil empregos já criados, a aposta nas energias renováveis poderá vir a triplicar este número, uma vez que se estima que as energias renováveis irão gerar mais 95 mil postos de trabalho diretos e outros 95 mil indiretos[103]. Se tal se confirmar, o setor será responsável por cerca de 293 mil postos de trabalho em Portugal.

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

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

A pobreza energética não é um problema exclusivamente português, mas Portugal figura entre os países da UE com índice de pobreza energética mais elevado, estando apenas melhor do que a Eslováquia, a Hungria e a Bulgária[105]. Estima-se que entre 1,8 e 3 milhões de pessoas em Portugal se encontrem nesta situação, das quais 660 mil se encontrem em pobreza energética severa[106].

Uma consequência direta da pobreza energética é a falta de conforto térmico, que pode ser compreendida como a capacidade de manter a temperatura de uma habitação nos intervalos entre os 18.º C e os 21.º C, no inverno, e os 19.º C e os 23.º C[107], no verão, é sobretudo atribuída a dois motivos. O primeiro é algo que persiste na maioria das habitações em Portugal, onde se estima que cerca de 75% não possuem condições de isolamento térmico.

---

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

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

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

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

[105] "Pobreza Energética em Portugal" *Histórias EDP*, EDP, 16 de março de 2021, https://www.edp.com/pt-pt/historias-edp/pobreza-energetica-em-portugal.

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

[107] "Pobreza Energética em Portugal", EDP, 23 de novembro de 2023.

O segundo motivo é o preço da energia. Embora os preços da energia em Portugal se mantenham mais ou menos em linha com os praticados na União[108], importa sublinhar que o salário médio em Portugal está abaixo do da média europeia. O salário médio português ocupa a 17.ª posição dos salários médios da Europa a 27[109].

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

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

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

- Promover a sustentabilidade energética e ambiental da habitação;
- Promover o acesso universal a serviços energéticos essenciais;
- Promover a ação territorial integrada;
- Promover o conhecimento e a atuação informada[113].

As medidas previstas passam pelo Vale Eficiência, a Tarifa Social de Energia, a redução dos custos do acesso à rede, o acesso ao mercado regulado, a aplicação de benefícios fiscais, como a aplicação da taxa reduzida do IVA à componente fixa das tarifas de acesso às redes nos fornecimentos de eletricidade e nos fornecimentos de gás natural, mediante o consumo, e a aplicação da taxa reduzida de IVA à entrega e instalação de painéis solares térmicos e fotovoltaicos, bem como por programas de apoio à melhoria das condições do conforto térmico das habitações, quer estas passem por intervenções nas mesmas ou pela aquisição de equipamentos e soluções energeticamente eficientes[114].

---

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

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

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

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

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

[113] DGEG, "Estratégia de Longo Prazo de Combate à Pobreza Energética".

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

As principais metas da ELPPE são:

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

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

De forma resumida, a temperatura global do planeta tem vindo a aumentar e está a prejudicar todas as formas de vida terrestre, sejam animais ou plantas. As temperaturas elevadas são responsáveis por fenómenos climáticos acentuados e são várias as zonas do globo que sofrem com secas extremas ou com inundações e tempestades. Regiões que, até meados do século XIX, nunca tinham passado por estas situações[116].

Quando se começou a estudar a razão destas alterações, a opinião científica foi unânime: todos apontaram como causa a emissão de gases de efeito de estufa, sendo o principal responsável o dióxido de carbono ($CO_2$). E estes, por sua vez, são emitidos através da queima de combustíveis fósseis: o petróleo, o carvão e o gás[117].

O grande objetivo estabelecido com o Acordo de Paris em 2015, de momento, é fazer com que a temperatura média do planeta não ultrapasse em mais de 1,5ºC a temperatura média dos anos pré-revolução industrial até 2030 e atingir a neutralidade carbónica até 2050[118]. Para tal, é necessário reduzir as emissões de gases com efeito de estufa, como o $CO_2$. Essa redução passa, em grande parte, pela transição energética, ou seja, pela transição da utilização e queima de combustíveis fósseis, para energia produzida a partir de fontes renováveis e limpas, como a hídrica, a eólica, a solar e o hidrogénio.

Portugal e a UE pretendem, até 2030, reduzir as emissões de gases com efeito estufa em entre 45% e 55%, atingir uma produção energética onde 47% dessa energia provenha de fontes renováveis e ter pelo menos 20% dos transportes alimentados também por fontes renováveis[119].

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

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

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

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

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

O desafio é grande, uma vez que cerca de 70% da energia consumida na Europa e em Portugal ainda depende dos combustíveis fósseis[120]. Essa dependência não se deve tanto à produção de energia elétrica, que em Portugal já provém de fontes renováveis em mais de 60%, mas deve-se muito ao consumo de combustíveis fósseis nos transportes rodoviários, na indústria e nos transportes aéreos[121].

Contudo, esperam-se impactos positivos e muito significativos com a prossecução dos objetivos para a transição energética. Para além de se limitarem os fenómenos naturais graves que decorrem das alterações climáticas, como as secas, tempestades e outros, melhorar-se-á também a qualidade do ar, impactando positivamente a saúde das pessoas, e estima-se que a transição energética se possa também tornar um motor do crescimento económico, criando cerca de 3,5 milhões na UE até 2030[122], podendo ascender aos 8 milhões de empregos criados na UE até 2050 se se cumprirem todos os objetivos estabelecidos no Acordo de Paris até esse ano[123].

**Subsetor da Eletricidade**

Em 2023, do total de energia consumida, 880 toneladas equivalente de petróleo (tep) foram geradas a partir de eletricidade[124]. No ano anterior, o consumo total atingiu 49 385 044 097 kWh, distribuídos da seguinte forma: 13 857 147 276 kWh no uso doméstico, 12 002 356 981 kWh de uso não doméstico, 19 675 607 910 kWh na indústria, 998 563 917 kWh na agricultura, 1 030 333 394 kWh na iluminação das vias públicas, 1 376 131 397 kWh nos edifícios do estado e 444 903 221 kWh noutras aplicações[125].

Foram gerados aproximadamente 49 043 GWh a partir de fontes renováveis em 2023[126], representando 75,8% da produção total de energia elétrica[127]. No mesmo ano, a produção bruta de energia elétrica alcançou 49 043 GWh, sendo composta por 13 145 GWh foi energia eólica, 208 GWh de energia geotérmica, 14 868 GWh de energia hídrica, 15 662 GWh de energia térmica e 5 160 GWh de energia fotovoltaica[128].

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

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

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

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

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

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

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

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

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

### Subsetor do Petróleo

Em 2021, as famílias portuguesas consumiram aproximadamente 50 345 Terajoule (TJ) de gasóleo e 33 001 TJ de gasolina[129]. Em 2023, do total da energia consumida, 8 542 tep foram derivadas do petróleo[130]. De acordo com dados do INE, em 2022 foram vendidas cerca de 994 577 toneladas (t) de gasolina sem chumbo 95, 78 612 t de gasolina sem chumbo 98, 4 455 058 t de gasóleo rodoviário, 316 590 t de Gasóleo colorido, 71 548 t de Gasóleo para aquecimento, 344 995 t de *fuel*, 218 373 t de coque de petróleo e de 342 t de outros produtos de petróleo[131]. O preço médio do litro de gasolina sem chumbo 95 foi de 1,73 €/L, a gasolina sem chumbo 98 teve o preço médio de 1,92 €/L, o gasóleo rodoviário custou 1,60 €/L e o *fuel* 1,06 €/L[132].

Em relação à importação de petróleo e derivados, a maior parte foi proveniente do Brasil, com aproximadamente 4 053 300 Nm3. Em seguida, foi importado de Espanha 2 162 915 Nm3. A Argélia e a Nigéria aparecem a seguir com 1 351 847 Nm3 e 1 207 800, respetivamente. Por fim, encontram-se o Azerbaijão com 769 597 Nm3, a Angola com 387 725 Nm3 e o Reino Unido com 58 223 Nm3, totalizando 13 260 549 Nm3[133].

### Subsetor do Gás

De acordo com os dados divulgados pelo INE, em 2021, as famílias portuguesas consumiram cerca de 12 005 TJ de energia em gás natural e 15 354 TJ de GPL[134]. Em 2023, aproximadamente 3 815 de tep consumidas em Portugal vinham do gás natural[135]. No ano anterior, segundo dados do INE, foram vendidas cerca de 222 406 toneladas (t) de gás butano, 546 678 t de gás propano e de 35 664 t de GPL[136], tendo a garrafa de gás butano chegado aos 2,40 €/kg, o propano em garrafa teve o preço médio de 2,79 €/kg e o propano canalizado foi de 2,84 €/kg[137].

Relativamente à importação de gás natural, a maior parte do gás foi importado à Nigéria, com cerca de 1 784 873 Nm3, logo de seguida encontra-se os EUA onde foi importado 1 695 801 Nm3 e por último encontra-se a Rússia com 373 739 Nm3, totalizando 4 075 560 Nm3[138].

[129] PORDATA, "Consumo energético das famílias: total e por alguns produtos energéticos", maio de 2024, https://www.pordata.pt/sites/default/files/202406/Portugal_Consumo_energetico_das_familias__total_e_por_alguns_produtos_energeticos.xlsx.
[130] PORDATA, "Consumo de energia primária: total e por tipo de fonte de energia", maio de 2024.
[131] PORDATA, "Venda de combustíveis para consumo", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Venda_de_combustiveis_para_consumo.xlsx.
[132] PORDATA, "Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente", maio de 2024, https://www.pordata.pt/sites/default/files/2024-06/Portugal_Precos_medios_de_venda_ao_publico_dos_combustiveis_liquidos_e_gasosos_-_Continente.xlsx.
[133] PORDATA, "Importações de energia: total e por principais países de origem", outubro de 2024, https://www.pordata.pt/sites/default/files/2024-10/Portugal_Importacoes-de-energia-por-principais-paises-de-origem.xlsx.
[134] PORDATA, "Consumo energético das famílias: total e por alguns produtos energéticos", maio de 2024.
[135] PORDATA, "Consumo de energia primária: total e por tipo de fonte de energia", maio de 2024.
[136] PORDATA, "Venda de combustíveis para consumo", maio de 2024.
[137] PORDATA, "Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente", maio de 2024.
[138] PORDATA, "Importações de energia: total e por principais países de origem", outubro de 2024.

Atualmente, o gás natural possui diversas aplicações, incluindo os setores da mobilidade, terciário, indústria e uso doméstico[139]. Cada uma destas utilizações oferece vantagens em comparação com outros tipos de combustíveis, tais como:

- **Setor da mobilidade**: O Gás Natural Veicular (GNV) e o Gás Natural Comprimido (GNC) oferecem uma redução de aproximadamente 20% nas emissões de CO2 em comparação com a gasolina e até 25% em relação ao gasóleo. Além disso, são mais baratos, exigem menos manutenção, são menos inflamáveis e emitem menos odor em comparação com os veículos com motores movidos a combustíveis tradicionais[140];
- **Setor terciário**: O preço é mais competitivo em comparação aos outros combustíveis, tem uma elevada eficiência, existe um fornecimento contínuo sem necessidade de armazenamento e tem uma elevada compatibilidade com equipamentos de *catering* e climatização[141];
- **Indústria**: O gás não produz cinzas nem outros resíduos sólidos, não necessita de estar armazenado nem de ser abastecido, tem um fornecimento contínuo e tem uma vasta cobertura nacional[142];
- **Utilização doméstica**: É mais sustentável em comparação com os restantes combustíveis fósseis, tem uma queima mais limpa reduzindo assim os custos de manutenção nos equipamentos e não tem necessidade de armazenamento[143].

### 1.1.2. Especificidades tecnológicas

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

A TO refere-se ao uso de *hardware* e *software* para monitorizar e controlar infraestruturas, processos e dispositivos físicos. A TO é principalmente composta por sistemas que desempenham múltiplas tarefas, desde funções de monitorização às de controlo de máquinas industriais. Por sua vez, estes sistemas são normalmente designados como Sistemas de Controlo Industrial, e incluem diversos dispositivos (ex: sensores de deteção de perda de água), sistemas e controlos e redes dos quais dependem múltiplos aspetos da gestão industrial. Os sistemas mais comuns são os SCADA, sistemas que recolhem dados de diversos locais e os enviam para o seu destino de tratamento[144].

O sistema de controlo SCADA é fundamental nas redes de transmissão e distribuição no setor da energia, sendo utilizado para monitorizar instalações em tempo real e controlar remotamente as operações das centrais. Estes sistemas permitem a recolha contínua de dados críticos, como a voltagem, corrente e frequência, possibilitando uma resposta rápida e eficiente a falhas ou interrupções, o que garante uma maior confiabilidade e segurança[145].

---

[139] Associação Portuguesa de Empresas de Gás, "Utilizações e Vantagens", https://www.apeg.pt/gas-natural/utilizacoes-vantagens/.
[140] Associação Portuguesa de Empresas de Gás, "Utilização no setor da mobilidade", https://www.apeg.pt/gas-natural/utilizacao-no-setor-da-mobilidade/.
[141] Associação Portuguesa de Empresas de Gás, "Utilização no Terciário", https://www.apeg.pt/gas-natural/setor-terciario/.
[142] Associação Portuguesa de Empresas de Gás, "Utilização na Indústria", https://www.apeg.pt/gas-natural/industria/.
[143] Associação Portuguesa de Empresas de Gás, "Utilização Doméstica", https://www.apeg.pt/gas-natural/utilizacao-domestica/.
[144] Fortinet, "What is OT Security?" https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security.
[145] SCADA INFO, "SCADA and Energy Management System", https://www.scadainfo.com/scada-and-energy-management-system/.

Os *PLCs* (*Programmable Logic Controller*) são fundamentais na gestão dos dispositivos nas subestações, como disjuntores, transformadores e sistemas de proteção. Graças à sua robusteza e uma rápida capacidade de resposta, os *PLCs* desempenham um papel crucial nas operações de controlo, assegurando a eficiência e confiabilidade nos processos essenciais para o funcionamento seguro e contínuo de todos os sistemas[146].

Um *Distributed Control System* (*DCS*), possibilita o controlo dos processos em múltiplas áreas, garantindo uma operação integrada e segura. No subsetor do petróleo, por exemplo, este sistema assegura que as condições críticas, como a pressão e a temperatura, permanecem dentro dos parâmetros de segurança, contribuindo para a eficiência e confiabilidade das operações[147].

**Subsetor da Eletricidade**

No setor da eletricidade em Portugal, algumas destas tecnologias incluem, por exemplo, na parte de produção, dispositivos de telemetria para medir os caudais, o fluxo de água nas barragens e detetar fugas[148], e para medir os ventos e fazer análises preditivas relativas aos parques eólicos. Já na parte da distribuição, acrescem os sistemas de gestão das reservas estratégicas de energia, sistemas de monitorização de incêndios perto de redes elétricas, que despoletam o envio de uma equipa ao terreno para avaliar/prevenir danos nos ativos e na população, sistemas de deteção de interrupção do fornecimento de energia elétrica, alimentados por algoritmos que auxiliam na deteção de falhas na infraestrutura de distribuição e sistemas dedicados que preveem as condições meteorológicas de determinadas zonas geográficas e assim sugerir as configurações corretas para os equipamentos instalados nessas zonas[149].

O *Energy Management System* (*EMS*) é uma extensão avançada do SCADA, projetada para otimizar o equilíbrio entre a oferta e a demanda de energia no subsetor da eletricidade. Este sistema auxilia na redução de perdas e no planeamento das operações, permitindo a integração eficiente das fontes renováveis e a gestão da resposta à demanda em tempo real[150].

Verifica-se também a utilização de *machine learning* e de Inteligência Artificial (IA) nalguns campos. Por exemplo, como foi referido em cima, já são aplicadas soluções para derivar a velocidade do vento observável num parque eólico e testar qual será o *output* energético num outro parque eólico com base nesses dados[151].

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

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

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

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

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

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

Está a ocorrer um investimento em sete áreas chave. O investimento nestas áreas reflete um alinhamento com as necessidades específicas do subsetor e as tendências globais da transição energética. Cada uma destas áreas aborda desafios técnicos, económicos e ambientais essenciais para a modernização e descarbonização do subsetor elétrico. Apesar disto, a relevância destes projetos também é estratégica, já que torna o subsetor mais eficiente, sustentável e adaptado aos desafios futuros. Alguns projetos já estão em andamento[152]:

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

A *BladeBug* está a desenvolver um projeto com o objetivo de resolver os desafios operacionais na manutenção e inspeção de turbinas eólicas. Tradicionalmente, estas inspeções, são manuais, complexas e dispendiosas, apresentando riscos para os técnicos envolvidos. Utilizando sistemas robóticos de inspeção nas turbinas eólicas, é esperado que se possa reduzir custos, minimizar os riscos para os trabalhadores e aumentar a eficácia da manutenção. Em junho de 2024, foi realizado um projeto-piloto em Albacete, utilizando robôs para a inspeção de pás de turbinas inacessíveis por corda. No decorrer desta ação foram realizadas inspeções de ensaios não destrutivos assim como funcionais[153].

Na área das redes de distribuição de energia e com o objetivo de tornar a distribuição mais inteligente, eficiente e resiliente, a EDP está a testar o Transformador Híbrido Inteligente (HIT) inovador da IONATE, que aumenta a visibilidade dos dados e o controlo do fluxo da energia das redes elétricas em tempo real. Esta inovação consegue estabilizar os fluxos de energia e aumenta a tolerância da rede às energias renováveis, maximizando assim a quantidade de energia transportada. Este projeto é importante para ajudar na transformação gradual da rede num sistema flexível e inteligente[154].

Atualmente, as centrais fotovoltaicas enfrentam desafios na identificação de falhas, que muitas vezes são difíceis de detetar. O projeto AI4PV visa aprimorar o desempenho operacional destas instalações fotovoltaicas por meio da aplicação de IA e análise de dados. Espera-se que, com a implementação deste projeto, a confiabilidade e a eficiência operacional melhorem significativamente, permitindo uma deteção precoce de falhas e diagnósticos mais precisos. Como resultado, o desempenho económico também deverá aumentar, reduzindo o tempo de inatividade das centrais[155].

[152] EDP, “Inovação na EDP”, https://www.edp.com/pt-pt/inovacao.

[153] EDP, “BladeBug: Inspeção e Manutenção de Turbinas Eólicas”, https://www.edp.com/pt-pt/edp-group/bladebug-inspecao-e-manutencao-de-turbinas-eolicas.

[154] EDP, “IONATE”, https://www.edp.com/pt-pt/inovacao/ionate.

[155] EDP, “AI4PV”, https://www.edp.com/pt-pt/inovacao/new/ai4pv.

Na área do hidrogénio verde, está a ser desenvolvido o programa BEHYOND que visa criar protótipos e implementar um projeto piloto para validar uma nova tecnologia de produção de hidrogénio em *offshore*. Os principais objetivos deste programa incluem o desenvolvimento de um módulo de produção de hidrogénio através de eletrólise, a criação de um sistema inovador para lidar com os desafios de intermitência das energias renováveis e a ampliação da participação do hidrogénio na demanda energética, promovendo assim a sustentabilidade[156].

O projeto FIRMe, lançado em 2023 pela E-REDES, é o primeiro mercado local de serviços de flexibilidade. O objetivo deste projeto é adaptar-se às exigências deste subsetor e testar o mercado, incentivando os prestadores de serviços a participar. Os consumidores e produtores são desafiados a ajustar o seu consumo ou a injetar energia na rede, recebendo em troca um valor acordado pela disponibilidade que oferecem. A plataforma disponibilidade informações sobre as necessidade e oportunidades, permitindo que todos os agentes do mercado participem[157].

A Agenda *Be.Neutral* tem como objetivo colocar Portugal na vanguarda da exportação de produtos ciber-físicos de mobilidade com emissões zero para várias cidades. O projeto visa desenvolver, industrializar e operar novos produtos e serviços de mobilidade[158]. O projeto ARIA2 tem como objetivo desenvolver e avaliar os serviços de informação com base em dados de observação do planeta para o setor de energia eólica, focando-se em infraestruturas *offshore* na Região Atlântica. Irá ser criado um painel integrado que irá centralizar os acessos a serviços, permitindo a visualização avançada de dados. Através da avaliação da erosão causada por chuva nas turbinas, será possível prever as necessidades de reparação dos sistemas de proteção. Este projeto tem como destinatários os proprietários e operadores de parques eólicos[159].

[156] EDP, "BEHYOND: sinergias entre o hidrogénio e a eólica offshore", https://www.edp.com/pt-pt/inovacao/behyond-sinergias-entre-o-hidrogenio-e-a-eolica-offshore.
[157] EDP, "FIRMe: Flexibilidade Integrada em Regime de Mercado", https://www.edp.com/pt-pt/edp-group/firme-flexibilidade-integrada-em-regime-de-mercado.
[158] EDP, "PRR Be Neutral – Ubiquitous Charging", https://www.edp.com/pt-pt/innovation/prr-be-neutral-ubiquitous-charging.
[159] EDP, "ARIA 2", https://www.edp.com/pt-pt/inovacao/aria-2.

**Subsetores do Petróleo e do Gás**

Nos subsetores do petróleo e do gás, os dispositivos de telemetria desempenham também funções importantes. Permitem sobretudo a rápida deteção de bloqueios e de fugas na rede de abastecimento. Igualmente importantes são os sistemas que permitem agendar e automatizar operações, controlar fluxos, recolher dados e monitorizar os níveis de compressão, tanto nos oleodutos e gasodutos, como nos tanques de armazenamento[160]. Também nestes subsetores se começa a verificar a utilização de soluções de IA, orientadas para a criação e análise de modelos geológicos de potenciais locais para novas prospeções de petróleo e gás natural[161].

Os *Safety Instrumented Systems* (*SIS*) são sistemas críticos de segurança que interrompem automaticamente as operações potencialmente perigosas ao detetar condições anormais. São essenciais em ambientes de alto risco, como refinarias e plataformas, desempenhando um papel crucial na prevenção de acidentes graves[162].

Em gasodutos, são utilizados sistemas específicos para a deteção de fugas, conhecidos como *Leak Detection Systems* (*LDS*). Estes são implementados ao longo das redes de gasodutos e previnem acidentes graves ao monitorizar e identificar fugas por meio de sensores de pressão integrados no SCADA, permitindo uma resposta rápida e precisas em emergências[163].

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

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

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

---

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

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

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

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

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

e numa poupança de 17,4 milhões de dólares, o que corresponde a 14 vezes o montante do investimento[165].

O projeto *Hyfuelup* tem como objetivo desenvolver uma tecnologia inovadora para produzir gás natural renovável a partir de resíduos florestais, com um investimento de 10,3 milhões de euros. Em parceria com 11 entidades, incluindo o Laboratório Nacional de Energia e Geologia e o Instituto Politécnico de Portalegre, o projeto utiliza um processo de gaseificação a temperaturas entre 800 e 1.000 graus *celsius* para converter a biomassa num gás combustível, rico em metano e hidrogénio. Esta inovação reside na produção de metano através deste processo. O foco deste projeto são os setores do transporte e mobilidade, permitindo a distribuição do metano para áreas sem acesso à rede de gás natural[166].

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

[165] AVEVA, "AVEVA Predictive Analytics", 2023, https://www.aveva.com/content/dam/aveva/documents/brochures/Brochure_AVEVA_PredictiveAnalytics_23-02.pdf
[166] HYFUELUP, "Shaping a better tomorrow with renewable natural gas", https://hyfuelup.eu/.
[167] catimProjetos, "Green Pipeline Project", https://www.projetoscatim.com/projects-green-pipeline.

## 1.2. Ameaças

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

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

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

Os sistemas *legacy* consistem em *hardware* ou *software* antigo que ainda cumpre as funções para as quais foi adquirido[168], mas que são difíceis de tornar seguros por já não receberem atualizações. Como são sistemas antigos, não podem ser integrados com outras tecnologias ou sistemas mais recentes, criando silos de dados[169] [170]. Devido à sua obsolescência, as capacidades criptográficas destes sistemas são limitadas, o que os torna vulneráveis a ameaças como o *ransomware* e ataques *DDoS*[171].

Segundo o *Threat Landscape Report de 2023* da ENISA, este setor, apesar de não deixar de ser um alvo, ficou na última posição em relação aos outros setores essenciais tendo sofrido, entre julho de 2022 e junho de 2023, cerca de 190 incidentes de cibersegurança (4% do total de incidentes registados)[172]. Os principais ataques passaram pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: "*Denial of Service", DoS*), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)[173]. O ataque predominante foi o *ransomware*, onde 25% dos casos foram operações de um só grupo (*Lockbit*) e 87% dos casos vieram de apenas 20 grupos[174].

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

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

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

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

172 ENISA, "ENISA Threat Landscape 2023", 19 de outubro de 2023, 13.

173 ENISA, "ENISA Threat Landscape 2023", 19 de outubro de 2023, 14.

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

Outra ameaça prende-se com o protocolo IEEE 1588 (*Precision Time Protocol - PTP*)[175]. Este protocolo, essencial para garantir a sincronização temporal de forma precisa, desempenha um papel crucial nas funções de proteção e controlo (P&C). Este protocolo apresenta vulnerabilidades significativas relativamente a incidentes de sincronização do tempo no setor de energia. Ataques como a introdução de atrasos e modificações de pacotes podem comprometer a fiabilidade do protocolo. Este comprometimento pode levar a atrasos na resposta a falhas e pode, também, comprometer a análise e o controlo dos sistemas nas subestações. Como a sincronização dos relógios nos sistemas SCADA e *EMS* é essencial para a coordenação dos sistemas, caso ocorra uma falha nesta sincronização, a tomada de decisões em tempo real pode ficar afetada[176].

Ainda sobre as ameaças relativas foram realizados testes experimentais com diferentes tipos de ataques ao protocolo *PTP*, incluindo atrasos, modificações de pacotes, ataques *DDoS* e *PTP Spoofing*. O *PTP* estabelece uma hierarquia de temporização *master-slave*[177] utilizando o algoritmo *Best Master Clock Algorithm* (*BMCA*)[178]. Este algoritmo escolhe o relógio mais preciso e estável para servir o relógio *master* da rede. Esta escolha é feita com base nas mensagens trocadas entre os relógios, que incluem informações como a qualidade e a prioridade do relógio. O *BMCA* garante que todos os dispositivos mantêm a sincronização com o melhor relógio disponível[179].

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

[175] IEEE, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", 24 de julho de 2008, https://standards.ieee.org/ieee/1588/4355/.
[176] Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588 under Time Synchronization Attacks", 4 de Agosto de 2019, 1, https://ieeexplore.ieee.org/abstract/document/8973494.
[177] Num sistema de comunicação, o *master* controla a comunicação e o *slave* apenas responde aos comandos do *master*. (Fonte: Ingrams Time Systems, "Master & Slave Systems", https://www.ingrams.com.au/master-and-slave-systems.)
[178] Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de agosto de 2019, 1 e 2.
[179] Nokia, "Best Master Clock Algorithm", https://infocenter.nokia.com/public/7705SAR234R1A/index.jsp?topic=%2Fcom.nokia.basic-system-guide%2Fbest-master-clock-algorithm.html.
[180] Um relógio transparente ou *transparent clock* atualiza as mensagens PTP com a informação sobre o tempo necessário para levar as mensagens através da rede desde um ponto de entrada até ao ponto de saída.
[181] Mingyu Han e Peter Crossley, "Vulnerability of IEEE 1588", 4 de agosto de 2019, 2.

De seguida, relativamente ao ataque de modificação de pacotes, foram introduzidos erros de 500 e 1000 microssegundos no campo *correctionField* das mensagens *Sync* (no modo de um e dois passos) e *Follow_Up* (no modo de dois passos), com o mecanismo de *P2P* ativo. Os resultados mostraram que esta modificação comprometeu a precisão da sincronização. Já no ataque de *DDoS*, os resultados experimentais mostraram que a sincronização dos relógios *slave* foi afetada pelo tráfego excessivo. Devido a esta injeção de tráfego, os pacotes *PTP* não conseguiram chegar aos relógios escravos, resultando na perda de sincronização entre os *slaves* X e Y e o relógio *master.* Por fim, no ataque de *spoofing*, quando o relógio de *spoofing* foi conectado ao sistema, conseguiu vencer a eleição no algoritmo *BMCA* (devido à alteração do campo da prioridade pelo emulador), ficando assim com maior prioridade em relação ao relógio *master* verdadeiro. Ambos os relógios *slave* detetaram a mudança e sincronizaram com o relógio de *spoofing*. Quando desconectado, os relógios *slave* voltaram a sincronizar com o *master* verdadeiro[182]. Os resultados evidenciam a necessidade de reforçar a segurança deste protocolo para prevenir ataques que podem comprometer os sistemas de controlo neste setor[183].

O artigo "*Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed*" apresenta uma plataforma de testes em tempo real para a análise vulnerabilidades de cibersegurança no protocolo Modbus RTU/Modbus TCP. Este protocolo é amplamente utilizado nos sistemas SCADA, em redes elétricas inteligentes (*smart grids*) e nos subsetores de petróleo e gás[184].

O protocolo *Modbus RTU/Modbus TCP* foi utilizado como referência para demonstrar a eficácia da plataforma de testes na execução de ciberataques a protocolos dos sistemas do subsetor da energia. A escolha deste protocolo deve-se a diversos fatores: o protocolo ainda é amplamente utilizado nos sistemas do setor. É considerado um protocolo simples e fácil de implementar, e as bibliotecas do protocolo estão disponíveis de forma gratuita para as empresas o implementarem. Apesar de ser amplamente utilizado, o protocolo apresenta vulnerabilidades significativas, como a ausência de criptografia e mecanismos de autenticação robustos[185]. Este protocolo funciona num modelo de comunicação *master-slave*, onde o *slave* inicia as consultas e o *master* responde. A comunicação pode ocorrer via rede, *TCP* ou *UDP*. Como o *Modbus* não incluí autenticação, autorização ou criptografia, permite que qualquer pedido bem formatado seja processado como válido. Este protocolo é composto por seis campos[186]:

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

[182] Mingyu Han e Peter Crossley, “Vulnerability of IEEE 1588”, 4 de agosto de 2019, 4.
[183] Mingyu Han e Peter Crossley, “Vulnerability of IEEE 1588”, 4 de Agosto de 2019, 5.
[184] Bo Chen et al., “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed”, 25 de junho de 2015, 1, https://ieeexplore.ieee.org/abstract/document/7129084.
[185] Bo Chen et al., “Implementing attacks for modbus”, 25 de junho de 2015, 2.
[186] Christopher Parian et al., “Fooling the Master: Exploiting Weaknesses in the Modbus Protocol”, 2454, https://www.sciencedirect.com/science/article/pii/S1877050920312576.

O *master* envia um pedido e o *slave* responde com o identificador da transação, identificador da unidade e a função, indicando sucesso. Em caso de erro, o código da função tem 128 adicionado ao seu valor. A simplicidade deste protocolo facilita a criação de pacotes falsos[187].

Um ataque *MITM* ocorre quando um computador não confiável consegue acesso à comunicação entre duas partes, sem que estejam cientes de tal intrusão. Para que este tipo de ataque seja bem-sucedido, o atacante deve estar na mesma sub-rede do computador-alvo e ser capaz de alterar as caches do *Address Resolution Protocol* (*ARP*). Desta forma, o atacante pode receber o tráfego de ambas as vítimas e agir como um *router*, encaminhando o tráfego recebido. No ambiente de testes deste estudo, o atacante alterou as *caches* do *ARP* cliente *Modbus*, após isso, conseguiu visualizar os pacotes de consulta e resposta trocados entre o *master* e o *slave* e foi utilizada a ferramenta *Wireshark* para analisar os mesmos. Com o conhecimento dos endereços de IP do *master* e do *slave*, foi possível ao atacante emular o *master* e enviar um comando *Modbus* para desligar o dispositivo eletrónico[188].

Para avaliar a sensibilidade deste protocolo a atrasos, o mesmo foi submetido a um ataque *TCP SYN Flood* para sobrecarregar o *master*. Este tipo de ataque aproveita-se do processo de *handshake* do *TCP* para iniciar várias conexões com endereços de IP falsos, saturando-o com pedidos falsos. Foram enviados cerca de 120 pedidos falsos por segundo. Antes deste ataque, a resposta a um comando era de 300 milissegundos, durante este ataque, a resposta passou a ser de 3 segundos. Este atraso impede que o centro de controlo tenha uma visão atualizada da rede, comprometendo as operações de funções críticas. A análise concluí que a falta de autenticação e proteção no protocolo torna-o vulnerável a ataques que podem afetar a estabilidade. Como recomendações, propõe-se a adição de autenticação, criptografia a nível de *IP* e outros mecanismos de defesa para mitigar estes riscos[189].

Ainda sobre ameaças do setor energético, segundo dados do CERT.PT, registaram-se em Portugal, entre 2019 e 2023, 144 ataques ao setor[190].

**Figura 1 - Número de incidentes no setor da Energia anualmente**


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

[187] Christopher Parian et al., "Fooling the Master: Exploiting Weaknesses in the Modbus Protocol", 2454.
[188] Bo Chen et al., "Implementing attacks for modbus", 25 de junho de 2015, 1-4.
[189] Bo Chen et al., "Implementing attacks for modbus", 25 de junho de 2015, 5-6.
[190] CNCS, "Incidentes e Setores", Conhecimento Situacional: Estatísticas, obtido a 24 de outubro de 2024, https://www.cncs.gov.pt/pt/estatistica/#cert.pt.

**Subsetor da Eletricidade**

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

Em 2001, o operador de eletricidade da Califórnia, foi vítima de um incidente de cibersegurança, onde os atacantes conseguiram acesso à rede interna do operador. Este ataque foi conduzido através de um método de infiltração, utilizando vários servidores e prestadores de serviços de Internet para ocultar a origem dos atacantes[191]. Apesar disto, os atacantes foram descobertos antes de conseguirem ter acesso ao controlador PLC[192].

Mais tarde, em 2012, foi criado o *malware* conhecido por *Flame*, tendo este sido espalhado pelo Médio Oriente e Norte de África, onde operou por pelo menos dois anos. Este *malware* era extremamente sofisticado e conseguia recolher dados como gravações de áudio, capturas de ecrã e comunicações *Bluetooth*, além de conseguir monitorizar as teclas digitadas. Utilizava certificados digitais falsos da *Microsoft* para se espalhar sem ser detetado[193]. Foi concebido para espionagem e análise de dados, e foi descoberto depois de o Ministério do Petróleo do Irão e a empresa nacional iraniana de petróleo denunciarem o furto e a eliminação de dados críticos nos seus sistemas[194].

Um outro exemplo marcante de um ciberataque com grande impacto foi o ataque à rede elétrica da Ucrânia em dezembro de 2015. Este ataque foi particularmente importante porque foi o primeiro em que efetivamente uma entidade externa ganhou o controlo dos sistemas de uma central elétrica e cortou o abastecimento de energia. Nalgumas zonas, o corte durou apenas uma hora, enquanto noutras só foi resolvido ao fim de seis horas. Ao todo, cerca de 230 mil pessoas foram afetadas pelo corte de energia. Crê-se que o acesso terá sido obtido pelos agentes de ameaça através de uma campanha de *spear-phishing* dirigida aos colaboradores de TI e administradores de sistemas de diversas companhias de distribuição de energia elétrica da Ucrânia[195].

Um outro caso ocorreu em Portugal - o ciberataque à EDP - a 13 de abril de 2020. Tratou-se de um ataque de *ransomware*, que utilizou o vírus *Ragnar Locker*. Parte da rede e dos sistemas da empresa ficaram bloqueados e, segundo a própria EDP, o normal funcionamento de alguns serviços e operações, como o atendimento ao cliente, ficou condicionado, apesar de não se ter registado qualquer impacto na continuidade do fornecimento de energia[196].

[191] The New York Times, "Hackers Attacked California Power", 10 de junho de 2001, https://www.nytimes.com/2001/06/10/us/hackers-attacked-california-power.html.
[192] ECS, "Energy Networks and Smart Grids", novembro de 2018, 5, https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf.
[193] Kim Zetter, "Meet 'Flame', The Massive Spy Malware Infiltrating Iranian Computers", Wired, 28 de maio de 2012, https://www.wired.com/2012/05/flame/.
[194] ECS, "Energy Networks and Smart Grids", novembro de 2018, 6.
[195] CISA, "Cyber-Attack Against Ukrainian Critical Infrastructure", 20 de julho de 2021, https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
[196] Miguel Prado, "EDP: imune à crise, mas não aos *hackers*", *Expresso*, 18 de abril de 2020, https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers.

De seguida, apresenta-se uma tabela que faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos[197], 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[198].
- **Agentes estatais:** 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[199].
- ***Hacktivistas*:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação, por uma forte elaboração ficcionada do ciberataque e das suas consequências bem como pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável[200].
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade, podendo ser maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento). Comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer, e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso[201]. No caso, consideraram-se os colaboradores internos maliciosos.

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

**Tabela 5 - Agentes de ameaça mais prováveis (Eletricidade)**

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

Legenda:
■ - Agente de ameaça provável

**Subsetor do Petróleo**

O incidente de cibersegurança na Colonial Pipeline, empresa norte-americana detentora do maior oleoduto dos Estados Unidos, ocorreu a 7 de maio de 2021 e foi um ataque de *ransomware* que afetou as operações da mesma durante cerca de cinco dias. O oleoduto, que cobre cerca de 8850 km e é capaz de transportar o equivalente a três milhões de barris de combustível por dia, ao longo do território entre o Texas e Nova Iorque, foi desligado, de modo a impedir que a infeção se alastrasse à TO do mesmo. Apesar de o próprio oleoduto não ter sido comprometido pelo ataque, as notícias do ciberataque e da paragem do funcionamento do oleoduto levaram a população a uma corrida aos postos de abastecimento, resultando em longas filas e a reservas esgotadas na costa leste dos EUA[202].

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

O acesso inicial à rede e aos sistemas da empresa terá sido obtido através da descoberta de uma palavra-passe de um ex-colaborador da empresa cujo perfil de utilizador ainda não tinha sido desativado. A palavra-passe foi introduzida numa VPN que não possuía autenticação multifator, dando acesso imediato à rede e a diversos sistemas[203]. A Colonial Pipeline acabaria por pagar o resgate exigido de 75 *bitcoins*, na altura valorizadas em cerca de 4,4 milhões de dólares, de modo a recuperar o controlo dos seus sistemas. Entre maio e junho, o Departamento de Justiça dos EUA conseguiu recuperar cerca de 85% das *bitcoin*s transferidas, mas devido à desvalorização que estas tinham sofrido, as *bitcoin*s recuperadas valiam, à data, cerca de 2,3 milhões de dólares, cerca de 52% do valor do resgate pago[204].

No final de janeiro de 2022, um ataque de *ransomware* afetou gravemente pelo menos 17 portos e terminais de petróleo na Europa Ocidental, impactando também o armazenamento e transporte de petróleo. O ataque causou o desvio de navios petroleiros, prejudicando as cadeias de abastecimento e dificultando o carregamento e descarregamento de produtos refinados. O grupo de cibercriminosos responsável pelo ataque foi identificado como sendo o grupo BlackCat e os relatórios de investigação sobre este incidente sugerem que o impacto foi maior nos sistemas de TI do que nos sistemas de TO[205].

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

**Tabela 6 - Agentes de ameaça mais prováveis (Petróleo)**

| Tipo de ameaça | Cibercriminosos | Agentes estatais | Hacktivistas | Colaboradores internos |
|---|---|---|---|---|
| *Ransomware* | ■ | ■ | ■ | ■ |
| *Malware* | ■ | ■ | ■ | ■ |
| Vulnerabilidades | ■ | ■ | ■ | ■ |
| *Phishing* | ■ | ■ | | |
| *DDoS* | ■ | ■ | ■ | |
| Manipulação de Sistemas (TI) | ■ | ■ | ■ | ■ |
| Manipulação de Sistemas (TO) | ■ | ■ | ■ | ■ |

Legenda:
■ - Agente de ameaça provável

[203] Stephanie Kelly e Jessica Resnick-ault, "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators", *Reuters*, 9 de junho de 2021, https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
[204] CISA, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years", 7 de maio de 2023.
[205] Pacific Maritime Magazine, "European Oil Port Terminals Crippled by Cyberattack and Ransomware", https://pacmar.com/article/european-oil-port-terminals-crippled-by-cyberattack-and-ransomware/.

**Subsetor do Gás**

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

Em 1982, num dos primeiros incidentes de cibersegurança conhecidos, ocorreu uma explosão num gasoduto na Sibéria. Este incidente teve origem externa e foi realizado através da introdução de *malware* nos sistemas SCADA de gestão do gasoduto[206]. Este malware duplicou a pressão durante um teste e, alegadamente, como resultado, ocorreu uma explosão equivalente a três toneladas de *TNT*[207].

Em 1999, a Gazprom, sofreu um incidente de segurança, onde um atacante interno conseguiu tomar conta de um quadro de distribuição que controlava o gás nos gasodutos[208], este atacante conseguiu invadir os sistemas SCADA da Gazprom com a ajuda interna e utilizando um *Trojan* para ultrapassar a segurança. Através do quadro de distribuição, foi possível controlar temporariamente o fluxo de gás nos gasodutos[209].

No mesmo ano, nos Estados Unidos da América (EUA), ocorreu um erro relacionado com um novo desenvolvimento de uma base de dados para o sistema operativo dos sistemas SCADA dos gasodutos da Olympic. Como consequência, ocorreu uma fuga de gás que provocou oito feridos e três mortos[210]. A investigação identificou vários problemas de segurança, incluindo: as escavações realizadas nas proximidades do gasoduto; as avaliações das inspeções internas; a gestão dos dados disponíveis para garantir a integridade do sistema; e o desempenho e segurança do sistema SCADA da Olympic[211].

Em 2012, a Saudi Aramco foi vítima do *malware Shamoon* e cerca de 35 mil computadores tiveram os seus dados parcial ou totalmente apagados pelo vírus. O propósito deste *malware* é apagar todos os dados por completo em vez de exigir resgate. Em resposta ao ataque, a Saudi Aramco desligou fisicamente todos os escritórios da Internet, o que levou a um regresso temporário a sistemas de papel. Apesar dos sistemas de produção de petróleo e gás não terem sido afetados, os sistemas de pagamento ficaram fora de serviço, causando filas de camiões de combustível que não podiam ser carregados por falta do processamento de pagamentos. A empresa demorou cinco meses a recuperar totalmente deste incidente[212].

---

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

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

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

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

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

211 NTSB, “Pipeline Rupture and Subsequent Fire in Bellingham, Washington”, 4, https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.

212 Zakariya Dehlawi e Norah Abokhodair, “Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident”, *paper* apresentado na *2013 IEEE International Conference on Intelligence and Security Informatics*, junho de 2013. https://www.researchgate.net/publication/261456882_Saudi_Arabia's_response_to_cyber_conflict_A_case_study_of_the_Shamoon_malware_incident.

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

**Tabela 7 - Agentes de ameaça mais prováveis (Gás)**

| Tipo de ameaça | Cibercriminosos | Agentes estatais | Hacktivistas | Colaboradores internos |
|---|---|---|---|---|
| *Ransomware* | ■ | ■ | ■ | ■ |
| *Malware* | ■ | ■ | ■ | ■ |
| Vulnerabilidades | ■ | ■ | ■ | ■ |
| *Phishing* | ■ | ■ | | |
| *DDoS* | ■ | ■ | ■ | |
| Manipulação de Sistemas (TI) | ■ | ■ | ■ | ■ |
| Manipulação de Sistemas (TO) | ■ | ■ | ■ | ■ |

Legenda:
■ - Agente de ameaça provável

## 1.3. Capacitação

Os operadores do setor energético entendem ter-se tornado largamente dependentes da sua infraestrutura digital para a realização de operações e na prestação de serviços eficientes. Entendem, também, que o aumento dessa dependência conduz a uma maior exposição a riscos de cibersegurança. Por este motivo, têm envidado esforços no sentido de se capacitarem e de se tornarem mais resilientes ao nível da cibersegurança[213].

Essa capacitação tem passado pela melhoria contínua da segurança dos sistemas internos, pela aquisição, implementação ou melhoria dos serviços de SOC, dedicados à monitorização contínua da segurança das infraestruturas de TI e de TO, pela realização de testes de resiliência operacional, pela aposta na formação na área dada aos colaboradores tanto ao nível de aquisição de competências técnicas, como de sensibilização, pela integração em grupos internacionais de partilha de informações sobre ameaças, técnicas e boas práticas de cibersegurança, bem como pela aquisição de seguros de cibersegurança[214] [215].

A par destas medidas, verifica-se que tem havido no setor uma aposta nas ferramentas de IA. Por enquanto, estas são essencialmente procuradas para a automatização de processos e para o processamento de grandes quantidades de dados sensíveis, e não tanto para funções diretamente relacionadas com cibersegurança. Os operadores referem, no entanto, que a cibersegurança continua a ser uma preocupação sempre que se procura adquirir ou implementar uma nova ferramenta que recorra a IA, investindo nas competências dos colaboradores para utilizarem estas ferramentas e limitando os seus ambientes de utilização, garantindo a segurança das entidades durante a utilização das ferramentas, bem como dos dados sensíveis por estas tratados[216].

**Subsetor da Eletricidade**

No subsetor elétrico, há também uma aposta crescente nas redes inteligentes ou *smart grids*. Estas redes são redes elétricas que utilizam tecnologias digitais, sensores e *software* para uma melhor resposta à oferta de energia em tempo real, de modo a minimizar custos e a manter a estabilidade e confiabilidade da rede. Estas redes inteligentes estão intimamente ligadas à cibersegurança, devido à dependência das tecnologias como os sensores e *software* para gerir e monitorizar a distribuição da energia em tempo real. Estas redes conectam uma vasta gama de dispositivos, o que aumenta a vulnerabilidade a incidentes de cibersegurança. Em Portugal, registou-se um crescimento de 15% nas *smart grids* em 2022, face a 2021, e em 2023 registou-se um crescimento de 22% face aos números de 2022[217].

A iniciativa "Cyber Range" da EDP, focada em cibersegurança e formação dos colaboradores, foi lançada em 2016 e procura consciencializar e capacitar a equipa de cibersegurança para identificar e responder a ciberataques, oferecendo um laboratório de segurança, uma área para exercícios práticos e uma academia de formação[218].

---

[213] EDP, “Relatório Anual Integrado 2023”, 51.

[214] EDP, “Relatório Anual Integrado 2023”, 51-52.

[215] Galp, “Relatório Integrado Anual 2022”, 138-139.

[216] EDP, “Relatório Anual Integrado 2023”, 51.

[217] EDP, “Relatório Anual Integrado 2023”, 68-69.

[218] EDP, “Cyber Range: Promover a sensibilização da cibersegurança”, julho de 2020, 1-2, https://www.edp.com/sites/default/files/2021-03/10_cyber_range_novo_PT.pdf.

A Endesa, em parceria com a CGI, iniciou uma transformação digital de forma a modernizar o seu modelo de negócio e aprimorar a experiência do cliente. Este projeto envolve a migração para um modelo de serviços flexível, permitindo ajustar os seus serviços com base na demanda, reduzir custos e acelerar o lançamento de novos produtos. Neste projeto de transformação digital, a cibersegurança é essencial para proteger as novas infraestruturas digital. Foram implementadas medidas para proteger os dados sensíveis dos clientes e garantir a segurança das operações digitais, abrangendo o *CRM*, análise de dados e plataformas de atendimento. Assim, é possível reduzir os riscos e manter a integridade dos sistemas num ambiente cada vez mais interconectado[219].

A E-Redes tem investido numa estratégia de capacitação em cibersegurança para proteger a infraestrutura digital crítica que sustenta as suas operações. Este investimento é essencial, visto que a empresa administra uma rede essencial para o fornecimento contínuo de energia elétrica, o que exige resiliência contra incidentes de cibersegurança. Entre as medidas, está a formação dos profissionais e colaboração com entidades especializadas para identificar e mitigar vulnerabilidades. Além disso, a E-Redes, adota uma política abrangente de segurança da informação, que inclui prevenção, integridade e disponibilidade dos dados[220].

**Subsetor do Petróleo e Gás**

Os subsetores do petróleo e gás são das indústrias mais relevantes e influentes a nível global, desempenhando um papel fundamental na economia e na sociedade moderna. A extração e a refinação, tanto de petróleo como de gás, fornecem combustível para os setores do transporte e aquecimento, mas também são essenciais para a produção de uma ampla gama de produtos químicos e materiais, incluindo plásticos, fertilizantes e medicamentos. A formação especializada também é crucial para assegurar a segurança nas operações, uma vez que o gás natural e os gases alternativos requerem conhecimentos técnicos e normas específicas para prevenir os riscos. Desta forma, a capacitação no setor do gás não atende apenas aos requisitos de conformidade legal, mas também promove a modernização da infraestrutura energética[221].

A Repsol, em parceria com o Instituto do Emprego e Formação Profissional (IEFP), integrou 26 novos colaboradores no seu Complexo Industrial de Sines, onde foram formados como Técnicos de Operação de Unidades Industriais. Este projeto fez parte de uma iniciativa para expandir e modernizar o complexo, com um investimento de 657 milhões de euros. O programa oferece uma formação extensa, abrangendo aulas práticas, teóricas e operacionais com foco na segurança e sustentabilidade, contribuindo para o desenvolvimento de uma indústria química mais sustentável e inovadora em Portugal[222]. Em parceria com a Escola Tecnológica do Litoral Alentejano (ETLA), a Repsol oferece cursos técnicos em áreas como a Mecatrónica e Química Tecnológica, além de estágios práticos e formação para jovens locais. Este compromisso tem como objetivo melhorar a segurança, bem-estar e desenvolvimento socioeconómico da comunidade[223].

---

[219] CGI, “Endesa aposta na transformação digital e reinventa o seu modelo de negócio”, https://www.cgi.com/portugal/pt-pt/case-study/business-consulting/endesa-aposta-na-transformacao-digital-e-reinventa-o-seu-modelo-de.

[220] E-Redes, “Cybersecurity: New challenges, the same priority”, https://www.e-redes.pt/en/networks-of-future/cybersecurity/cybersecurity.

[221] Compete 2030, “Europa lidera combate à emergência climática”, 8 de julho de 2024, https://www.compete2030.gov.pt/comunicacao/europa-lidera-combate-a-emergencia-climatica/.

[222] Epcol, “Repsol contrata novo grupo de colaboradores e lança curso com o IEFP para os formar”, 17 de março de 2022, https://www.epcol.pt/noticias-das-associadas/repsol-contrata-novo-grupo-de-colaboradores-e-lanca-curso-com-o-iefp-para-os-formar/1236.

[223] REPSOL, “Formação”, https://sines.repsol.pt/pt/comunidade/seguranca/formacao/index.cshtml.

As principais empresas de petróleo e gás em Portugal, como a Galp, estão fortemente focadas em fortalecer a cibersegurança. No caso da Galp, a empresa participa da Rede Nacional de CSIRT, uma rede nacional que promove a resposta rápida a incidentes de cibersegurança e a partilha de informações com outras empresas públicas e privadas[224]. A Galp também integra a iniciativa global "Cyber Resilience Pledge" do Fórum Económico Mundial, que promove a colaboração internacional para fortalecer a resiliência digital, implementando práticas de cibersegurança específicas para estes subsetores[225].

Internamente, a Galp adotou um modelo de cibersegurança em colaboração com a Microsoft, utilizando uma plataforma integrada de monitorização e resposta a ameaças, como o Microsoft 365 E5. Esta plataforma consolida informações de segurança num único painel, permitindo à equipa de cibersegurança visualizar e controlar as vulnerabilidades de maneira centralizada, uma medida especialmente importante para a proteção das suas operações. Com uma equipa especializada de cibersegurança, a Galp também realiza auditorias frequentes e investe na formação para garantir que todos os colaboradores estejam preparados para adotar práticas seguras no uso dos sistemas digitais, adaptando as políticas de segurança às necessidades das diferentes funções e localizações do trabalho[226].

[224] Security Magazine, “GALP dá mais um passo na sua segurança e integra rede nacional CSIRT”, 20 de julho de 2021, https://www.securitymagazine.pt/2021/07/20/galp-da-mais-um-passo-na-sua-seguranca-e-integra-rede-nacional-csirt/.
[225] Galp, “Galp e empresas de energia unidas contra ciber-ataques no Fórum Económico Mundial”, 25 de maio de 2022, https://www.galp.com/media/comunicados-de-imprensa/comunicado/id/1351/galp-e-empresas-de-energia-unidas-contra-ciber-ataques-no-forum-economico-mundial.
[226] Security Magazine, “Galp Energia mantém segurança dos serviços críticos com plataforma xDR com M365 E5”, 6 de setembro de 2024, https://www.securitymagazine.pt/2024/09/06/galp-energia-mantem-seguranca-dos-servicos-criticos-com-plataforma-xdr-com-m365-e5/.

## 1.4. Investimento em cibersegurança

O relatório *NIS Investments 2022*, da ENISA, que investigou em maior detalhe os setores da saúde e da energia, oferece dados sobre os investimentos realizados em cibersegurança. Segundo o relatório, a cibersegurança tem-se tornado uma prioridade dentro do investimento tecnológico, com cerca de 74% dos operadores europeus a terem aumentado o volume de investimento em cibersegurança face ao ano anterior (2020). Os operadores na UE têm investido, sobretudo, nas capacidades de análise de dados, IA e *machine learning*. O aumento das redes de sensores utilizados para a recolha de dados e telemetria tem também sido um objetivo da maioria dos operadores[227].

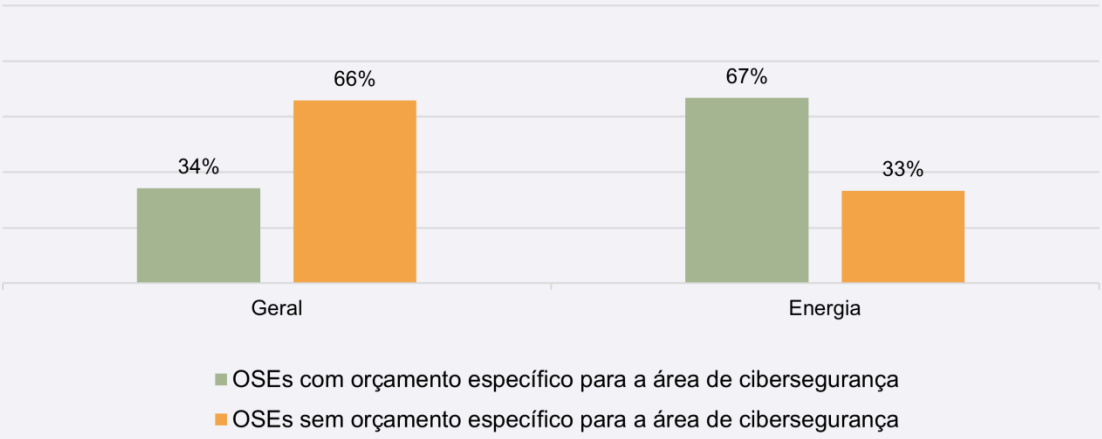
A aquisição de serviços em nuvem (*cloud services*) tem também crescido, com cerca 45% dos operadores a terem aumentado os investimentos nesta área. Concomitantemente, 39% dos operadores procuram reduzir os custos com sistemas *legacy* e *data centres* internos, transferindo-os para a nuvem[228].

Durante o ano de 2021, a mediana do investimento nas TIC foi de cerca de 20 milhões de euros entre os operadores do setor energético a nível europeu. Já o investimento em TI teve um valor mediano de um milhão de euros. Terá ainda havido, em Portugal, um investimento médio de cerca de 150 mil euros em TO durante o ano de 2021[229].

A CLC, juntamente com Galp, REN, EDP e E-REDES, participa ativamente no ISAC-EnergyPT, em colaboração com o Centro Nacional de Cibersegurança, para enfrentar o aumento das ameaças de cibersegurança[230].

Deste setor, cerca de 67% das entidades têm um orçamento específico para a área de cibersegurança, enquanto a média geral ronda os 34% (**Gráfico 109**).

**Gráfico 109 - Orçamento específico para a área de cibersegurança**




[227] ENISA, "NIS Investments", novembro de 2022, 11.
[228] ENISA, "NIS Investments", novembro de 2022, 11.
[229] ENISA, "NIS Investments", novembro de 2022, 64.
[230] CLC, "Relatório de Gestão & Contas 2023", 35, https://www.clc.pt/DocsCLC/2024/CLC_RC_2023.pdf.

Relativamente às áreas de aplicação do orçamento de cibersegurança, 100% aplica na segurança das redes, na aquisição de *software* e *hardware,* e formação, 83% na análise de segurança, na capacitação em tecnologia e em gestão de vulnerabilidades, e 50% na contratação de pessoal e governança (**Gráfico 110 e 110.1**).

**Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança**

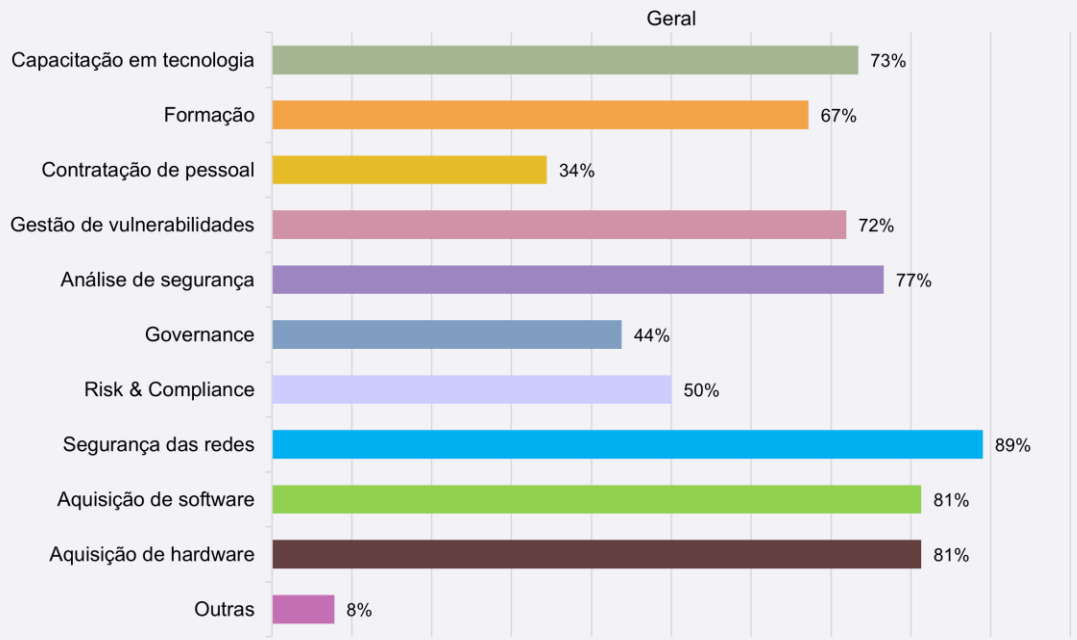
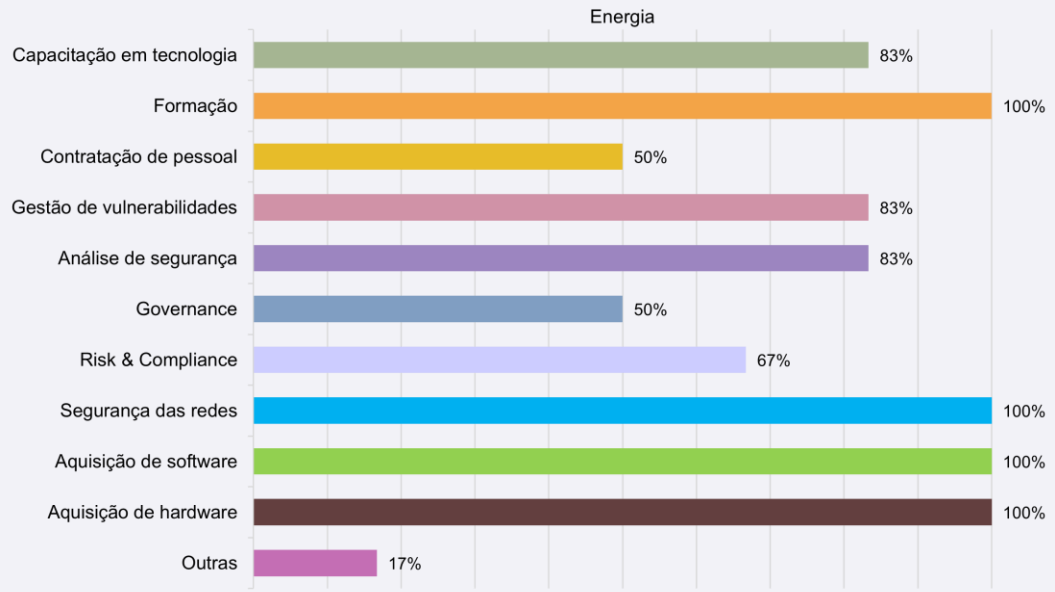
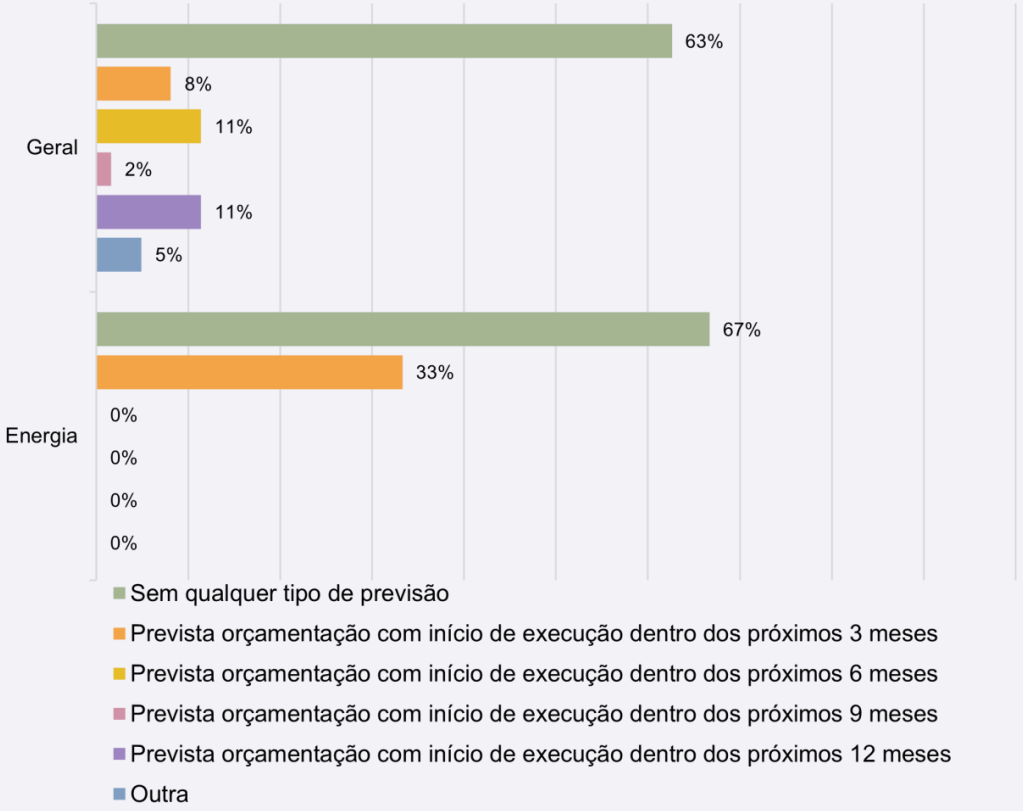



**Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança**



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 67% não tem qualquer previsão para a orçamentação e 33% tem previsto a orçamentação para os próximos 3 meses (**Gráfico 111**).

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




### Subsetor da Eletricidade

O setor energético, mais concretamente o subsetor da eletricidade, tem vindo a investir paulatinamente na área de cibersegurança. Um exemplo disso são as declarações prestadas pela EDP no seguimento do ciberataque de 2020, nas quais se refere que a empresa tinha, recentemente, realizado um investimento na ordem dos 50 milhões de euros em segurança informática[231]. O relatório de contas de 2023 da mesma empresa indica ainda um investimento global de dois mil milhões de euros, entre 2023 e 2026, na transformação digital, no qual se inclui a cibersegurança e a ciberresiliência, embora não seja indicada a quantia alocada a estas temáticas[232].

[231] Prado, "EDP: imune à crise, mas não aos hackers".

[232] EDP, "Relatório Anual Integrado 2023", 52.

De acordo com o relatório de gestão de 2023, a EDP implementou uma transformação digital significativa, investindo cerca de 2 mil milhões de euros em TOTEX digital[233] entre 2023 e 2026, com foco na ciberresiliência. Apesar dos esforços realizados, o risco de ciberataques cresceu em frequência e em gravidade. Para mitigar estes riscos, a EDP promoveu ações de formação e sensibilização sobre segurança da informação, organizando "digital talks" para aumentar o conhecimento em cibersegurança, e contratou um seguro de risco de cibersegurança.[234].

Novamente, a EDP, investiu também na criação da *Digital Global Community*, uma plataforma virtual que promove a colaboração e a partilha de conhecimento em tecnologias digitais, incluindo cibersegurança. Atualmente, esta comunidade conta com quase dois mil membros, refletindo o compromisso da empresa em fomentar a inovação e a troca de experiências no âmbito digital. A EDP ainda implementou outro programa denominado All Cyber, destinado a fortalecer a cibersegurança da organização como um todo. Este programa estabelece um processo global robusto de monitorização e resposta a ameaças e abrange três áreas principais, nomeadamente, a definição de um modelo organizacional de cibersegurança, a criação de um sistema para proteger a documentação e a informação, e o estabelecimento de métricas e *KPIs* de cibersegurança a nível global[235].

Em 2019, o INESC TEC e o grupo EDP firmaram um contrato-programa de cinco anos para impulsionar a inovação no setor energético, com um investimento superior a um milhão de euros em consultoria avançada, pesquisa, desenvolvimento e formação. O objetivo é maximizar a energia renovável, desenvolver redes inteligentes, integrar veículos elétricos e explorar novas tecnologias. A colaboração, que já conta com mais de 20 anos, abrange também áreas cruciais como cibersegurança, garantindo a proteção das infraestruturas digitais, monitorização em tempo real e a segurança das *smart grids* no contexto da evolução do setor energético[236].

A E-Redes, no seu Plano de Desenvolvimento e Investimento da Rede de Distribuição, para o período de 2021 a 2025, incluiu um foco estratégico na área da cibersegurança. Este investimento, estimado em 6,4 milhões de euro, vista principalmente a atualização dos sistemas de *hardware* e *software* da empresa, fortalecendo a sua infraestrutura digital e protegendo-a contra ameaças emergentes[237].

[233] O termo TOTEX digital refere-se ao investimento total em ativos digitais, englobando tanto os custos operacionais como os de capital necessários para implementar e manter a infraestrutura digital da empresa. (Fonte: Nicholas Woodroof, "TOTEX: commercial creativity and the supply chain of the future", OilField Technology, 12 de agosto de 2019, https://www.oilfieldtechnology.com/special-reports/12082019/totex-commercial-creativity-and-the-supply-chain-of-the-future/).

[234] EDP, "Parte I – Relatório de Gestão 2023", setembro de 2024, 50, https://www.edp.com/sites/default/files/2024-09/Parte%20I%20-%20Relat%C3%B3rio%20de%20Gest%C3%A3o%202023.pdf.

[235] EDP, "Parte I – Relatório de Gestão 2023", setembro de 2024, 167-168.

[236] BIP, "INESC TEC e EDP assinam contrato-programa na área de energia", junho de 2019, https://bip.inesctec.pt/noticias/inesc-tec-e-edp-assinam-contrato-programa-na-area-de-energia/.

[237] E-Redes, "Plano de Desenvolvimento e Investimento da Rede de Distribuição: Período 2021-2025", 122-123, https://www.erse.pt/media/0wji5213/anexo-i_j-proposta-ren-portg%C3%A1s-distribui%C3%A7%C3%A3o.pdf.

**Subsetor do Petróleo**

Em 2023, as métricas de segurança e descarbonização representaram 25% dos indicadores de desempenho anual de todos os colaboradores e membros da Comissão Executiva da Galp. A metodologia OKR (Objectives and Key Results), uma abordagem de gestão que define objetivos claros e mensuráveis e os resultados chave para alcançá-los, também foi implementada, incluindo objetivos focados na sustentabilidade para 2024, abordando temas como cibersegurança, descarbonização e energias renováveis[238].

A Galp deu prioridade à cibersegurança para evitar falhas significativas, investindo em infraestruturas de dados e cultivando uma forte cultura em cibersegurança. A empresa conta com uma equipa de resposta a incidentes que opera 24/7. Em 2023, lançou um novo *roadmap* de cibersegurança e iniciou campanhas de sensibilização para colaboradores e clientes. Reconhecida como uma das melhores do setor de energia em cibersegurança, a Galp também promove a cooperação na Aliança Portuguesa de Cibersegurança para fortalecer a proteção da economia digital[239].

É adotada uma abordagem abrangente para mitigar riscos de cibersegurança. A empresa garante a identificação, proteção, deteção e resposta a ciberameaças em todas as operações. Para isso, implementa medidas técnicas e processuais que asseguram a visibilidade de fragilidades nos seus sistemas e nos prestadores de serviços, realizando avaliações regulares e simulando ataques externos. Também é seguido um *roadmap* de melhorias contínuas até 2024, com base em avaliações de maturidade realizadas em 2022[240].

Foi iniciado um projeto de revitalização dos *PLCs* de segurança no Parque de Aveiras, visando substituir processadores e módulos de entrada/saída nos sistemas de controlo (DCS), sistemas de proteção (SGS) e sistemas de incêndio e gás (FGS). O principal objetivo é melhorar o controlo e a segurança da infraestrutura, evitando interrupções nos processos de receção, armazenamento, movimentação e expedição da CLC. Também foram adjudicados dois projetos essenciais para aumentar a disponibilidade e a cibersegurança, sendo o *revamping* do sistema SCADA do oleoduto e a expansão das infraestruturas SCADA do Parque[241].

A CLC criou uma área dedicada à cibersegurança e desenvolveu um *roadmap* plurianual para melhorar a proteção e maturidade organizacional. Implementou ainda melhorias conforme a *framework* NIST CSF, incluindo processos de *backups*, gestão de vulnerabilidades e uma solução de gestão de acessos privilegiados, *CyberArk*, para controlar os acessos críticos na infraestrutura[242]. A empresa assegura a identificação, proteção, deteção e resposta a ciberameaças que afetam a sua tecnologia, pessoas e processos, em todas as suas operações. Para garantir a segurança, foi implementado um conjunto de medidas e mecanismos de proteção e deteção, adaptando-se continuamente às ameaças de cibersegurança enfrentadas[243].

[238] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 30, https://www.galp.com/corp/Portals/0/Recursos/Investidores/IMR2023/PT/RelatorioIntegradoAnual2023HQ.pdf.
[239] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 125.
[240] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 171.
[241] CLC, “Relatório de Gestão & Contas 2023”, 25.
[242] CLC, “Relatório de Gestão & Contas 2023”, 26.
[243] CLC, “Relatório de Gestão & Contas 2023”, 35.

De acordo com o relatório de contas de 2023 da Repsol, a empresa investiu aproximadamente 15 milhões de euros em formação, que totalizou mais de 840 mil horas. Este investimento concentrou-se particularmente na capacitação em cibersegurança, fornecendo aos colaboradores as habilidades necessárias para utilizar diversas ferramentas e aplicações digitais[244].

**Subsetor do Gás**

O investimento em cibersegurança no subsetor do gás está a ser impulsionado pela crescente digitalização das infraestruturas críticas e pelo aumento significativo de incidentes de cibersegurança. Segundo um relatório da Accenture, entre 2017 e 2019, os investimentos em cibersegurança aumentaram 49%, enquanto os recursos destinados à *IoT* registaram uma redução de 4%[245].

Em 2023, as métricas de segurança e descarbonização representaram 25% dos indicadores de desempenho anual de todos os colaboradores e membros da Comissão Executiva da Galp[246].

A Galp deu prioridade à cibersegurança para evitar falhas significativas, investindo em infraestruturas de dados e cultivando uma forte cultura em cibersegurança. A empresa conta com uma equipa de resposta a incidentes que opera 24/7. Em 2023, lançou um novo *roadmap* de cibersegurança e iniciou campanhas de sensibilização para colaboradores e clientes. Reconhecida como uma das melhores do setor de energia em cibersegurança, a Galp também promove a cooperação na Aliança Portuguesa de Cibersegurança para fortalecer a proteção da economia digital[247].

É adotada uma abordagem abrangente para mitigar riscos de cibersegurança. A empresa garante a identificação, proteção, deteção e resposta a ciberameaças em todas as operações. Para isso, implementa medidas técnicas e processuais que asseguram a visibilidade de fragilidades nos seus sistemas e nos prestadores de serviços, realizando avaliações regulares e simulando ataques externos. Também é seguido um *roadmap* de melhorias contínuas até 2024, com base em avaliações de maturidade realizadas em 2022[248].

[244] Repsol, “Integrated Management Report 2023”, 97, https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/informes-anuales/2023/integrated-management-report-2023.pdf.
[245] Accenture, “Fast forward: accelerating the journey to reinvention”, 8, https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-157/accenture-fast-forward-accelerating-the-journey-to-reinvention.pdf.
[246] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 30.
[247] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 125.
[248] GALP, “Parte 1: Relatório Integrado de Gestão 2023”, 171.

## 1.5. RJSC e legislação setorial

O setor da energia e respetivos subsetores são alvos de legislação europeia e nacional há largos anos, embora a legislação em matéria de cibersegurança tenha surgido mais tardiamente, sobretudo a partir da segunda metade da década de 2010, altura em que começam a surgir diversos diplomas legais que fazem menção específica à cibersegurança. Não obstante, diplomas anteriores apresentavam já provisões sobre a segurança física e a necessidade de realizar análises de risco entre os produtores e distribuidores de energia. Ver-se-ão, de seguida, alguns desses diplomas, quer de âmbito setorial ou subsetorial, quer de âmbito geral.

**Subsetor da Eletricidade**

Uma das primeiras Diretivas mais relevantes em matéria de segurança no subsetor da Eletricidade foi a Diretiva 2005/89/CE, relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas, de 18 de janeiro de 2006[249]. Embora este fosse um diploma sem referências específicas à cibersegurança, o mesmo incluía a necessidade de os operadores manterem um nível adequado de segurança do funcionamento das redes, bem como a disponibilidade de capacidade de produção[250]. Para tal, os Estados-membros deviam, entre outros pontos, "promover medidas de incentivo à adoção de tecnologias de gestão da procura em tempo real, tais como sistemas de medição tecnologicamente avançados"[251] junto dos operadores. Esta Diretiva foi depois transposta para a ordem jurídica nacional pelo Decreto-Lei n.º 23/2009, de 20 de janeiro[252].

Essa mesma Diretiva só seria atualizada pelas instituições europeias 14 anos depois, já em 2019, através do Regulamento (UE) 2019/941, relativo à preparação para riscos no setor da eletricidade[253]. Este Regulamento impõe aos operadores do subsetor da eletricidade a necessidade de realizarem avaliações de risco para a segurança de abastecimento de eletricidade, e define também a metodologia a ser adotada para identificar cenários de crise de eletricidade a nível regional e nacional. Esta metodologia inclui a consideração de riscos como "as consequências de ataques maliciosos"[254] e de riscos relacionados com os "princípios que regem o tratamento de informações sensíveis"[255].

[249] Diretiva 2005/89/CE do Parlamento Europeu e do Conselho de 18 de janeiro de 2006 relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas, *Jornal Oficial da União Europeia*, 1, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005L0089.

[250] Diretiva 2005/89/CE, artigo 1.º.

[251] Diretiva 2005/89/CE, artigo 5.º, alínea d).

[252] Decreto-Lei n.º 23/2009, de 20 de janeiro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/23-2009-602570.

[253] Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho de 5 de junho de 2019 relativo à preparação para riscos no setor da eletricidade e que revoga a Diretiva 2005/89/CE, Jornal Oficial da União Europeia, 1, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0941.

[254] Regulamento (UE) 2019/941, artigo 5.º, n.º 2 alínea c).

[255] Regulamento (UE) 2019/941, artigo 5.º, n.º 3, alínea e).

### Subsetor do Petróleo

O subsetor do petróleo não é amplamente legislado em matéria de cibersegurança a nível setorial, estando principalmente sujeito aos diplomas de âmbito geral ou transversal sobre este tema. Existe, no entanto, a Diretiva 2012/18/UE, mais conhecida como Diretiva SEVESO III[256], relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas. Não incidindo especificamente sobre cibersegurança, esta Diretiva exige aos operadores que implementem uma Política de Prevenção de Acidentes Graves[257], um Sistema de Gestão de Segurança[258] e Planos de Emergência[259] em caso de acidente. Embora no ano de publicação da Diretiva o texto não incluísse menções à cibersegurança, os planos, políticas e sistemas exigidos devem ter em consideração os riscos de cibersegurança a que as organizações estejam ou possam vir a estar expostas. Esta Diretiva foi depois transposta para o ordenamento jurídico interno através do Decreto-Lei n.º 150/2015, de 5 de agosto[260].

### Subsetor do Gás

O subsetor do gás, tal como o do petróleo, também não s.e encontra amplamente regulado em matéria de cibersegurança. Contudo, neste subsetor, é de referir que foi publicado, em outubro de 2010, o Regulamento (UE) n.º 994/2010, relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás. Este Regulamento impunha aos operadores de gás a obrigação de realizarem avaliações de risco[261], nas quais poderiam ser também incluídos os riscos de cibersegurança. O Regulamento de 2010 foi depois atualizado em 2017, através do Regulamento (UE) 2017/1938, que, mantendo a imposição da realização de avaliações de risco, inclui entre os riscos específicos a considerar, as avarias de TIC, os ciberataques e a falta de manutenção adequada dos componentes tecnológicos[262].

---

[256] A Diretiva acolhe o nome “SEVESO” porque Seveso se refere a uma cidade do norte de Itália onde ocorreu um grave acidente industrial em 1976, no qual uma fábrica de produtos químicos libertou uma grande quantidade de dioxina, um composto altamente tóxico, contaminando a área circundante e afetando gravemente a saúde pública e o meio ambiente.

[257] Diretiva 2012/18/UE do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas, que altera e subsequentemente revoga a Diretiva 96/82/CE do Conselho, *Jornal Oficial da União Europeia*, artigo 8.º, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0018.

[258] Diretiva 2012/18/EU, artigo 8.º e Anexo III.

[259] Diretiva 2012/18/EU, artigo 12.º.

[260] Decreto-Lei n.º 150/2015, de 5 de agosto, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/150-2015-69951097.

[261] Regulamento (UE) n.º 994/2010 do Parlamento Europeu e do Conselho de 20 de Outubro de 2010 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga a Diretiva 2004/67/CE do Conselho, *Jornal Oficial da União Europeia*, artigo 9.º, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0001:0022:PT:PDF.

[262] Regulamento (UE) 2017/1938 8 do Parlamento Europeu e do Conselho de 25 de outubro de 2017 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010, *Jornal Oficial da União Europeia*, Anexo IV, n.º 3, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017R1938.

## Âmbito geral

No que diz respeito à legislação de âmbito geral para o setor da energia, um dos primeiros diplomas de relevo foi a Diretiva 2008/114/CE, de 8 de dezembro, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção[263]. Esta Diretiva estabeleceu as bases para a identificação dos operadores do setor da energia como operadores de infraestrutura crítica, e impôs-lhes obrigações como a elaboração de Planos de Segurança, nos quais deveriam já constar medidas relativas à segurança dos sistemas de informação[264]. Esta Diretiva foi transposta para a ordem jurídica interna portuguesa através do Decreto-Lei n.º 62/2011, de 9 de maio, entretanto atualizado pelo Decreto-Lei n.º 20/2022, de 28 de janeiro. O Decreto-Lei mais recente estabelece já que "as contramedidas e procedimentos de segurança permanentes" devem incluir "soluções em matéria de cibersegurança, nos termos previstos nos artigos 9.º e 10.º do Decreto-Lei n.º 65/2021, de 30 de julho"[265].

Para referir o Decreto-Lei n.º 65/2021, de 30 de julho, é importante referir a legislação que conduziu até ao mesmo. Em 2016, foi publicada a Diretiva (UE) 2016/1148, conhecida como Diretiva NIS. A sua transposição para o ordenamento jurídico interno, através da Lei n.º 46/2018, estabeleceu o Regime Jurídico da Segurança do Ciberespaço (RJSC) e que impôs diversas obrigações de cibersegurança à Administração Pública, Operadores de Infraestrutura Crítica e aos Operadores de Serviços Essenciais em análise neste relatório, entre outras entidades. De modo a melhor explicitar as obrigações de cibersegurança decorrentes do RJSC, foi publicado o Decreto-Lei n.º 65/2021, que o regulamenta. É então deste Decreto-Lei que decorrem as obrigações de nomear um ponto de contacto permanente junto do CNCS[266], de nomear um responsável de segurança[267], de realizar anualmente uma análise de risco de cibersegurança, de elaborar inventário de ativos[268] e um relatório anual[269] e de os submeter ao CNCS, e de implementar Planos de Segurança que contemplem a cibersegurança[270], bem como as obrigações de notificação dos incidentes de cibersegurança relevantes que impactem as operações destas entidades[271]. A Diretiva NIS e a legislação nacional desta decorrente estabelecem-se como os primeiros grandes atos legislativos em matéria de cibersegurança, tendo lançado as bases para mais e melhor legislação, tanto de âmbito setorial como de âmbito geral sobre essa matéria.

[263] Diretiva 2008/114/CE do Conselho de 8 de dezembro de 2008 relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção, *Jornal Oficial da União Europeia*, 1, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114.

[264] Diretiva 2008/114/CE, Anexo II, n.º 3.

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

[266] Decreto-Lei n.º 65/2021, artigo 4.º.

[267] Decreto-Lei n.º 65/2021, artigo 5.º.

[268] Decreto-Lei n.º 65/2021, artigo 6.º.

[269] Decreto-Lei n.º 65/2021, artigo 8.º.

[270] Decreto-Lei n.º 65/2021, artigo 7.º.

[271] Decreto-Lei n.º 65/2021, artigos 11.º a 15.º.

Volvidos seis anos após a publicação da Diretiva NIS, as instituições europeias publicaram a Diretiva (UE) 2022/2555[272], mais vulgarmente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: "setores de importância crítica"[273] e "outros setores críticos"[274]. Os setores já visados pela NIS 1 inserem-se nos setores de importância crítica. Dentro de alguns destes, são também abrangidos mais setores e subsetores. São também introduzidas novas obrigações.

Começando pela inclusão de novos setores, a Diretiva NIS 2 passa a visar também, no setor da energia, operadores de sistemas de aquecimento urbano ou sistemas de arrefecimento urbano, bem como operadores de produção, armazenamento e transporte de hidrogénio[275]. 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[276]. 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[277].

A nova Diretiva encoraja ainda a que as entidades abrangidas estabeleçam, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como as relacionadas com "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[278].

[272] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), *Jornal Oficial da União Europeia*, 80, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285

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

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

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

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

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

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

## 1.6. Standards e boas práticas aplicáveis

Sendo o setor da energia vital ao nível económico e social, é fundamental que a sua disponibilidade não fique comprometida. Para tal, e tal como a Diretiva NIS prevê, foram desenvolvidas várias políticas e *standards* que criam e asseguram uma rede energética europeia transversal e sustentável. No caso da Diretiva NIS, dentro do setor da Energia, são distinguidos três subsetores: Eletricidade, Gás e Petróleo.

***Standards* e boas práticas do subsetor da Eletricidade**

No subsetor da eletricidade, a empresas de geração, distribuição e transmissão de energia adotam uma abordagem baseada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsetor da Eletricidade[279]:

**Tabela 8 - Standards e Boas Práticas (Subsetor Eletricidade)**

| *Standards* | Boas práticas |
|---|---|
| • ISO 27019;<br>• NERC CIP Series;<br>• IEE Standard 1402-2000;<br>• IEC 61850. | • Cybersecurity model electricity subsector cybersecurity capability maturity model (esc2m2) – U.S. Department of Energy;<br>• NISTR 7628 – Guidelines for Smart Grid Cyber Security: Vol. 1;<br>• ENISA Appropriate security measures for Smart Grids – ENISA. |

[279] ENISA, “Mapping of OES Security Requirements to Specific Sectors”, 18 de Janeiro de 2018, 9, https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.

Na tabela anterior estão os *standards* e boas práticas referentes ao subsetor da eletricidade. De seguida, apresenta-se um breve sumário de cada um:

- **ISO 27019:** Fornece diretrizes para a segurança da informação nos sistemas de controlo industrial da energia[280];
- **NERC CIP Series:** Estabelece uma série de normas e requisitos para a segurança das infraestruturas críticas do setor de energia[281];
- **IEE Standard 1402-2000:** É uma norma para a avaliação e seleção de sistemas de proteção contra incêndios nas estações elétricas[282];
- **IEC 61850:** É uma norma internacional que define um padrão para a comunicação de estações elétricas e sistemas de automatização de redes elétricas[283];
- **Cybersecurity model electricity subsector cybersecurity capability maturity model (esc2m2) – U.S. Department of Energy:** É uma ferramenta que ajuda as organizações a avaliar e melhorar as suas capacidades de cibersegurança[284];
- **NISTR 7628 – Guidelines for Smart Grid Cyber Security: Vol. 1:** Fornece orientações de cibersegurança nos sistemas de energia inteligentes[285];
- **ENISA Appropriate security measures for Smart Grids – ENISA:** Fornece orientações de cibersegurança nos sistemas de energia inteligentes[286].

***Standards* e boas práticas do subsetor do Petróleo**

No subsetor do petróleo, a empresas de exploração, refinação e distribuição de petróleo seguem uma abordagem fundamentada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*, para salvaguardar as suas operações contra incidentes de cibersegurança e assegurar a integridade dos seus sistemas de controlo e automatização.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsetor do Petróleo[287]:

**Tabela 9 - Standards e Boas Práticas (Subsetor Petróleo)**

| *Standards* | Boas práticas |
|---|---|
| • Chemical Facility Anti-Terrorism Standards (CFATS). | • API STD 1164 - Pipeline SCADA Security;<br>• Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2). |

[280] ISO, "ISO/IEC 27019:2017", https://www.iso.org/standard/68091.html.

[281] NERC, "Standards", https://www.nerc.com/pa/Stand/Pages/Default.aspx.

[282] IEEE, "IEEE Guide for Physical Security of Electric Power Substations", https://standards.ieee.org/ieee/1402/6050/.

[283] IEC, "Find out more about IEC 61850", https://iec61850.dvl.iec.ch/.

[284] Department of Homeland Security, "ELECTRICITY SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ES-C2M2)", fevereiro de 2014, 1, https://www.energy.gov/oe/articles/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014.

[285] NIST, "Guidelines for Smart Grid Cybersecurity", https://csrc.nist.gov/pubs/ir/7628/r1/final.

[286] ENISA, "Appropriate security measures for smart grids", dezembro de 2012, https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids.

[287] ENISA, "Mapping of OES Security Requirements to Specific Sectors", 14.

Na tabela anterior estão os *standards* e boas práticas referentes ao subsetor do Petróleo. De seguida, apresenta-se um breve sumário de cada um:

- **Chemical Facility Anti-Terrorism Standards (CFATS):** São regulamentos dos EUA destinados a proteger instalações que lidam com substâncias químicas perigosas[288];
- **API STD 1164 - Pipeline SCADA Security:** Estabelece diretrizes para a segurança de sistemas de controlo e de automatização (SCADA) nos oleodutos[289];
- **Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2):** É uma ferramenta desenvolvida para ajudar organizações do setor do petróleo e do gás a avaliar e melhorar a sua postura de cibersegurança[290].

### *Standards* e boas práticas do subsetor do Gás

No subsetor do gás, a empresas de exploração, transporte e distribuição adotam uma abordagem fundamentada em padrões internacionais de segurança, como a ISO 27001 e a *NIST Cybersecurity Framework*, para salvaguardar as suas operações contra incidentes de cibersegurança e assegurar a integridade dos seus sistemas de controlo e automatização.

A tabela seguinte sumariza os *standards* e boas práticas aplicados ao subsetor do Gás[291]:

**Tabela 10 - Standards e Boas Práticas (Subsetor Gás)**

| *Standards* | Boas práticas |
|---|---|
| • Chemical Facility Anti-Terrorism Standards (CFATS). | • API STD 1164 - Pipeline SCADA Security;<br>• Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2);<br>• GIE - Gas Infrastructure Europe Security Risk Assessment Methodology;<br>• Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA). |

[288] Kansas Adjutant General's Department, "Chemical Facility Antiterrorism Standards (CFATS)", https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard.
[289] API, "API Standard 1164, 3rd Edition", https://www.api.org/products-and-services/standards/important-standards-announcements/1164.
[290] U.S. Department of Homeland Security, "OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)", fevereiro de 2014, https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014.
[291] ENISA, "Mapping of OES Security Requirements to Specific Sectors", 14.

Na tabela anterior estão os *standards* e boas práticas referentes ao subsetor do Gás. De seguida, apresenta-se um breve sumário de cada um:

- **Chemical Facility Anti-Terrorism Standards (CFATS):** São regulamentos dos EUA destinados a proteger instalações que lidam com substâncias químicas perigos[292];
- **API STD 1164 - Pipeline SCADA Security:** Estabelece diretrizes para a segurança de sistemas de controlo e de automatização (SCADA) nos oleodutos[293];
- **Oil and Natural Gas subsector cybersecurity capability maturity model - (ONG-C2M2):** É uma ferramenta desenvolvida para ajudar organizações do setor do petróleo e do gás a avaliar e melhorar a sua postura de cibersegurança[294];
- **GIE - Gas Infrastructure Europe Security Risk Assessment Methodology:** É uma *framework* projetada para ajudar os operadores das infraestruturas de gás a avaliar e gerir os riscos de segurança[295];
- **Control Systems Cyber Security Guidelines for the Natural Gas Pipeline Industry - Interstate Natural Gas Association of America (INGAA):** É um conjunto de melhores práticas para proteger sistemas de controlo em *pipelines* de gás natural[296].

[292] Kansas Adjutant General's Department, "Chemical Facility Antiterrorism Standards (CFATS)", https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard.

[293] API, "API Standard 1164, 3rd Edition", https://www.api.org/products-and-services/standards/important-standards-announcements/1164.

[294] U.S. Department of Homeland Security, "OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)", fevereiro de 2014, https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014.

[295] GIE, "Security Risk Assessment Methodology", https://www.gie.eu/wp-content/uploads/filr/2751/GIE_Security_Risk_Assessment_Methodology_May2015.pdf.

[296] AGA, "NATURAL GAS CYBERSECURITY GUIDELINES & STANDARDS PORTFOLIO", março de 2017, 1, https://www.aga.org/wp-content/uploads/2022/11/ong_cybersecurity_guidelines_and_standards_002.pdf.

## 1.7. Desafios

Embora alguns países incluídos no estudo "*Sectorial Implementation of the NIS Directive in the Energy Sector"*, antes do aparecimento da Diretiva NIS, tivessem já as suas abordagens desenvolvidas, outros desenvolveram novas metodologias nela baseadas. As abordagens foram ajustadas e trabalhadas com o objetivo de estarem crescentemente harmonizadas com a Diretiva[297].

Para determinar os critérios de identificação dos OSE, os Estados-Membros tiveram em consideração várias fontes, entre as quais:

1) Discussões/reuniões com especialistas (37%);
2) Dados públicos sobre o setor (19%);
3) Estatísticas nacionais (17%)
4) Dados de cada setor através de parcerias público-privadas (17%);
5) Outros (10%).

Existem duas abordagens seguidas para identificação dos OSE[298]:

**Tabela 11 - Abordagem para identificação de OSE**

| Abordagem Estatal (73%) | Abordagem orientada pelo operador (27%) |
|---|---|
| O papel de liderança é assumido por uma ou mais agências governamentais/ministérios que têm a responsabilidade de identificar os Serviços Essenciais e OSE - na maioria dos casos, os próprios ministérios responsáveis. | Os operadores autoavaliam-se quanto ao cumprimento de critérios específicos e, em seguida, registam-se na lista de OSE. Esta abordagem não exija que as autoridades nacionais identifiquem os operadores individuais das infraestruturas críticas – é dever dos operadores notificar as autoridades quando se enquadram nos critérios predefinidos. |

Para a identificação de OSE no setor da energia, existem diferentes metodologias seguidas pelos Estados-Membros. Um mesmo Estado-Membro pode decidir seguir uma ou mais metodologias para este processo de identificação no setor energético. A preferida e utilizada pela maioria (13 Estados-Membros) diz respeito à identificação dos OSE (de um modo global) e a segunda metodologia mais escolhida baseia-se na identificação de infraestruturas críticas da Diretiva ECI (*European Critical Infrastructures*) (8). Entre outras metodologias seguidas, encontram-se as análises de risco nacionais (4) e os exercícios/formações (1)[299].

[297] NIS Cooperation Group, "Sectorial implementation of the NIS Directive in the Energy sector", outubro de 2019, 4, https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf.
[298] NIS Cooperation Group, "Sectorial implementation of the NIS Directive in the Energy sector", outubro de 2019, 29.
[299] NIS Cooperation Group, "Sectorial implementation of the NIS Directive in the Energy sector", outubro de 2019, 28.

Observa-se um aumento de incidentes de cibersegurança no setor de energia, que podem causar impactos significativos para a sociedade e economia – devido às características dos serviços prestados –, gerar multas regulatórias e prejudicar significativamente a reputação das empresas, em virtude de possíveis paralisações parciais ou totais dos serviços[300] [301].

**Subsetor da Eletricidade**

Segundo o Relatório "*Sectorial Implementation of the NIS Directive in the Energy Sector"*, e para a maioria dos inquiridos, o critério mais importante para identificar um OSE no subsetor da eletricidade corresponde ao número de pessoas que dependem dos serviços, de acordo com 11 Estados-Membros. Como segundo e terceiro critérios, com igual valor (apontado por 9 Estados-Membros), encontra-se a prestação de um serviço dependendo da rede e sistemas de informação e a quantidade de serviços ou bens produzidos, tal como os critérios de avaliação de importância para a economia como sociedade[302].

O relatório "Cyber-Physical Security Considerations for the Electricity Sub-Sector" indica que, à medida que este subsetor adota tecnologias avançadas, como dispositivos de monitorização, controlo e *IoT*, aumentam as vulnerabilidades. Primeiramente, o subsetor enfrenta riscos significativos no que diz respeito à proteção de cibersegurança dos sistemas SCADA. Estes sistemas, são essenciais para a monitorização e operação das redes, tornam-se vulneráveis a ataques que exploram falhas de segurança nestas tecnologias. Ataques, como os de *ransomware*, podem explorar *VPNs* e sistemas SCADA para aceder a pontos críticos da infraestrutura.

A segurança física das infraestruturas é também um desafio, principalmente para as subestações distribuídas geograficamente e expostas a invasões físicas e sabotagem. A utilização de dispositivos de pequeno porte, como *drones*, possibilita ataques físicos que evitam os sistemas de segurança convencionais. Além disso, a gestão da cadeia de abastecimento é crucial, pois a aquisição de componentes para os *ICS* e *SCADA* depende da segurança dos fornecedores. Se um componente for comprometido, este pode impactar a segurança do sistema, principalmente se estiver amplamente distribuído no setor.

Outro desafio importante é a proteção dos dispositivos de *IoT*, que são amplamente integrados nos sistemas de monitorização e controlo. Estes dispositivos possuem vulnerabilidades específicas relacionadas com *design* e configuração, sendo críticos em casos onde o *software* não recebe atualizações de segurança. Tais falhas tornam o sistema suscetível a invasões que comprometam a integridade dos dados e a segurança da rede, ressaltando a importância de práticas de cibersegurança robustas, como o isolamento das redes e um controlo rigoroso de acessos remotos.

Para mitigar estes desafios, o relatório recomenda práticas como o fortalecimento dos padrões de segurança, monitorização contínuo das redes e a colaboração entre as equipas de segurança física e de cibersegurança[303].

[300] PwC, "A leadership agenda to take on tomorrow", março de 2024, 7, https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf.

[301] CNCS, "Riscos & Conflitos 2024", 33, https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf.

[302] NIS Cooperation Group, "Sectorial implementation of the NIS Directive in the Energy sector", outubro de 2019, 31.

[303] CISA, "SECTOR SPOTLIGHT: Cyber-Physical Security Considerations for the Electricity Sub-Sector", novembro de 2022, 1-2, https://www.cisa.gov/sites/default/files/2022-11/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf.

**Subsetores do Petróleo e do Gás**

Também de acordo com o Relatório "*Sectorial Implementation of the NIS Directive in the Energy Sector"*, para a maioria dos inquiridos, os dois critérios mais importantes para a identificação dos OSE no subsetor do petróleo é a prestação de um serviço dependente da rede e dos sistemas de informação, bem como a quantidade de serviço ou bem produzido (indicado por 9 Estados-Membros). Já no subsetor do Gás, para a maioria dos inquiridos, os dois critérios mais importantes para a identificação dos OSE é o número de pessoas que dependem dos serviços (indicado por 11 Estados-Membros) e, de seguida, a importância para a economia e atividades sociais, tamanho da entidade e quantidade de bens produzidos ou transportados (referido por 9 Estados-Membros).

Ainda de acordo com o mesmo relatório, para a maioria dos inquiridos, o critério mais importante de identificação de um OSE no subsetor do gás é a prestação de um serviço dependente de redes e sistemas de informação (12) e depois segue-se a sua importância para a economia (9). Como terceiro critério, surge a quantidade de bens ou serviços produzidos.

A Repsol reconhece os riscos de cibersegurança associados ao aumento da digitalização e à evolução das ameaças, incluindo fatores geopolíticos e avanços na IA. Para enfrentar estes desafios, a empresa implementou um Modelo Operacional de Cibersegurança focado na resiliência dos sistemas e atualiza regularmente os planos estratégicos. Em 2023, não ocorreram incidentes significativos de cibersegurança, graças a processos avançados de deteção e a mais de 50 iniciativas, como avaliações da postura de cibersegurança e otimizações dos processos de resposta a incidentes[304].

O setor do petróleo e gás enfrentam desafios críticos de cibersegurança, sobretudo devido à sua complexa infraestrutura digital. A operação integrada das redes industriais, sistemas de controlo e equipamentos digitais expõem estes subsetores a ameaças crescentes. Um incidente de cibersegurança pode impactar tanto a segurança dos trabalhadores como o meio ambiente, além de provocar perdas financeiras significativas e uma interrupção da produção. O foco em ciberresiliência passa por criar defesas robustas e adotar estratégias de recuperação rápidas e eficientes. Isto incluí proteger as redes e os dados sensíveis, assim monitorizar continuamente as ameaças emergentes, bem como promover a formação contínua dos profissionais para que reconheçam os riscos potenciais e ajam proactivamente. Estes esforços são fundamentais para reduzir vulnerabilidades e garantir a segurança das operações numa escala global[305].

Os ativos estão frequentemente distribuídos em vastas áreas geográficas, incluindo locais *offshore* remotos e profundos, onde muitos dos equipamentos são antigos e carecem de recursos de segurança modernos, tornando-os alvos vulneráveis. A integração dos sistemas de fornecedores e as dificuldades em estabelecer redes seguras nas plataformas também contribuem para que exista uma superfície de ataque. Os desafios operacionais incluem a necessidade de manter os sistemas num funcionamento contínuo, onde as interrupções podem causar perdas financeiras elevadas. O foco na eficiência operacional frequentemente precede as atualizações de segurança. Por outro lado, os desafios financeiros surgem devido à alta regulamentação e elevados custos da indústria, enquanto os desafios legislativos refletem a falta de normas rigorosas comparadas aos outros OSE, dificultando a proteção efetiva contra incidentes de segurança[306].

[304] Repsol, "Integrated Management Report 2023", 108.
[305] World Economic Forum, "Strengthening cybersecurity in the oil and gas industry", janeiro de 2023, www.weforum.org/impact/cyber-resilience-oil-and-gas/.
[306] Abubakar Sadiq Mohammed et al., "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022, 16-18, https://dl.acm.org/doi/10.1145/3548691.

De acordo com o Instituto Nacional de Padrões e Tecnologia (NIST) dos EUA, os sistemas de GNL são particularmente vulneráveis a ciberataques devido a riscos intrínsecos, como a dependência de sistemas de terceiros geridos remotamente e tecnologias a bordo vulneráveis, como *PLCs*, *GPS* e *AIS*. Os incidentes de cibersegurança podem resultar em riscos de segurança graves, incluindo fugas de tanques de combustível e libertação de GNL. As ameaças internas são outra preocupação significativa. Aumentar a consciencialização em cibersegurança dos colaboradores é crucial, uma vez que os ataques começam, frequentemente, com a confiança comprometida de funcionários[307].

A integração dos sistemas de fornecedores e as dificuldades em estabelecer redes seguras nas plataformas também contribuem para que exista uma superfície de ataque. Os desafios operacionais incluem a necessidade de manter os sistemas num funcionamento contínuo, onde as interrupções podem causar perdas financeiras elevadas. O foco na eficiência operacional frequentemente precede as atualizações de segurança. Por outro lado, os desafios financeiros surgem devido à alta regulamentação e elevados custos da indústria, enquanto os desafios legislativos refletem a falta de normas rigorosas comparadas aos outros OSE, dificultando a proteção efetiva contra incidentes de segurança[308].

[307] Gas-cybersecurity, “Cybersecurity in the Energy Sector, Gas Subsector”, https://www.gas-cybersecurity.com/.

[308] Abubakar Sadiq Mohammed et al., “Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective”, setembro de 2022, 16-18.

## 1.8. Recomendações

Segundo o relatório da ENISA que descreve as ameaças contra os serviços dos fornecedores de energia que dependem da disponibilidade de redes precisas em tempo e comunicação[309], as recomendações e boas práticas de segurança a seguir pelo setor dividem-se em recomendações gerais a aplicar e recomendações técnicas baseadas em diferentes cenários tecnológicos.

Técnicas baseadas em cenários tecnológicos:

1. **Unidades de Medida de Fase** (*phasor measurement units* (PMU), no original), são dispositivos críticos na monitorização da rede elétrica em tempo real. Permitem medir a voltagem e a corrente de um sistema de energia e são essenciais para o controlo eficiente e seguro da rede. Contudo, estas unidades podem ser alvos de incidentes de cibersegurança, como intrusões que comprometam a integridade dos dados recolhidos ou até mesmo a operação das PMUs.
    i) **Estabelecer perímetros de segurança eletrónica**: A recomendação de estabelecer perímetros de segurança para PMUs ajuda a isolar estas unidades de redes mais amplas e protegê-las contra acessos não autorizados. Com um perímetro bem definido, é possível controlar rigorosamente quem pode, e o que pode interagir com as PMUs, reduzindo o risco de incidentes de cibersegurança que poderiam manipular os dados ou sabotar o funcionamento do sistema;
    ii) **Minimizar a quantidade de pontos de acesso eletrónicos**: Reduzir os pontos de acesso minimiza as possibilidades de exploração por atacantes. Quanto menor o número de pontos de entrada, mais fácil é monitorizar e proteger cada um deles;
    iii) **Utilizar segregação de rede**: Implementar segregação da rede, com a criação de zonas de segurança distintas para PMUs, ajuda a limitar os danos caso um agente de ameaça consiga comprometer um dispositivo ou componente da rede garantindo que um possível incidente não se espalhe para outras partes da infraestrutura crítica;
    iv) **Utilizar *firewalls* com "*whitelist*" (negar, *by default*):** A utilização de *firewalls* com regras de "*whitelist*" faz com que apenas dispositivos ou endereços IP específicos consigam estabelecer conexões com as PMUs, restringindo severamente as tentativas de acesso, pois, por defeito, todas as conexões não autorizadas são bloqueadas.
    v) **Implementar IPSec nos dispositivos de *gateway*:** Implementar IPSec nas interfaces de rede dos dispositivos de *gateway* permite a encriptação e autenticação de dados de forma robusta, protegendo contra ataques do tipo *man-in-the-middle*, onde um agente de ameaça interceta ou altera a comunicação entre a PMU e outras partes do sistema.

[309] ENISA, "Power Sector Dependencies on Time Service", 2020.

b) **Camada de transporte (TCP/UDP):** responsável pela comunicação entre dispositivos na rede, podem ser exploradas por agentes de ameaça para comprometer a integridade e confidencialidade dos dados que transitam entre os dispositivos.
   i) **Fecho de portas não utilizadas:** É uma prática fundamental para reduzir a superfície de ataque, onde cada porta aberta num dispositivo ou servidor representa uma possível vulnerabilidade. Ao fechar portas desnecessárias, a organização minimiza as oportunidades para os atacantes explorarem o sistema.
   ii) ***Firewalls* com regras de "*whitelist*":** Semelhante à recomendação anterior, a aplicação de *firewalls* com listas de permissões ajudam a garantir que somente comunicações legítimas possam circular pela rede,
   iii) **Ligações VPN encriptadas:** O uso de VPNs com encriptação assegura que os dados trocados entre sistemas e utilizadores remotos sejam protegidos de intercetação ou alteração por terceiros, principalmente em cenários de comunicação remota ou externa à infraestrutura.
   iv) **Evitar ligações bidirecionais remotas e implementar SSH quando necessário**: Manter ligações remotas unidimensionais, onde a comunicação apenas pode ocorrer de dentro para fora, limita a possibilidade de intrusões ou comandos maliciosos enviados para dentro da rede. Caso a comunicação bidirecional seja necessária, deve ser implementado o uso de protocolos seguros, como o *SSH* (*Secure Shell*), para garantir a segurança na transmissão dos dados.

c) **Servidor e protocolo NTP/PTP**: O *Network Time Protocol* (*NTP*) e o *PTP* são fundamentais para a sincronização dos relógios nos sistemas. A precisão do tempo é essencial para garantir o funcionamento coordenado de diversos dispositivos e processos em tempo real, como é o caso das PMUs.
   i) **Utilizar criptografia para dados sensíveis:** Protege a integridade e confidencialidade dos dados, prevenindo que informações críticas, como *timestamps,* sejam manipuladas.
   *ii)* **Harmonizar sistemas temporais *Universal Time Coordinated* (UTC) para facilitar correlação de dados:** Ao utilizar uma base de tempo unificada, como o *UTC* (*Coordinated Universal Time*), facilita-se a correlação de dados na rede, o que é fundamental para a deteção de anomalias ou falhas. Caso sistemas diferentes utilizem tempos diferentes poderá dificultar a identificação de eventuais problemas.
   iii) **Utilizar *Access Control Lists* (ACLs), assim como *firewalls* para filtrar ligações a servidores NTP:** O uso de *ACLs* e *firewalls* ajuda a filtrar e limitar as conexões de rede ao servidor NTP, garantindo que apenas dispositivos autorizados possam solicitar a sincronização de tempo, protegendo contra ataques de *DoS* (*Denial of Service*).
   iv) **Proteger o protocolo NTP com vários caminhos entre os relógios *master* e *slave*:** Utilizar múltiplos caminhos entre relógios *master* e *slave* oferece redundância e aumenta a segurança do sistema visto que, se um caminho for comprometido ou sofrer uma falha, a sincronização do tempo pode ser mantida através de outros caminhos, garantindo a precisão e confiabilidade da rede.

A “Recomendação (UE) 2019/553 da Comissão de 3 de abril de 2019 sobre a cibersegurança no setor da energia”, constitui um documento vital na consolidação de recomendações a adotar por parte deste setor e a definir as principais questões relacionadas com a cibersegurança. Este documento considera determinadas realidades[310]:

1) o progresso tecnológico de redes (inteligentes) energéticas alavanca exposição a novos riscos;
2) a reformulação do Regulamento Mercado Interno da Eletricidade considera agora a adoção de normas técnicas para a eletricidade;
3) a importância e necessidade de avaliar continuamente e de modo adequado todos os riscos;
4) a priorização do reforço da ciber-resiliência: adoção da Diretiva NIS;
5) a comunicação de incidentes como obrigatória nos setores essenciais, como a energia;
6) o reforço, pretendido pela Comissão Europeia, de partilha de informação entre partes interessadas através de eventos específicos em matéria de cibersegurança;
7) Os Estados-membros são responsáveis por “assegurar que todas as partes interessadas (operadores de redes de energia, fornecedores de tecnologias e OSE identificados pela NIS) aplicam as medidas de preparação que se impõem em matéria de cibersegurança, relacionadas com os requisitos em tempo real”, tais como:
    a) aplicação das normas de segurança mais atualizadas nas instalações e, caso necessário, aplicação de medidas de segurança física complementares caso medidas de cibersegurança não sejam suficientes;
    b) aplicar normas internacionais em contexto de cibersegurança;
    c) aplicar restrições em tempo real, em particular na classificação de ativos;
    d) garantir o nível de qualidade de serviço requerido pelas restrições em tempo real, através da implementação de redes privadas para sistemas de proteção à distância;
    e) atribuir diferentes zonas lógicas num sistema global e, para cada zona, atribuir critérios de tempo e processos;
    f) escolher protocolos de comunicação seguros;
    g) adotar mecanismos de autenticação adequados para qualquer comunicação.

[310] Comissão Europeia, Direção-Geral da Energia, Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.

O documento destaca, também, algumas recomendações que podem mitigar os “efeitos de cascata”. Isto significa que, uma vez que as redes elétricas e gasodutos na Europa se encontram fortemente independentes, deve ser garantida uma comunicação transversal com todas as partes interessadas num momento de crise ou incidentes de cibersegurança - um ciberataque capaz de criar falhas ou perturbações num sistema energético, pode, direta ou indiretamente, ser responsável por provocar efeitos em cascata com grande alcance no restante sistema. Neste contexto, algumas das recomendações a ser seguidas pelos operadores de rede de energia são, por exemplo, as seguintes[311]:

1) garantir que todos os novos dispositivos IoT têm nível de segurança adequado;
2) ponderar efeitos ciberfísicos no momento de revisão periódica dos planos de continuidade;
3) estabelecer critérios de conceção e uma arquitetura para uma rede resiliente.

O documento foi redigido considerando que o setor está atualmente exposto a “mudanças como o progresso tecnológico, acoplamento de setores e a digitalização”, tornando as redes elétricas cada vez mais inteligentes.

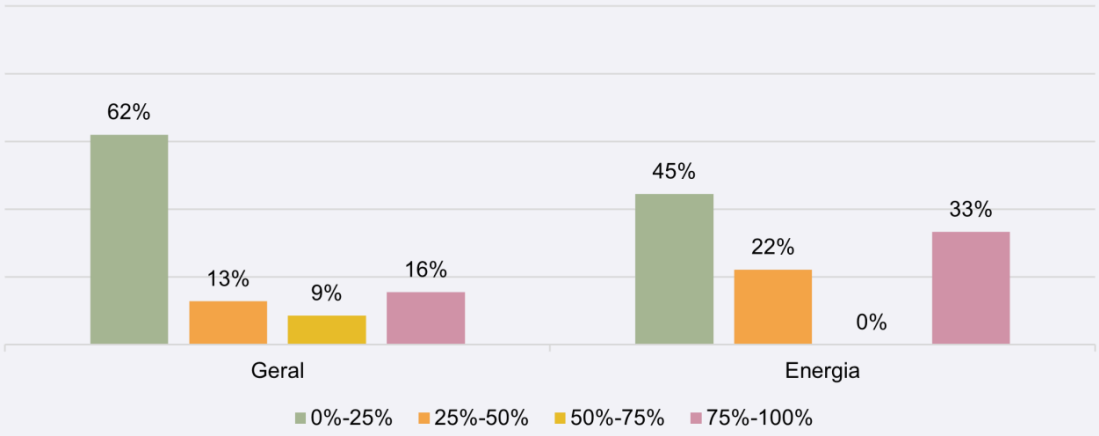
Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da energia e subsequentes subsetores, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

[311] Comissão Europeia, Direção-Geral da Energia, Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.

## Formação

A sensibilização para todo o tipo de riscos de cibersegurança e a formação para identificar possíveis tentativas de ataques de segurança são essenciais para impedir que estas se concretizem, pois, a formação leva a que medidas de prevenção, como a realização de *backups*, sejam implementadas. A formação (**Gráfico 33**) nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Podemos verificar que o setor da energia tem uma percentagem maior de trabalhadores com formação básica em cibersegurança comparativamente com o geral. Apesar disso, 45% dos operadores tem uma percentagem aproximada de trabalhadores com formação básica em cibersegurança de 0 a 25%, um valor considerado baixo e que deve ser aumentado.

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



Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor da energia disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), metade das formações são de caráter facultativo, e não obrigatório (**Gráfico 39**).

**Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores**

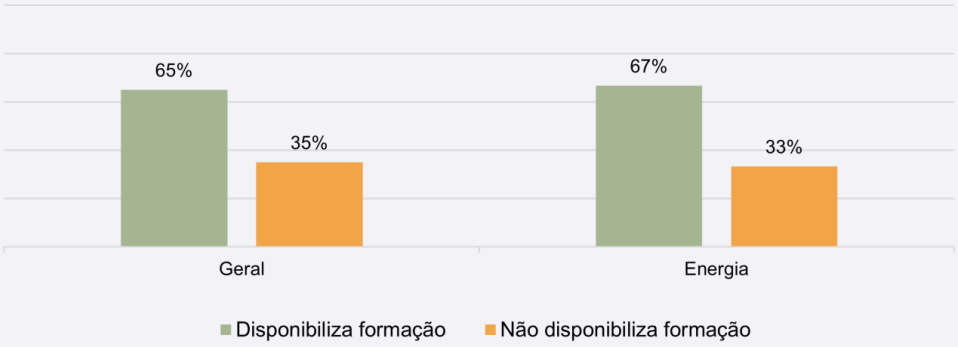
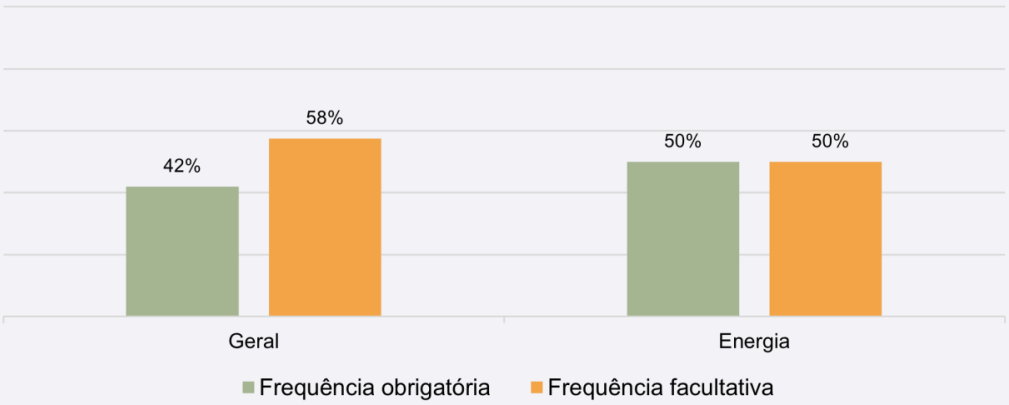
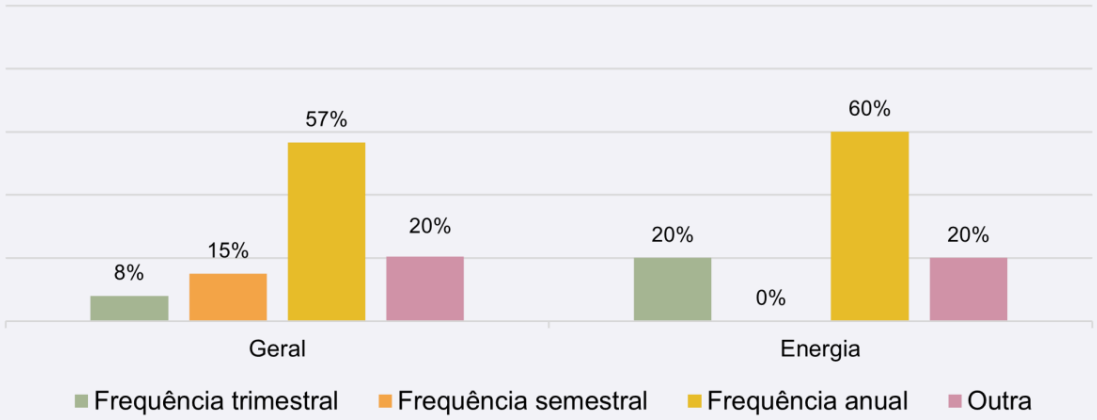



**Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa**



Além disso, na maioria das entidades, os momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor da energia poderá ser insuficiente para assegurar a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores. Assim sendo, recomenda-se que os momentos de formação para a sensibilização dos colaboradores ocorram semestralmente e que a participação nos mesmos seja obrigatória.

**Gráfico 41 - Frequência média dos momentos de formação**




**Medidas de proteção contra ameaças de cibersegurança**

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que o setor da energia, comparativamente com os restantes, é um dos setores onde menos se utiliza sistemas de gestão de *passwords*, a utilização de *browser* que proteja a privacidade, controlos biométricos para identificação e autenticação de utilizadores e *VPN*.

Nesse sentido, recomenda-se aos OSE do setor da energia que:

- Aumentem a equipa de especialistas em cibersegurança;
- Realizem análises de risco com periodicidade mínima anual;
- Implementem sistemas de gestão de *passwords*;
- Implementem *VPN* em, pelo menos, acessos remotos;
- Implementem, onde possível, métodos de autenticação multifator.

Medidas como estas auxiliam a impedir acessos iniciais por parte dos agentes de ameaça e a que os mesmos não sejam capazes de progredir na exploração dos dados, sistemas e ficheiros quando um primeiro acesso é obtido.

**Políticas, procedimentos e planos de cibersegurança**

De acordo com os dados obtidos no questionário, todos os OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança. Adicionalmente, apenas 67% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

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

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

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

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

Quanto à realização de testes de intrusão, 72% dos OSE realizam os mesmos, estando a percentagem acima do geral (72% vs 50%). É importante a realização deste tipo de testes, pois é mais uma maneira de identificar vulnerabilidades, corrigi-las e tornar os OSE mais resilientes em matéria de cibersegurança.

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

- **Controlos básicos**: controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais**: controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches* proteção contra *malware* e *browsers*;
- **Controlos organizacionais**: controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de intrusão e exercícios de *Red Team*[312].

[312] Hassanzadeh et al., “A Review of Cybersecurity Incidents”, 4.

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos[313]:

**Tabela 12 - Controlos de Segurança da CIS (Energia)**

| Categoria | Controlo de segurança |
|---|---|
| **Controlos básicos** | Inventário e Controlo de Ativos |
| | Inventário e Controlo de Ativos de *Software* |
| | Proteção de Dados |
| | Configuração Segura de Ativos e *Software* |
| | Gestão de Contas |
| | Gestão de Controlo de Acessos |
| | Gestão Contínua de Vulnerabilidades |
| | Gestão de Logs de Auditoria |
| **Controlos fundacionais** | Proteções de *e-mail* e de Navegadores |
| | Defesas Contra *Malware* |
| | Recuperação de Dados |
| | Gestão da Infraestrutura de Rede |
| | Monitorização e Defesa da Rede |
| **Controlos organizacionais** | Formação e Consciencialização em Segurança |
| | Gestão de Fornecedores de Serviços |
| | Segurança de Aplicações de *Software* |
| | Gestão e Resposta a Incidentes |
| | Testes de Penetração |

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

313 Hassanzadeh et al., "A Review of Cybersecurity Incidents", 6.

**Recomendações Subsetor da Eletricidade**

Um relatório da Comissão Europeia em conjunto com a ENISA dá conta de quatro recomendações para o subsetor da eletricidade:

1. A postura de cibersegurança e a resiliência podem ser melhoradas através de boas práticas para mitigar o *ransomware*, monitorizar possíveis vulnerabilidades, garantir a segurança dos recursos humanos e gerir ativos. É, também, necessário reforçar a cooperação com a rede técnica dos Estados-Membros, as CSIRTs, as autoridades policiais e parceiros internacionais. Adicionalmente, os Estados-Membros devem realizar autoavaliações para o subsetor da eletricidade, de acordo com a Diretiva 2022/2555[314] e a Diretiva relativa à resiliência das entidades críticas[315];
2. É necessário melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
3. É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança;
4. Deve ser reforçada a cibersegurança das cadeias de abastecimento com avaliações das dependências dos fornecedores de alto risco[316].

[314] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022L2555.

[315] Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557.

[316] European Commission, "Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors", 24 de julho de 2024, https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors.

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

**Tabela 13 - Cenários de risco (Eletricidade)**

| Cenários de risco |
| --- |
| **Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis.** Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial. |
| **Comprometimento de serviços *WEB*,** através de um *URL* malicioso ou *script* malicioso que direciona um colaborador da entidade para um website falso e instala *software* malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados. |
| **Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis**, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador. |
| Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL Injection ou Cross-site Scripting). |
| **Negação de serviço distribuído (DDoS)** a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate. |
| **FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade**, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade. |
| **VIOLAÇÃO DE DADOS** da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão. |
| ***RANSOMWARE*** que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público. |

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf)

**Recomendações Subsetor do Petróleo**

Um estudo sobre a cibersegurança dos sistemas físicos nos subsetores do petróleo e gás indica que a implementação da *IoT* e de sistemas controlados remotamente têm aumentado as vulnerabilidades nestes subsetores. Para mitigar estes riscos, é fundamental aprimorar determinadas situações, tais como:

- Melhorar os sistemas de deteção de intrusões (*IDS*) para atender melhor às necessidades específicas dos subsetores do petróleo e gás, pois os sistemas existentes são limitados;
- Substituir os protocolos *ModbusRTU* e *ModbusTCP* que são considerados inseguros;
- Melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
- É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança[317].

[317] Abubakar Sadiq Mohammed et al, "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022, 22.

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

**Tabela 14 - Cenários de risco (Petróleo)**

| Cenários de risco |
| --- |
| **Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis.** Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial. |
| **Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis**, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador. |
| Intrusão em base de dados de clientes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (SQL Injection ou Cross-site Scripting). |
| **VIOLAÇÃO DE DADOS** da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão. |
| **Infeção com *software* malicioso que conecta os dispositivos da entidade a uma BOTNET**, tornando-os zombies, fornecendo poder computacional a ataques de DDoS e de criptomineração, ou comprometendo os sistemas e/ou serviços (ex: RDP, FTP) através de tentativa de força-bruta. |
| ***RANSOMWARE*** que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público. |

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf)

**Recomendações Subsetor do Gás**

Um estudo sobre a cibersegurança dos sistemas físicos nos subsetores do petróleo e gás indica que a implementação da *IoT* e de sistemas controlados remotamente têm aumentado as vulnerabilidades nestes subsetores. Para mitigar estes riscos, é fundamental aprimorar determinadas situações, tais como:

- Melhorar os sistemas de deteção de intrusões (*IDS*) para atender melhor às necessidades específicas dos subsetores do petróleo e gás, pois os sistemas existentes são limitados;
- Substituir os protocolos *ModbusRTU* e *ModbusTCP* que são considerados inseguros;
- Melhorar a consistência de cibersegurança e a partilha de informações entre entidades;
- É necessário criar um plano de contingência, de gestão de crise e de colaboração operacional em caso de incidente de cibersegurança[318].

[318] Abubakar Sadiq Mohammed et al, "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022, 22.

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

**Tabela 15 - Cenários de risco (Gás).**

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

(Fonte: CNCS, “Riscos & Conflitos 2021”, última atualização em 21 de outubro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurança-cncs.pdf).

# Notas metodológicas

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

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

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

# Bibliografia


- Accenture, “Fast forward: accelerating the journey to reinvention”. https://www.accenture.com/content/dam/accenture/final/a-com-migration/r3-3/pdf/pdf-157/accenture-fast-forward-accelerating-the-journey-to-reinvention.pdf.
- Almeida, Gonçalo. “Preço da eletricidade dispara para novo máximo. Já subiu 115% com a guerra”. CNN Portugal, 6 de março de 2022. https://cnnportugal.iol.pt/geral/eletricidade-em-portugal-atinge-novo-maximo-historico-segunda-feira-preco-subiu-115-com-a-guerra/20220306/6224b6bc0cf2cc58e7e70a67.
- Alphonsus, Ryan e Mohammad Abdullah. “A review on the applications of programmable logic controllers (PLCs)”, julho de 2016. https://www.sciencedirect.com/science/article/abs/pii/S1364032116000551.
- American Gas Association. “Natural Gas Cybersecurity Guidelines & Standards Portfolio”, março de 2017. https://www.aga.org/wp-content/uploads/2022/11/ong_cybersecurity_guidelines_and_standards_002.pdf.
- 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.
- API, “API Standard 1164, 3rd Edition”. https://www.api.org/products-and-services/standards/important-standards-announcements/1164.
- ARC Advisory Group, “Oil & Gas Operations Technology and Supplier Selection”. https://www.arcweb.com/technology-evaluation-and-selection/oil-gas-operations-technology-supplier-selection.
- Arkadiusz Hulewicz, Zbigniew Krawiecki e Krzysztof Dziarski, “Distributed control system DCS using a PLC controller”, 15 de julho de 2019. https://www.itm-conferences.org/articles/itmconf/pdf/2019/05/itmconf_zkwe2019_01041.pdf.
- Arne Björnberg e Ann Phang, “Euro Health Consumer Index 2018”, Health Consumer Powerhouse, 2019. https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf
- Associação Portuguesa de Empresas de Gás, “Utilização Doméstica”. https://www.apeg.pt/gas-natural/utilizacao-domestica/.
- Associação Portuguesa de Empresas de Gás, “Utilização na Indústria”. https://www.apeg.pt/gas-natural/industria/.
- Associação Portuguesa de Empresas de Gás, “Utilização no setor da mobilidade”. https://www.apeg.pt/gas-natural/utilizacao-no-setor-da-mobilidade/.
- Associação Portuguesa de Empresas de Gás, “Utilização no Terciário”. https://www.apeg.pt/gas-natural/setor-terciario/.
- Associação Portuguesa de Empresas de Gás, “Utilizações e Vantagens”. https://www.apeg.pt/gas-natural/utilizacoes-vantagens/.

- AVEVA, “AVEVA Predictive Analytics”, 2023. https://www.aveva.com/content/dam/aveva/documents/brochures/Brochure_AVEVA_PredictiveAnalytics_23-02.pdf.
- Banco de Portugal, “Economia numa imagem”, março de 2022. https://www.bportugal.pt/page/economia-numa-imagem-148-0.
- BIP, “INESC TEC e EDP assinam contrato-programa na área de energia”, junho de 2019. https://bip.inesctec.pt/noticias/inesc-tec-e-edp-assinam-contrato-programa-na-area-de-energia/.
- Boaz, Lawrence Shubi Kaijage and Ramadhani Sinde. “An overview of pipeline leak detection and location systems”, julho de 2014. https://ieeexplore.ieee.org/abstract/document/7055147.
- Caixa Geral de Depósitos, “Relatório de Gestão e Contas 2023”. https://www.cgd.pt/Investor-Relations/Informacao-Financeira/CGD/Relatorios-Contas/Pages/Relatorios-Contas-CGD.aspx.
- Castaño, David, Daniel Marcos, Ana Fonseca e Pedro Lains. Os Petróleos em Portugal: Do Estado à Privatização 1937-2012. Lisboa: Imprensa de Ciências Sociais, 2017.
- CatimProjetos, “Green Pipeline Project”. https://www.projetoscatim.com/projects-green-pipeline.
- Center for Internet Security. “The 18 CIS Critical Security Controls”, CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- CGI, “Endesa aposta na transformação digital e reinventa o seu modelo de negócio”. https://www.cgi.com/portugal/pt-pt/case-study/business-consulting/endesa-aposta-na-transformacao-digital-e-reinventa-o-seu-modelo-de.
- Chen, Bo, Nishant Pattanaik, Ana Goulart, Karen L. Butler-Purry, Deepa Kundur. “Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed”, 25 de junho de 2015. https://ieeexplore.ieee.org/abstract/document/7129084.
- CISA, “Cyber-Attack Against Ukrainian Critical Infrastructure”, 20 de julho de 2021. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01.
- CISA, “The Attack on Colonial Pipeline: What We’ve Learned & What We’ve Done Over the Past Two Years”, 7 de maio de 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
- CISA. “Sector Spotlight: Cyber-Physical Security Considerations for the Electricity Sub-Sector”, novembro de 2022. https://www.cisa.gov/sites/default/files/2022-11/Sector%20Spotlight%20Cyber-Physical%20Security%20Considerations%20Electricity%20Sub-Sector%20508%20compliant.pdf.
- 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, “Incidentes e Setores”, Conhecimento Situacional: Estatísticas. https://www.cncs.gov.pt/pt/estatistica/#cert.pt.
- CNCS, “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”, maio de 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.
- CNCS, ISAC. https://www.cncs.gov.pt/pt/isac/.
- CNCS, ISAC. https://www.cncs.gov.pt/pt/isac/.

- Colégio Nacional de Energia e Minas, "O petróleo nas nossas vidas. Com excepção da água, o petróleo é o líquido mais presente nas nossas vidas", Ingenium, II Série, n.º 158 (março/abril de 2017).
- Comissão Europeia. "€1.3 billion from the Digital Europe Programme for Europe's digital transition and cybersecurity". https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity.
- Comissão Europeia. "Risk assessment report on cyber resilience on EU's telecommunications and electricity sectors", 24 de julho de 2024. https://digital-strategy.ec.europa.eu/en/news/risk-assessment-report-cyber-resilience-eus-telecommunications-and-electricity-sectors.
- Compete 2030, "Europa lidera combate à emergência climática", 8 de julho de 2024. https://www.compete2030.gov.pt/comunicacao/europa-lidera-combate-a-emergencia-climatica/.
- Conselho Europeu, "Horizonte Europa". https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Correia, Rafael. "Acordo de Paris pode criar oito milhões de empregos na energia até 2050". Revista Sustentável, 30 de julho de 2021. https://www.revistasustentavel.pt/destaques/acordo-de-paris-pode-criar-oito-milhoes-de-empregos-na-energia-ate-2050/.
- Decreto-Lei n.º 150/2015, de 5 de agosto, Diário da República. https://diariodarepublica.pt/dr/detalhe/decreto-lei/150-2015-69951097.
- Decreto-Lei n.º 23/2009, de 20 de janeiro, Diário da República. https://diariodarepublica.pt/dr/detalhe/decreto-lei/23-2009-602570.
- Decreto-Lei n.º 65/2021, de 30 de julho, Diário da República. https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.
- Dehlawi, Zakariya e Norah Abokhodair. "Saudi Arabia's response to cyber conflict: A case study of the Shamoon malware incident". Paper apresentado na 2013 IEEE International Conference on Intelligence and Security Informatics, junho de 2013. https://www.researchgate.net/publication/261456882_Saudi_Arabia's_response_to_cyber_conflict_A_case_study_of_the_Shamoon_malware_incident.
- Department for Science, Innovation & Technology, "Cyber security breaches survey 2023", 19 de abril de 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
- Department of Homeland Security. "Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)", fevereiro de 2014. https://www.energy.gov/oe/articles/electricity-subsector-cybersecurity-capability-maturity-model-v-11-february-2014.
- Direção-Geral de Energia e Geologia, "Estratégia Nacional de Longo Prazo para o Combate à Pobreza Energética 2023-2050". https://www.dgeg.gov.pt/pt/areas-transversais/relacoes-internacionais/politica-energetica/estrategia-nacional-de-longo-prazo-para-o-combate-a-pobreza-energetica/.
- Direção-Geral de Energia e Geologia, "História da Prospeção e Pesquisa". https://www.dgeg.gov.pt/pt/areas-setoriais/geologia/petroleo-armazenamento-de-co2/geologia-do-petroleo/historia-da-prospecao-e-pesquisa/.
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285

- Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2557.
- Diretiva (UE) 2023/1791 do Parlamento Europeu e do Conselho, de 13 de setembro de 2023, relativa à eficiência energética e que altera o Regulamento (UE) 2023/955. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32023L1791.
- Diretiva 2005/89/CE do Parlamento Europeu e do Conselho de 18 de janeiro de 2006 relativa a medidas destinadas a garantir a segurança do fornecimento de eletricidade e o investimento em infraestruturas, Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32005L0089.
- Diretiva 2012/18/UE do Parlamento Europeu e do Conselho de 4 de julho de 2012 relativa ao controlo dos perigos associados a acidentes graves que envolvem substâncias perigosas, que altera e subsequentemente revoga a Diretiva 96/82/CE do Conselho, Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32012L0018.
- ECS, “Energy Networks and Smart Grids”, novembro de 2018. https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf.
- EDP. “A nossa transformação digital”, Inovação na EDP. https://www.edp.com/pt-pt/inovacao/transformacao-digital.
- EDP. “AI4PV”. https://www.edp.com/pt-pt/inovacao/new/ai4pv.
- EDP. “ARIA 2”. https://www.edp.com/pt-pt/inovacao/aria-2.
- EDP. “BEHYOND: sinergias entre o hidrogénio e a eólica offshore”. https://www.edp.com/pt-pt/inovacao/behyond-sinergias-entre-o-hidrogenio-e-a-eolica-offshore.
- EDP. “BladeBug: Inspeção e Manutenção de Turbinas Eólicas”. https://www.edp.com/pt-pt/edp-group/bladebug-inspecao-e-manutencao-de-turbinas-eolicas.
- EDP. “Cyber Range: Promover a sensibilização da cibersegurança”, julho de 2020. https://www.edp.com/sites/default/files/2021-03/10_cyber_range_novo_PT.pdf.
- EDP. “FIRMe: Flexibilidade Integrada em Regime de Mercado”. https://www.edp.com/pt-pt/edp-group/firme-flexibilidade-integrada-em-regime-de-mercado.
- EDP. “Inovação na EDP”. https://www.edp.com/pt-pt/inovacao.
- EDP. “IONATE”. https://www.edp.com/pt-pt/inovacao/ionate.
- EDP. “O que é a transição energética e qual o impacto na forma como vivemos?”. https://www.edp.com/pt-pt/o-que-e-a-transicao-energetica-e-qual-o-impacto-na-forma-como-vivemos.
- EDP. “Parte I – Relatório de Gestão 2023”, setembro de 2024. https://www.edp.com/sites/default/files/2024-09/Parte%20I%20-%20Relat%C3%B3rio%20de%20Gest%C3%A3o%202023.pdf.
- EDP. “Pobreza Energética em Portugal”. Histórias EDP, 16 de março de 2021. https://www.edp.com/pt-pt/historias-edp/pobreza-energetica-em-portugal.
- EDP. “PRR Be Neutral – Ubiquitous Charging”. https://www.edp.com/pt-pt/innovation/prr-be-neutral-ubiquitous-charging.
- EDP. “Uma história de dois séculos: Portugal acende a primeira lâmpada”, Histórias EDP, 14 de agosto de 2019. https://www.edp.com/pt-pt/historias-edp/uma-historia-de-dois-seculos-portugal-acende-a-primeira-lampada.
- Empowering EU ISACs, “European ISACs”. https://www.isacs.eu/european-isacs.
- ENISA. “Appropriate security measures for smart grids”, dezembro de 2012. https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids.
- ENISA. “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. “Cybersecurity Skills Conference: Strengthening human capital in the EU”. https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.
- ENISA. “ENISA Threat Landscape 2023”, 19 de outubro de 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.
- ENISA. “Mapping of OES Security Requirements to Specific Sectors”, 18 de janeiro de 2018. https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.
- ENISA. “NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist”, 11 de dezembro de 2020, https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
- ENISA. “NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist”, 11 de dezembro de 2020, https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
- ENISA. “NIS Investments”, 2021. https://www.enisa.europa.eu/publications/nis-investments-2021.
- ENISA. “NIS Investments”, 2022. https://www.enisa.europa.eu/publications/nis-investments-2022.
- ENISA. “NIS Investments”, 2023. https://www.enisa.europa.eu/publications/nis-investments-2023.
- Epcol. “Repsol contrata novo grupo de colaboradores e lança curso com o IEFP para os formar”, 17 de março de 2022. https://www.epcol.pt/noticias-das-associadas/repsol-contrata-novo-grupo-de-colaboradores-e-lanca-curso-com-o-iefp-para-os-formar/1236.
- E-Redes. “Cybersecurity: New challenges, the same priority”. https://www.e-redes.pt/en/networks-of-future/cybersecurity/cybersecurity.
- E-Redes. “Plano de Desenvolvimento e Investimento da Rede de Distribuição: Período 2021-2025”. https://www.erse.pt/media/0wji5213/anexo-i_j-proposta-ren-portg%C3%A1s-distribui%C3%A7%C3%A3o.pdf.
- ERSE, “Caracterização do Sector do Gás Natural em Portugal”, janeiro de 2007. https://provedordocliente.edp.pt/Files/PDF/Caracteriza%C3%A7%C3%A3o%20do%20Sector%20do%20G%C3%A1s%20Natural%20em%20Portugal.pdf.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”. https://www.ee-isac.eu/impact/#.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), “Impact”. https://www.ee-isac.eu/impact/#.
- Eurostat. “Electricity price statistics”. Dados extraídos em outubro de 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Electricity_price_statistics#Electricity_prices_for_household_consumers.
- Eurostat. “New indicator on annual average salaries in the EU”, 19 de dezembro de 2022. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/DDN-20221219-3.
- Eurostat. “Renewable energy statistics”. dados relativos a 2022, extraídos em dezembro de 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Renewable_energy_statistics.
- Executive Digest. “Quais são as empresas com maior volume de negócios em Lisboa?”, Executive Digest, 25 de agosto de 2023. https://executivedigest.sapo.pt/noticias/quais-sao-as-empresas-com-maior-volume-de-negocios-em-lisboa/?doing_wp_cron=1709902761.2706060409545898437500.

- Federal Trade Commission. Equifax Data Breach Settlement", fevereiro de 2024. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.
- ForeNova, "Cyber Threat Analysis Done the Right Way". https://www.forenova.com/threat-detection/how-to-conduct-a-cyber-threat-analysis.
- Fortinet, "What is OT Security?". https://www.fortinet.com/solutions/industries/scada-industrial-control-systems/what-is-ot-security.
- Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", janeiro de 2024.
- Francisco de la Fuente Sanchéz, entrevistado por Jorge Branco em "Eletrificação total do território", ISCTE, 2013, https://repositorio.iscte-iul.pt/bitstream/10071/6095/1/Eletrifica%c3%a7%c3%a3o%20total%20do%20territ%c3%b3rio.pdf.
- Fundação Galp Energia. "Gás A História Natural". https://www.fundacaogalp.com/Portals/1/Documentos/livro-gas-a-historia-natural.pdf.
- Galp. "As nossas raízes: cronologia ilustrada". https://www.galp.com/corp/pt/sobre-nos/a-galp/as-nossas-raizes.
- Galp. "Galp e empresas de energia unidas contra ciber-ataques no Fórum Económico Mundial", 25 de maio de 2022. https://www.galp.com/media/comunicados-de-imprensa/comunicado/id/1351/galp-e-empresas-de-energia-unidas-contra-ciber-ataques-no-forum-economico-mundial.
- GALP. "Parte 1: Relatório Integrado de Gestão 2023". https://www.galp.com/corp/Portals/0/Recursos/Investidores/IMR2023/PT/RelatorioIntegradoAnual2023HQ.pdf.
- Gas Infrastructure Europe. "Security Risk Assessment Methodology", maio de 2015. https://www.gie.eu/wp-content/uploads/filr/2751/GIE_Security_Risk_Assessment_Methodology_May2015.pdf.
- Gas-cybersecurity, "Cybersecurity in the Energy Sector, Gas Subsector". https://www.gas-cybersecurity.com/.
- Guerra, Ana. "IBM e Galp juntas em projeto de Inteligência Artificial". Ntech.news, 12 de julho de 2018. https://www.ntech.news/ibm-e-galp-juntas-em-projeto-de-inteligencia-artificial/.
- Han, Mingyu and Peter Crossle. "Vulnerability of IEEE 1588 under Time Synchronization Attacks", 4 de agosto de 2019. https://ieeexplore.ieee.org/abstract/document/8973494.
- Hassanzadeh, Amin, Amin 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.
- HYFUELUP. "Shaping a better tomorrow with renewable natural gas". https://hyfuelup.eu/.
- IEC. "Find out more about IEC 61850". https://iec61850.dvl.iec.ch/.
- IEEE. "IEEE Guide for Physical Security of Electric Power Substations". https://standards.ieee.org/ieee/1402/6050/.
- IEEE. "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", 24 de julho de 2008. https://standards.ieee.org/ieee/1588/4355/.
- IEFP. "Cheque-Formação + Digital". https://www.iefp.pt/cheque-formacao-digital.
- 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.
- Ingrams Time Systems, "Master & Slave Systems". https://www.ingrams.com.au/master-and-slave-systems.
- IPCC. "Framing and Context". https://www.ipcc.ch/sr15/chapter/chapter-1/.
- Irani, Zahir, Raul Abril, Vishanth Weerakkody, Amizan Omar e Uthayasankar Sivarajah. "The impact of legacy systems on digital transformation in European public administration: Lesson

learned from a multi case analysis". Government Information Quarterly vol. 40, n.º 1, janeiro de 2023. https://www.sciencedirect.com/science/article/pii/S0740624X22001204.
- ISO, "ISO/IEC 27001:2022". https://www.iso.org/standard/27001.
- ISO. "ISO/IEC 27019:2017". https://www.iso.org/standard/68091.html.
- Kansas Adjutant General's Department, "Chemical Facility Antiterrorism Standards (CFATS)". https://www.kansastag.gov/310/Chemical-Facility-Antiterrorism-Standard.
- Kelly, Stephanie e Jessica Resnick-ault. "One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators". Reuters, 9 de junho de 2021. https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/.
- Kim Zetter, "Meet 'Flame', The Massive Spy Malware Infiltrating Iranian Computers", Wired, 28 de maio de 2012. https://www.wired.com/2012/05/flame/.
- Lei n.º 46/2018, de 13 de agosto, Diário da República. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- Lusa. "'Portugal desperdiça todos os anos várias barragens do Alqueva' em fugas de água", Público, 6 de maio de 2023. https://www.publico.pt/2023/05/06/azul/noticia/portugal-desperdica-anos-varias-barragens-alqueva-fugas-agua-2048583.
- Marktest. "Gás canalizado: penetração aumenta mas não chega à maioria da população", Marktest, 11 de dezembro de 2018. https://www.marktest.com/wap/a/n/id~2470.aspx.
- Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- Mohammed, Abubakar e et al., "Cybersecurity Challenges in the Offshore Oil and Gas Industry: An Industrial Cyber-Physical Systems (ICPS) Perspective", setembro de 2022. https://dl.acm.org/doi/10.1145/3548691.
- NAVIA. "Business & Operations Intelligence", Porquê o NAVIA. https://www.naviasolutions.com/porque-o-navia/.
- NERC, "Standards". https://www.nerc.com/pa/Stand/Pages/Default.aspx.
- Neto, Rita. "Gás natural dispara 55% e bate recorde com guerra na Ucrânia", Eco, 2 de março de 2022. https://eco.sapo.pt/2022/03/02/gas-natural-dispara-55-para-recorde-de-194-euros-por-mwh/.
- NIS Cooperation Group. "Sectorial implementation of the NIS Directive in the Energy sector", outubro de 2019. https://smart-lighting.es/wp-content/uploads/2019/11/SectorialimplementationoftheNISDirectiveintheEnergysectorpdf.pdf.
- NIST. "Guidelines for Smart Grid Cybersecurity". https://csrc.nist.gov/pubs/ir/7628/r1/final.
- Nokia. "Best Master Clock Algorithm". https://infocenter.nokia.com/public/7705SAR234R1A/index.jsp?topic=%2Fcom.nokia.basic-system-guide%2Fbest-master-clock-algorithm.html.
- NTSB. "Pipeline Rupture and Subsequent Fire in Bellingham, Washington". https://www.ntsb.gov/investigations/AccidentReports/Reports/PAR0202.pdf.
- Oliveira, Ana. "Dependência europeia de combustíveis fósseis subiu em 2022. Portugal fica ligeiramente abaixo dos 70%". ECO, 30 de janeiro de 2024. https://eco.sapo.pt/2024/01/30/dependencia-europeia-de-combustiveis-fosseis-subiu-em-2022-portugal-fica-ligeiramente-abaixo-dos-70/.
- Oliveira, Ana. "Emprego nas renováveis cresce a pique com solar a brilhar. E os "fósseis"?". CNN Portugal, 22 de julho de 2023. https://cnnportugal.iol.pt/energia/energias-renovaveis/emprego-nas-renovaveis-cresce-a-pique-com-solar-a-brilhar-e-os-fosseis/20230722/64b902ccd34e72171a0b5971.
- Pacific Maritime Magazine. "European Oil Port Terminals Crippled by Cyberattack and Ransomware". https://pacmar.com/article/european-oil-port-terminals-crippled-by-cyberattack-and-ransomware/.

- Parian, Christopher, Terry Guldimann, Sajal Bhatia. “Fooling the Master: Exploiting Weaknesses in the Modbus Protocol”. https://www.sciencedirect.com/science/article/pii/S1877050920312576.
- PORDATA. “Consumo de energia elétrica: total e por tipo de consumo”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica__total_e_por_tipo_de_consumo.xlsx.
- PORDATA. “Consumo de energia primária: total e por tipo de fonte de energia”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-09/PORTUGAL_314.xlsx.
- PORDATA. “Consumo energético das famílias: total e por alguns produtos energéticos”, maio de 2024. https://www.pordata.pt/sites/default/files/202406/Portugal_Consumo_energetico_das_familias__total_e_por_alguns_produtos_energeticos.xlsx.
- PORDATA. “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- PORDATA. “Importações de energia: total e por principais países de origem”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Importacoes-de-energia-por-principais-paises-de-origem.xlsx.
- PORDATA. “População empregada: total e por setor de atividade económica. Quantas pessoas trabalham na agricultura, indústria, comércio ou outros serviços?”, Indicador: Eletricidade, gás e água, 2023. https://www.pordata.pt/portugal/populacao+empregada+total+e+por+setor+de+atividade+economica-3384-304037.
- PORDATA. “Preços médios de venda ao público dos combustíveis líquidos e gasosos - Continente”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Precos_medios_de_venda_ao_publico_dos_combustiveis_liquidos_e_gasosos_-_Continente.xlsx.
- PORDATA. “Produção bruta de energia elétrica: total e por tipo de produção de energia elétrica”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-eletrica-por-fonte-de-energia.xlsx.
- PORDATA. “Produção de energia elétrica a partir de fontes renováveis (%)”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-10/Portugal_Producao-de-energia-eletrica-a-partir-de-fontes-renovaveis-percentagem.xlsx.
- PORDATA. “Produção de energia elétrica: total e a partir de fontes renováveis”, outubro de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Consumo_de_energia_eletrica__total_e_por_tipo_de_consumo.xlsx.
- PORDATA. “Venda de combustíveis para consumo”, maio de 2024. https://www.pordata.pt/sites/default/files/2024-06/Portugal_Venda_de_combustiveis_para_consumo.xlsx.
- Portugal Energia. “Plano Nacional Energia e Clima 2021-2030”. https://www.portugalenergia.pt/setor-energetico/bloco-3/.
- PORTUGAL.GOV.PT. “Estratégia de Longo Prazo de Combate à Pobreza Energética aprovada em Conselho de Ministros”, 23 de novembro de 2023. https://www.portugal.gov.pt/pt/gc23/comunicacao/comunicado?i=estrategia-de-longo-prazo-de-combate-a-pobreza-energetica-aprovada-em-conselho-de-ministros.
- Prado, Miguel. “EDP: imune à crise, mas não aos hackers”. Expresso, 18 de abril de 2020. https://expresso.pt/economia/2020-04-18-EDP-imune-a-crise-mas-nao-aos-hackers.
- PwC. “A leadership agenda to take on tomorrow”, março de 2024. https://www.pwc.com/gx/en/ceo-survey/2021/reports/pwc-24th-global-ceo-survey.pdf.
- Rankia. “Cotação Galp Energia”. https://www.rankia.pt/cotacoe/galp-energia/.
- Recomendação (UE) 2019/553 da Comissão de 3 de Abril de 2019 sobre a cibersegurança no setor da energia, 2019.

- Recuperar Portugal. “Investimento RE-C01-i06: Transição Digital da Saúde (300 M€)”, 8 de junho de 2021. https://recuperarportugal.gov.pt/2021/06/08/investimento-re-c01-i06/.
- Redutskiy, Yury. “Optimization of Safety Instrumented System Design and Maintenance Frequency for Oil and Gas Industry Processes”, março de 2017. https://www.researchgate.net/publication/315971691_Optimization_of_Safety_Instrumented_System_Design_and_Maintenance_Frequency_for_Oil_and_Gas_Industry_Processes.
- Regulamento (UE) 2017/1938 8 do Parlamento Europeu e do Conselho de 25 de outubro de 2017 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga o Regulamento (UE) n.º 994/2010. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32017R1938.
- Regulamento (UE) 2019/941 do Parlamento Europeu e do Conselho de 5 de junho de 2019 relativo à preparação para riscos no setor da eletricidade e que revoga a Diretiva 2005/89/CE. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019R0941.
- Regulamento (UE) n.º 994/2010 do Parlamento Europeu e do Conselho de 20 de outubro de 2010 relativo a medidas destinadas a garantir a segurança do aprovisionamento de gás e que revoga a Diretiva 2004/67/CE do Conselho. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:295:0001:0022:PT:PDF.
- REN. “Produção de energia renovável bate recorde em 2023”, 2 de janeiro de 2024. https://www.ren.pt/pt-pt/media/noticias/producao-de-energia-renovavel-bate-recorde-em-2023.
- Repsol. “Formação”. https://sines.repsol.pt/pt/comunidade/seguranca/formacao/index.cshtml.
- Repsol. “Gás natural e gás propano e butano - conheça as diferenças”. https://www.repsol.pt/particulares/assessoramento/gas-natural-e-gas-propano-e-butano/.
- Repsol. “Integrated Management Report 2023”. https://www.repsol.com/content/dam/repsol-corporate/en_gb/accionistas-e-inversores/informes-anuales/2023/integrated-management-report-2023.pdf.
- Resolução do Conselho de Ministros n.º 11/2024, Diário da República, 8 de janeiro de 2024. https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/11-2024-836222486.
- RISI. “CIA Trojan Causes Siberian Gas Pipeline Explosion”. https://www.risidata.com/index.php?/Database/Detail/cia-trojan-causes-siberian-gas-pipeline-explosion.
- RISI. “Hacker Takes Over Russian Gas System”. https://www.risidata.com/Database/Detail/hacker-takes-over-russian-gas-system.
- RTP. “Introdução do gás natural em Portugal”, 25 de setembro de 1990. https://arquivos.rtp.pt/conteudos/introducao-do-gas-natural-em-portugal/.
- SCADA INFO. “SCADA and Energy Management System”. https://www.scadainfo.com/scada-and-energy-management-system/.
- Securing Legacy OT Systems: Challenges and Strategies”, Security Boulevard, 24 de abril de 2023. https://securityboulevard.com/2023/04/securing-legacy-ot-systems-challenges-and-strategies/.
- Security Magazine. “GALP dá mais um passo na sua segurança e integra rede nacional CSIRT”, 20 de julho de 2021. https://www.securitymagazine.pt/2021/07/20/galp-da-mais-um-passo-na-sua-seguranca-e-integra-rede-nacional-csirt/.
- Security Magazine. “Galp Energia mantém segurança dos serviços críticos com plataforma xDR com M365 E5”, 6 de setembro de 2024. https://www.securitymagazine.pt/2024/09/06/galp-energia-mantem-seguranca-dos-servicos-criticos-com-plataforma-xdr-com-m365-e5/.
- Silva, Douglas, Caio Catarina e Eric Batlle. “Advanced oil recovery associated with carbon capture and storage”. Research, Society and Development, vol. 11, n.º 1, janeiro de 2022. http://dx.doi.org/10.33448/rsd-v11i1.24599.
- Sulaiman Asif. “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, Knowledge Hut, 5 de setembro de 2023. https://www.knowledgehut.com/blog/security/threat-analysis.

- The New York Times, “Hackers Attacked california Power”, 10 de junho de 2001. https://www.nytimes.com/2001/06/10/us/hackers-attacked-california-power.html.
- TORRES VEDRAS WEB. “História da Exploração Petrolífera em Portugal: Avanços e Desafios na Indústria”, 14 de fevereiro de 2024. https://torresvedrasweb.pt/historia-da-exploracao-petrolifera-em-portugal-avancos-e-desafios-na-industria/.
- U.S. Department of Homeland Security, “OIL AND NATURAL GAS SUBSECTOR CYBERSECURITY CAPABILITY MATURITY MODEL (ONG-C2M2)”, fevereiro de 2014. https://www.energy.gov/oe/articles/oil-and-natural-gas-subsector-cybersecurity-capability-maturity-model-february-2014.
- Woodroof, Nicholas. “TOTEX: commercial creativity and the supply chain of the future”. OilField Technology, 12 de Agosto de 2019. https://www.oilfieldtechnology.com/special-reports/12082019/totex-commercial-creativity-and-the-supply-chain-of-the-future/.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.
- World Economic Forum, “Strengthening cybersecurity in the oil and gas industry”, janeiro de 2023. www.weforum.org/impact/cyber-resilience-oil-and-gas/.
- World Economic Forum. “Global Cybersecurity Outlook 2024”, janeiro de 2024. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

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