CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de **Cibersegurança**

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

Saúde

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 2016/1148[1] (também conhecida como Diretiva NIS), derivada da necessidade formalizada pelo Parlamento Europeu e Conselho da UE da implementação e harmonização de medidas destinadas a garantir um elevado nível de segurança das redes e da informação em toda a UE. Esta necessidade advém, desde logo, da necessidade de garantir a fiabilidade, a segurança e a confiança nas atividades económicas e societais e no mercado interno.

Assim, a Diretiva NIS tem por objetivo desenvolver as capacidades de cibersegurança em toda a União, mitigar os riscos associados às ameaças contra os sistemas de rede e informação utilizados para prestar serviços essenciais e garantir a continuidade de tais serviços perante incidentes. Pretende-se, portanto, contribuir para a segurança da União e para o eficaz funcionamento da sua economia e sociedade. A Diretiva NIS estabelece, entre outros, requisitos de segurança e de notificação para os Operadores de Serviços Essenciais (OSE), categorizando-os em setores e subsetores. No contexto português, esta Diretiva foi transposta através da Lei n.º 46/2018, de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço (RJSC).

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

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

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

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

A tabela seguinte elenca os setores de atividade nos quais os operadores podem ser classificados como OSE.

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

O presente relatório, decalcado do relatório geral sobre os OSE, analisa, individualmente, o setor da Saúde. O mesmo avalia o estado da cibersegurança no setor, debruçando-se sobre a sua história, as suas especificidades tecnológicas, ameaças no contexto cibersegurança, investimento realizado nesse mesmo contexto, e outros tópicos.

O relatório contém ainda recomendações para o setor, elaboradas com base nas conclusões retiradas sobre investimento, capacitação, ameaças identificadas e outros fatores que tenham sido destacados nas respostas obtidas ao questionário realizado pelo CNCS aos OSE deste setor. Embora o CNCS tenha preparado dois questionários – um para as entidades reguladoras de cada setor e outro para os OSE - não foi possível obter respostas de nenhuma entidade reguladora no setor da saúde, pelo que serão apenas apresentados os resultados conseguidos através do questionário destinado aos Operadores de Serviços Essenciais.

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 resulta 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 do Centro Nacional de Cibersegurança (CNCS).

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.

O presente relatório individual diz respeito apenas ao setor da Saúde.

Objetivos do relatório

Este relatório teve como principais objetivos:

- Identificar e avaliar o estado da cibersegurança em Portugal, no que diz respeito ao setor da Saúde, 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 do setor no país nas várias esferas em que incide a respetiva temática;
- Produzir um Relatório sobre o setor da Saúde que engloba a caracterização, regulamentação e recomendações, no âmbito do Observatório de Cibersegurança, de modo a mensurar o estado da cibersegurança nacional no setor no âmbito do RJSC;

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 uma breve análise sobre a nova Diretiva NIS 2, incidindo sobre as novas entidades abrangidas e sobre as novas obrigações face ao diploma.

Análise do questionário dirigido aos Operadores de Serviços Essenciais (OSE)

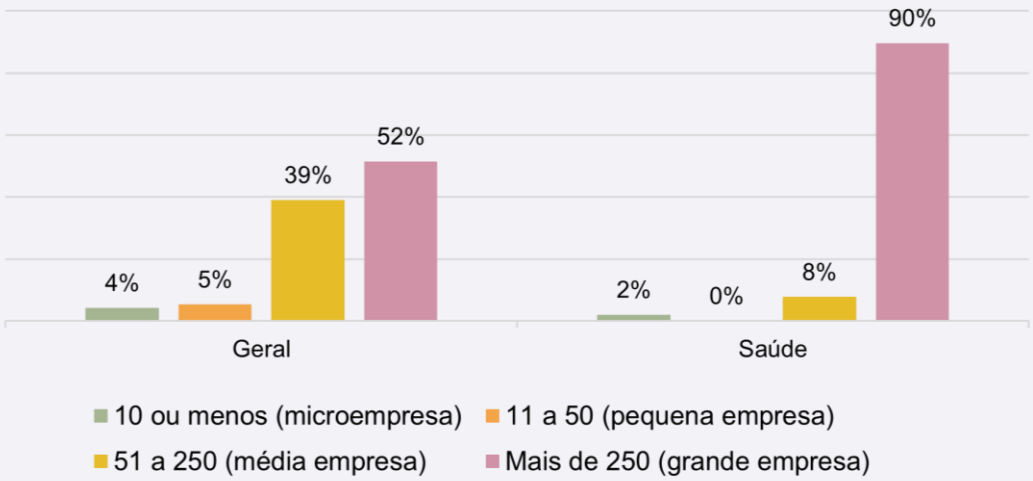
Tal como referido, no âmbito deste relatório, de modo a melhor conhecer e analisar o atual estado de cibersegurança nos setores relativos aos Operadores de Serviços Essenciais (OSE), foram elaborados dois questionários para auxiliar essa análise. O primeiro relatório foi dirigido às entidades reguladoras dos setores em questão, e o segundo aos próprios Operadores de Serviços Essenciais desses setores. No entanto, **no caso do setor da saúde, não houve qualquer entidade reguladora a responder ao questionário enviado**, pelo que neste relatório se apresentam apenas os resultados obtidos através do questionário dirigido aos OSE.

O questionário dirigido aos Operadores de Serviços Essenciais foi extenso, incidindo sobre as dimensões humanas, técnico-tecnológicas, processuais e de investimento ao nível da cibersegurança. As respostas ao questionário foram recolhidas entre 11 e 29 de setembro de 2023.

O questionário destinado aos Operadores de Serviços Essenciais foi partilhado, no total, 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.

Resultados do questionário dirigido aos Operadores de Serviços Essenciais

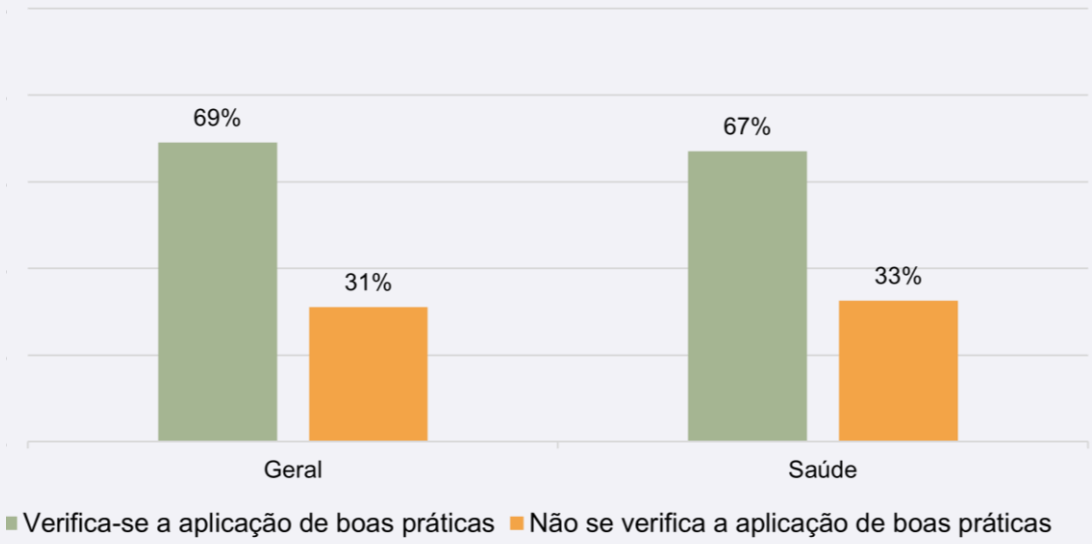
Gráfico 1 - Número de colaboradores na organização



O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas (4% e 5%, respetivamente). No setor da saúde, as grandes empresas são mais comuns, representando 90% das entidades, com apenas 8% sendo médias empresas e 2% microempresas. 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[4].

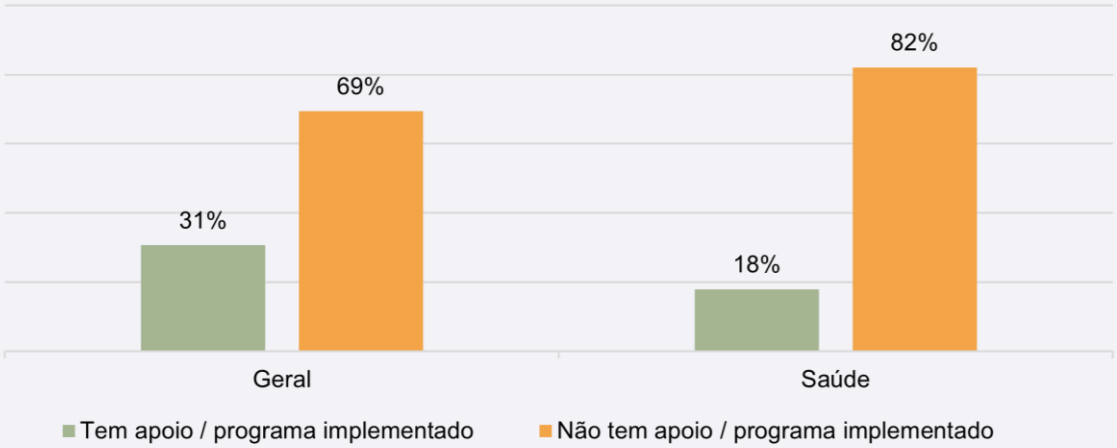
[4] PORDATA, "Empresas: total e por dimensão", dados de 2022, https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.

Gráfico 2 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



De um modo geral, os operadores percecionam a adoção de boas práticas de cibersegurança por parte dos seus colaboradores. Alguns exemplos dessas boas práticas são a não partilha de palavras-passe, o bloqueio do computador durante momentos de ausência da estação de trabalho, o cuidado com a informação confidencial do operador ou a denúncia de *e-mails* suspeitos/tentativas de *phishing*, entre outras. Na generalidade, dois terços dos operadores consideram que há uma efetiva adoção dessas boas práticas pelos seus colaboradores.
No setor da saúde a perceção de que estas boas práticas são aplicadas observa-se em 67% dos OSE inquiridos.

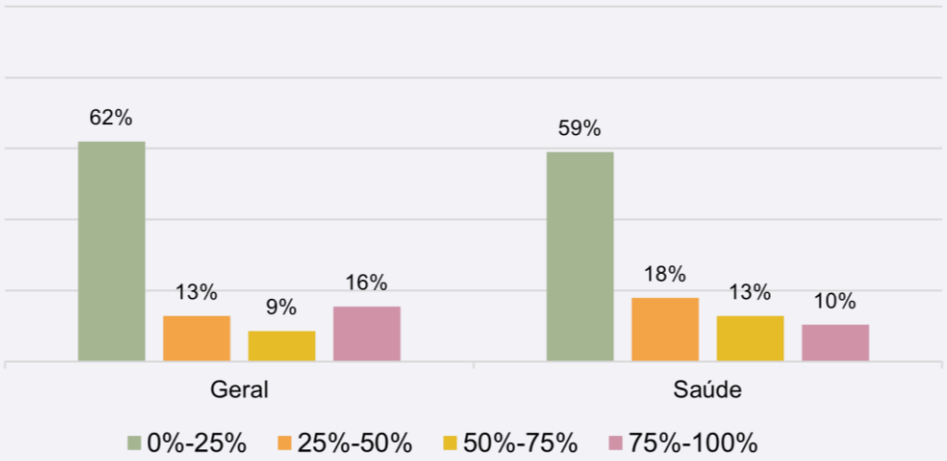
Gráfico 3 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança



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

Na saúde, mais de 80% 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 9.**

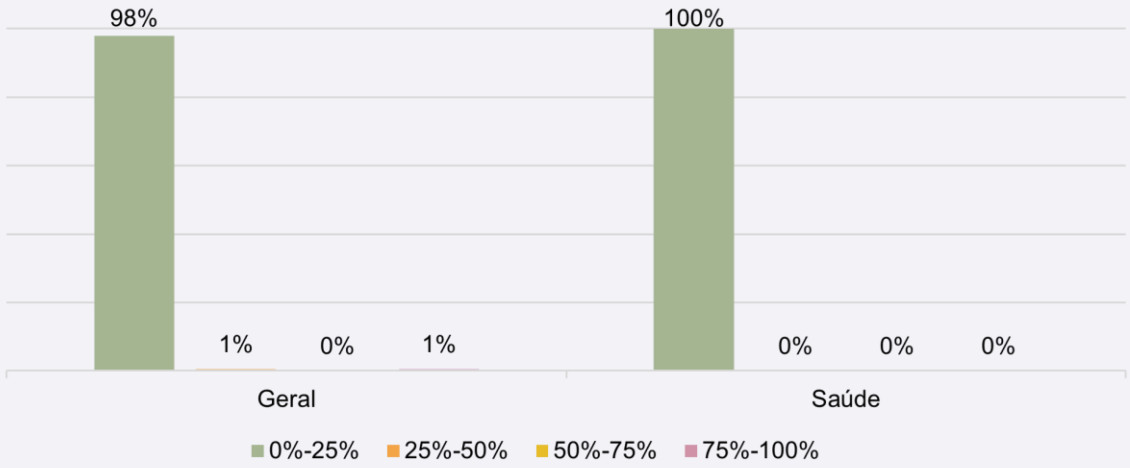
Gráfico 4 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança



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

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

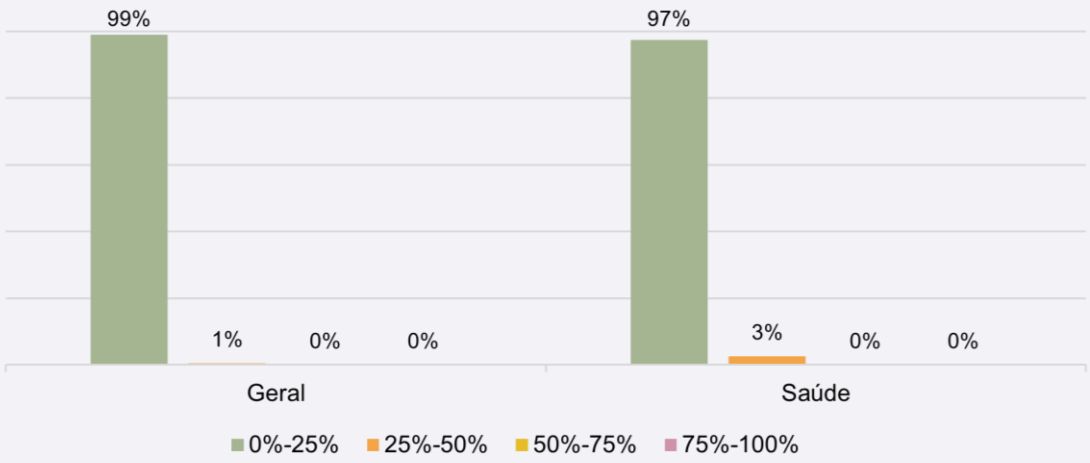
Gráfico 5 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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.

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, onde no setor da saúde 100% representa o intervalo de 0%-25%.

Gráfico 6 - Percentagem aproximada de trabalhadores do operador com certificações em cibersegurança

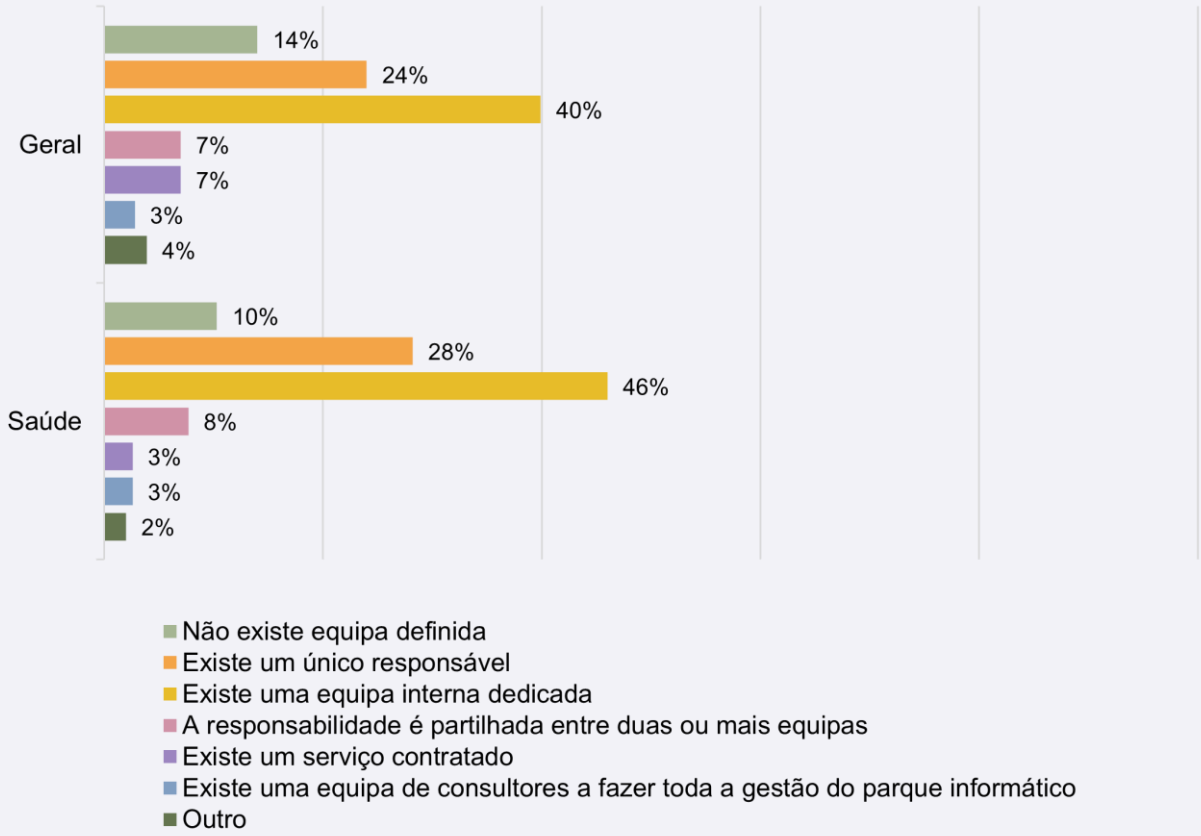


A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. O setor da saúde destaca-se face ao panorama geral, onde 3% dos operadores indicaram haver 25%-50% de colaboradores com certificações em cibersegurança.

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[5].

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

Gráfico 7 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (helpdesk), em matéria de cibersegurança e/ou tecnologias da informação

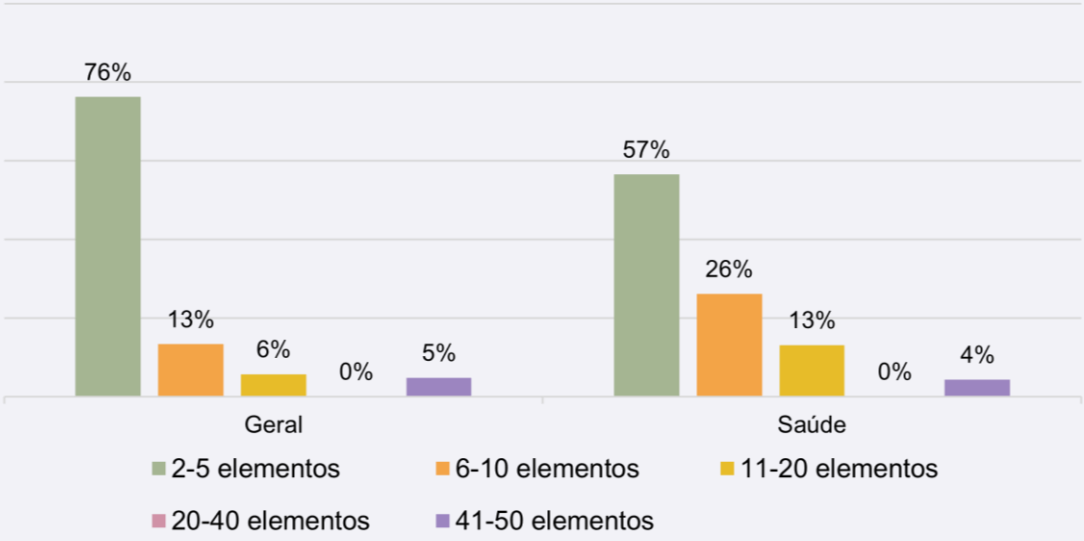


De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (24% dos casos).

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.

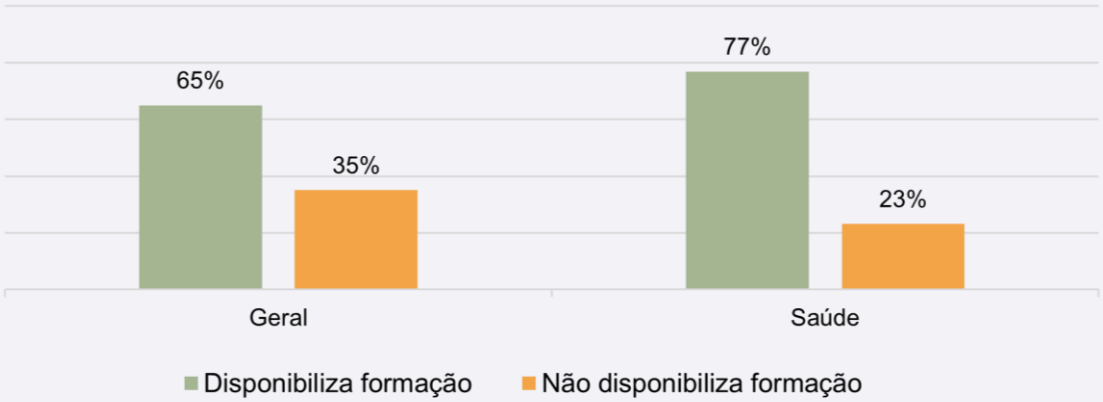
Os OSE do setor da saúde contam, maioritariamente, com uma ou mais equipas dedicadas (46%) ou com um único responsável (28%), verificando-se também o recurso à contratação externa em 3% dos casos, a não existência de equipa definida (em 10% dos OSE inquiridos), a partilha de a responsabilidade entre duas ou mais equipas e aquelas onde uma equipa de consultores faz toda a gestão do parque informático (3%), já outras situações correspondem a 2% dos casos.

Gráfico 8 - 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. O setor da saúde segue a tendência geral sendo que 57% possui equipas de 2-5 elementos, 26% conta com equipas de 6-10 elementos e 13% com equipas de 11-20 elementos. Os restantes 4% referem-se a grandes equipas de 41-50 elementos.

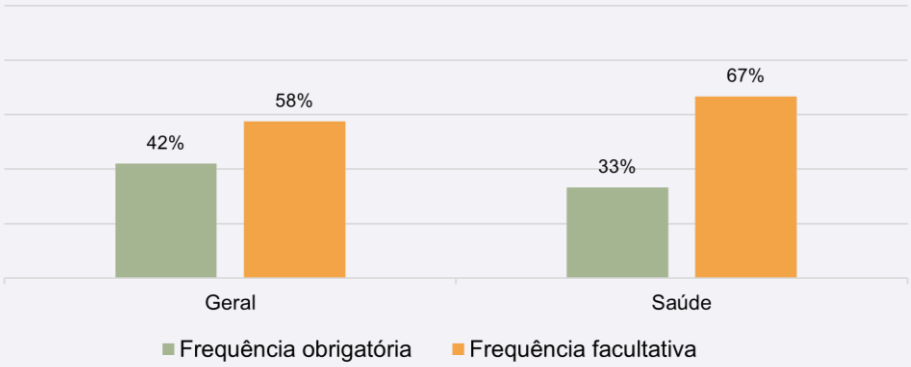
Gráfico 9 - Disponibilização de formação em cibersegurança aos colaboradores



Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. O setor da saúde destaca-se por 77% dos OSE terem indicado disponibilizar formação em cibersegurança aos seus colaboradores, superando a média 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[6]. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado "Estado da Cibersegurança em Portugal", indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

Gráfico 10 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



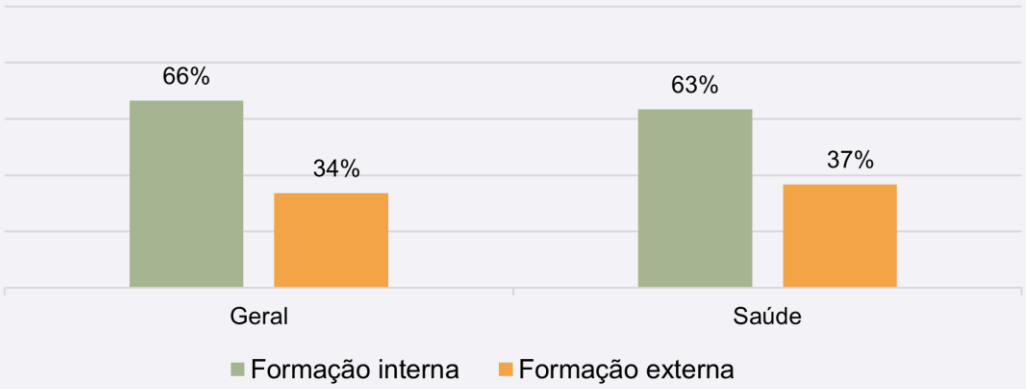
De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais a tendência de as formações serem

[6] 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

obrigatórias é mais baixa, como no setor da saúde, onde apenas 33% da formação tem caráter obrigatório em vez de facultativo.

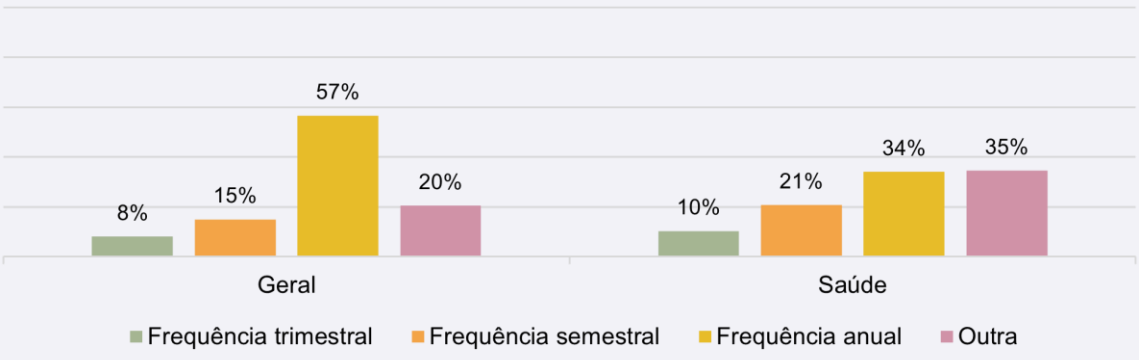
Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSE e demais empresas em Portugal. Enquanto em 42% dos OSE que disponibilizam formação, esta é de caráter obrigatório, apenas em 19,2% das empresas portuguesas 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[7].

Gráfico 11 - 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. O setor da saúde é um dos setores onde mais se recorre a entidades externas para ministrar formação, respetivamente 37% de OSE a optarem por esse método.

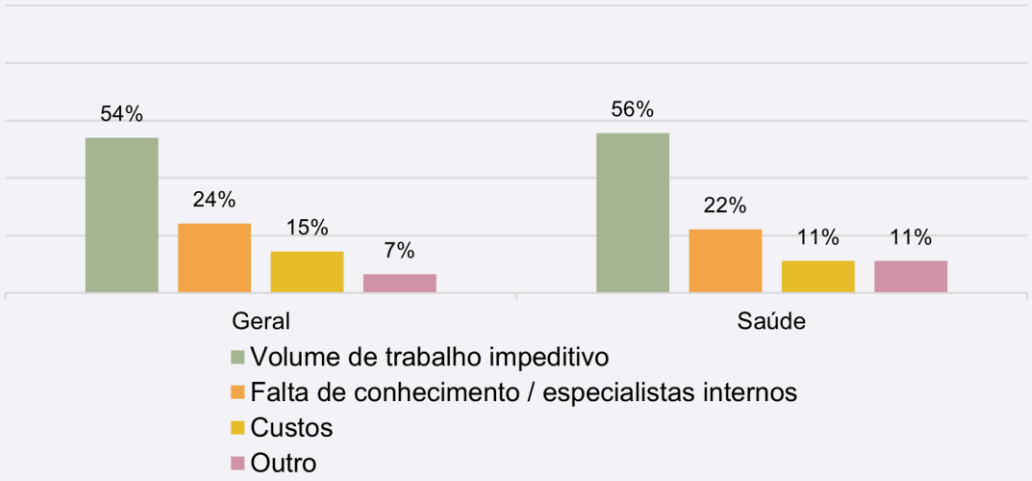
Gráfico 12 - Frequência média dos momentos de formação



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

Em termos gerais, a maioria dos OSE que disponibiliza formação indica que a frequência média dos momentos de formação é anual (57%). Por sua vez, o setor da saúde foi o que apresentou uma distribuição mais variada da frequência média dos momentos de formação.
Entre os OSE que indicaram "Outra" frequência (20%), tanto se registam frequências superiores à trimestral, chegando os momentos de formação a ser mensais ou mesmo semanais, como frequências inferiores à anual, onde não existe uma periodicidade definida e os momentos de formação sucedem de modo *ad hoc*. Por exemplo, o setor da saúde é um dos que apresenta percentagens mais elevadas na opção "Outra", tanto se registaram respostas indicando momentos de formação semanais ou mesmo diários, como respostas que indicavam que não se realizaram momentos de formação em cibersegurança em mais de um ano.

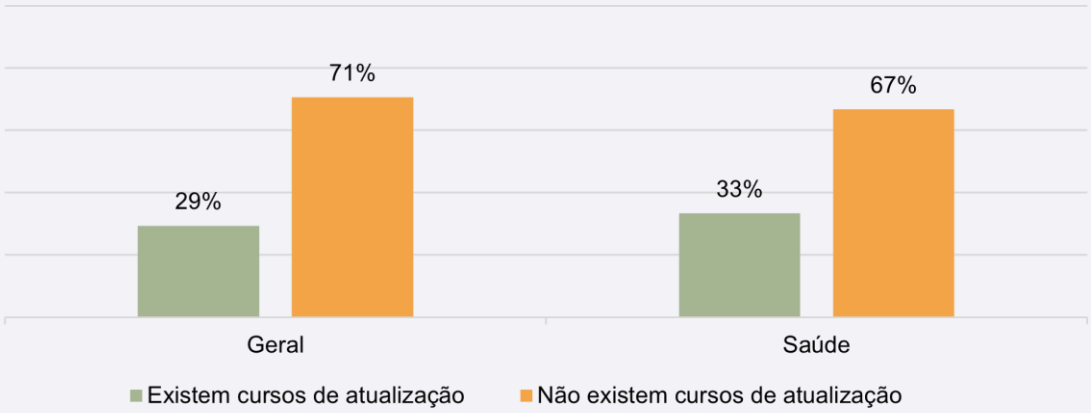
Gráfico 13 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam



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 saúde, o principal motivo indicado continua a ser o volume de trabalho impeditivo, indicado por 56% dos OSE que não disponibilizam formação. Este setor é também um dos únicos a indicar "Outros" motivos para a falta de formação. Esses outros motivos passam, segundo os OSE do setor, pela falta de planos de formação dentro das organizações e pela alocação de recursos financeiros a formação noutras áreas que não a cibersegurança.

Gráfico 14 - Existência de cursos de atualização (“refresher courses”) para os colaboradores



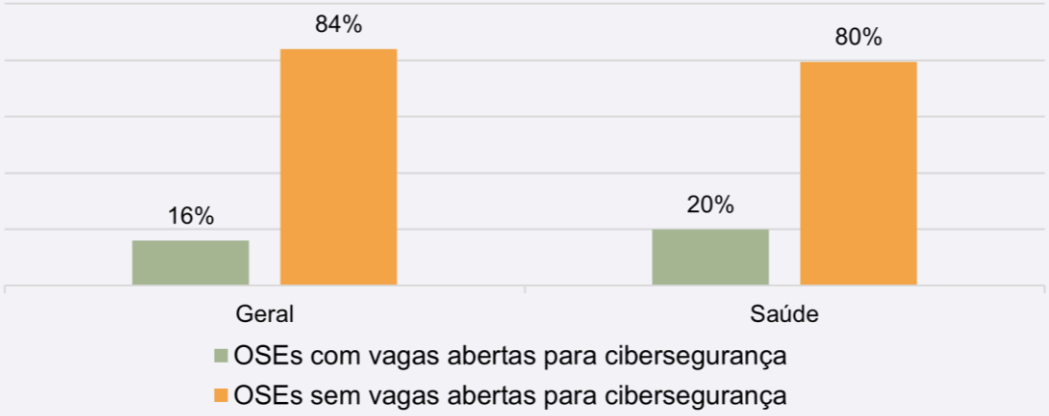
A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos. O setor da saúde espelha a percentagem geral, com apenas mais 4% dos OSE a disponibilizarem este tipo de cursos ou formações.

Gráfico 15 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas

A vasta maioria dos OSE inquiridos (91%) considera haver um cenário de escassez de profissionais de cibersegurança e áreas relacionadas no mercado de trabalho. Especificamente, nos setores da banca e das infraestruturas do mercado financeiro, todos os OSE inquiridos consideram que há falta de profissionais na área. O setor da saúde apenas varia em 1 p.p. face ao valor geral.

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[8] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[9]. 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[10]. 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), a admissão de colaboradores em trabalho totalmente remoto, e a 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[11] [12].

Gráfico 16 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. No setor da saúde, apenas 20% dos OSE dispõem de vagas abertas para a cibersegurança.

Embora não se possa fazer uma associação direta entre vagas para cibersegurança e para pessoal especialista em TIC, os dados do IUTICE de 2022 mostram que, nesse ano, apenas 6,2% das empresas portuguesas tentaram recrutar pessoal especialista em TIC[13].

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

[9] 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.

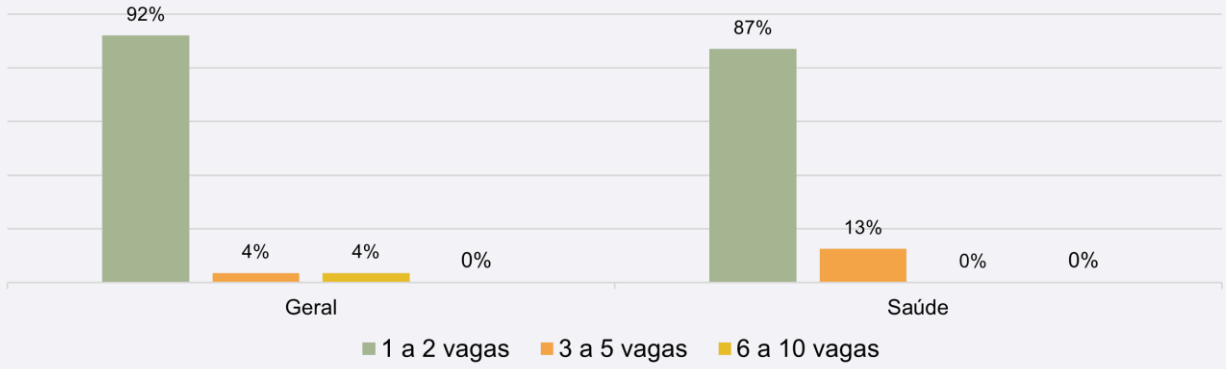
[10] ENISA, "NIS Investments", 2022, 16, https://www.enisa.europa.eu/publications/nis-investments-2022.

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

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

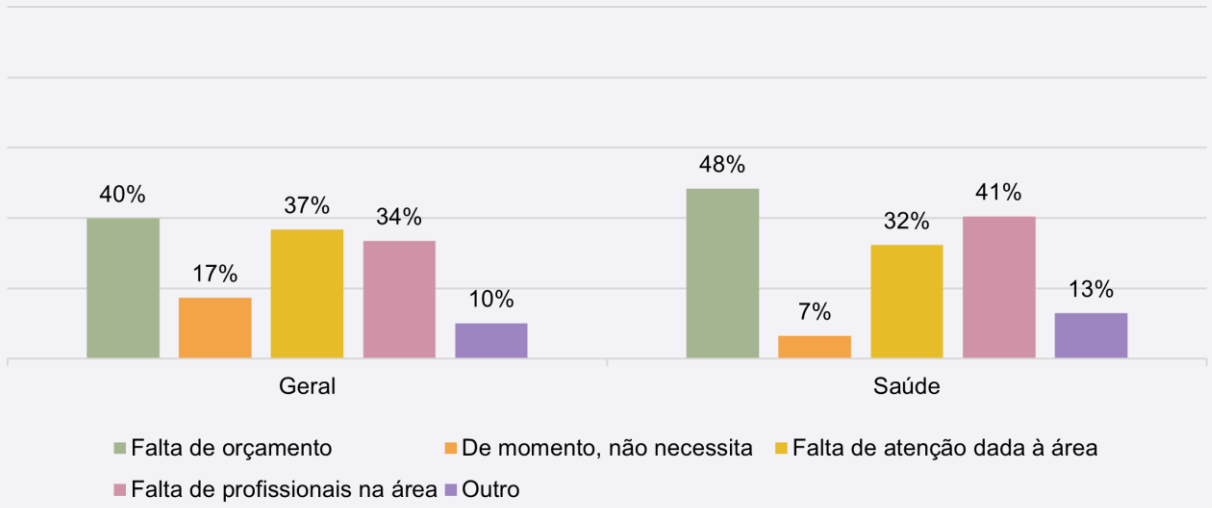
[13] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 15.

Gráfico 17 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança



Entre os 16% de OSE que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Apenas no setor da saúde se registaram OSE com 3 a 5 vagas em aberto.

Gráfico 18 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança

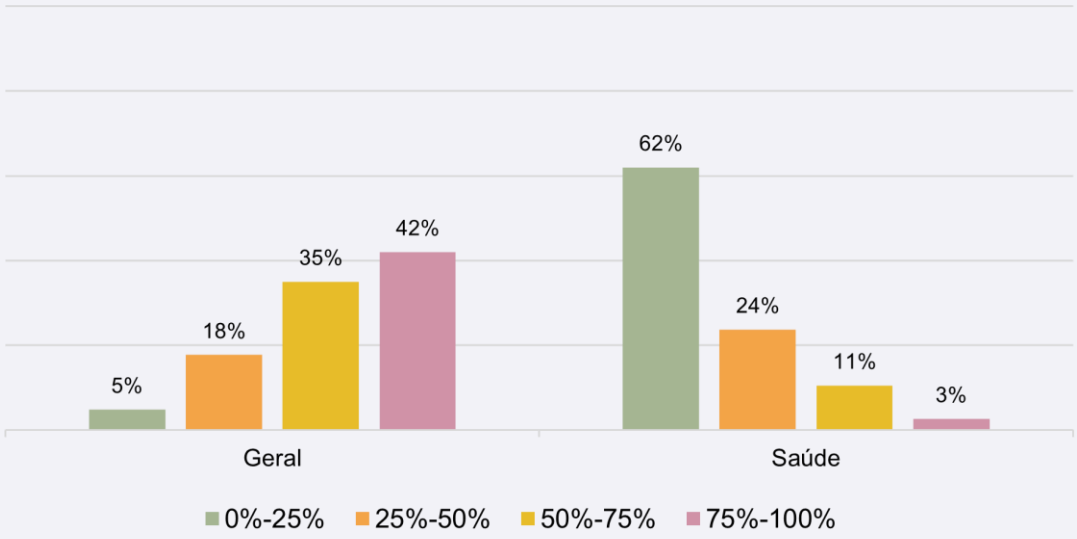


No seguimento das questões sobre vagas em aberto para a área de cibersegurança, questionou-se também os motivos pelos quais os OSE não teriam tais vagas disponíveis.
A resposta mais comum foi a falta de orçamento, indicada por 40% dos OSE sem vagas em aberto, seguida da falta de atenção dada à área (37%) 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. Sectorialmente, a saúde apesenta os mesmos motivos que os demais.
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[14].

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"[15], objetivo esse que não pode ser cumprido quando há falta de atenção dada à área. Tratando-se de Operadores de Serviços Essenciais, esta lacuna torna-se ainda mais grave. Recorda-se, também, que é uma boa prática constante de normativos internacionais, como a ISO/IEC 27001, que a direção/administração das organizações demonstre o seu compromisso para com segurança da informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio[16].

Gráfico 19 - 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, sendo que o setor da saúde é o mais evidente, no qual mais de 60% dos OSE indicam uma percentagem de até 25% dos colaboradores com acesso a equipamentos digitais na realização do seu trabalho.

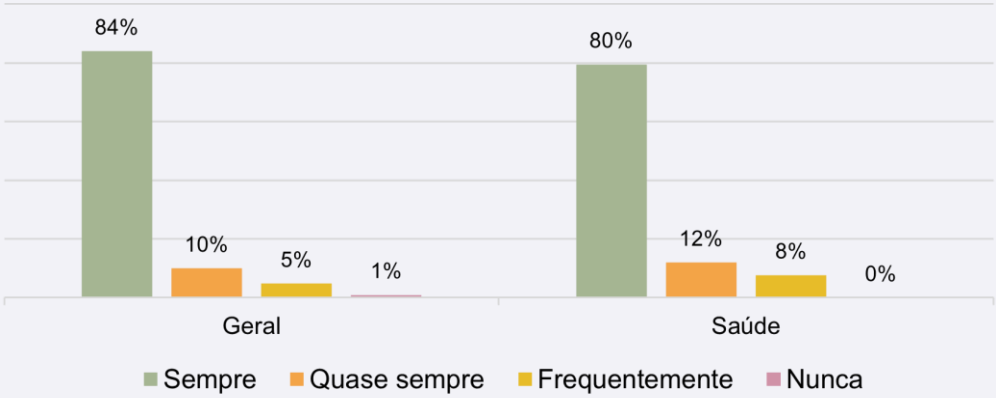
[14] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 15-17.

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

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

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[17].

Gráfico 20 - OSE que são responsáveis pelo fornecimento dos equipamentos necessários às funções dos colaboradores



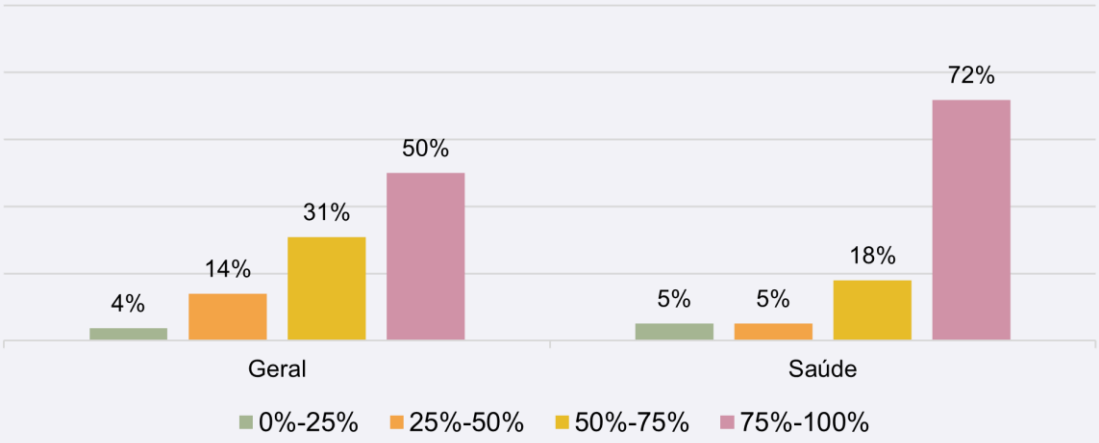
Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos nos setores da energia, dos transportes, da banca e das infraestruturas do mercado financeiro indicaram ser os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

No setor da saúde, houve 80% de OSE a indicar que eram sempre responsáveis pelo fornecimento dos equipamentos. Ressalva-se ainda que não se registaram situações em que os OSE nunca fornecem os equipamentos, impondo esse encargo aos colaboradores.

Novamente, sublinha-se que segundo o IUTICE de 2022, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais, abrangendo 28,1% do pessoal ao serviço[18].

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

Gráfico 21 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções

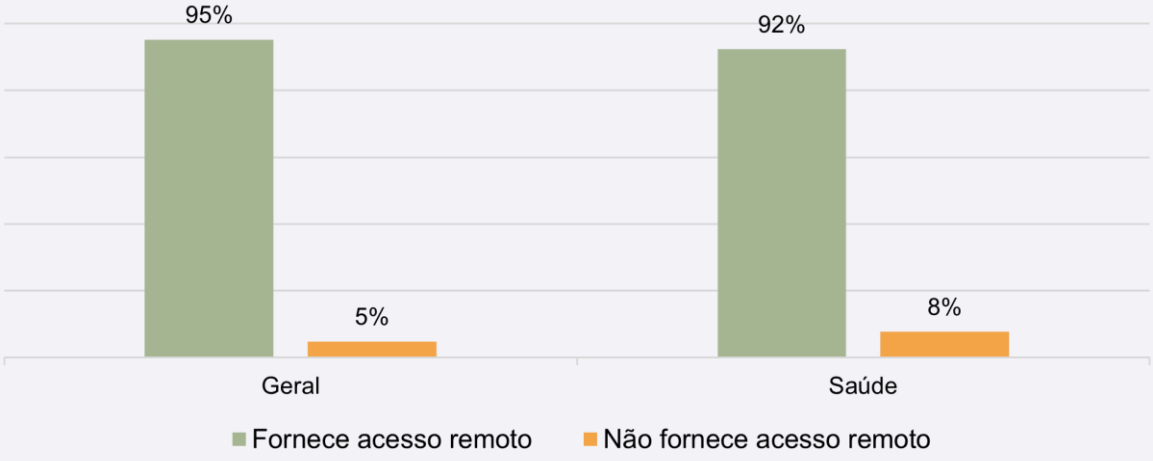


A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.
No setor da saúde, a faixa predominante continua a ser aquela em que 75%-100% dos colaboradores tem acesso à Internet no desempenho das suas funções, embora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

Voltando a comparar com dados do IUTICE, mas agora com o de 2023, verifica-se que há mais colaboradores com acesso à Internet no contexto específico dos OSE do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSE onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando setorialmente onde possível, como nos setores da energia e dos transportes, os OSE continuam a apresentar mais colaboradores com acesso à Internet: segundo o IUTICE, no setor da energia, há 39,8% de colaboradores com acesso à Internet, enquanto o questionário realizado demonstra que em 89% dos OSE desse setor, 50% dos colaboradores ou mais têm acesso à Internet; e no setor dos transportes, 56,6% dos colaboradores têm acesso à Internet no contexto empresarial português, enquanto no contexto dos OSE 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho[19].

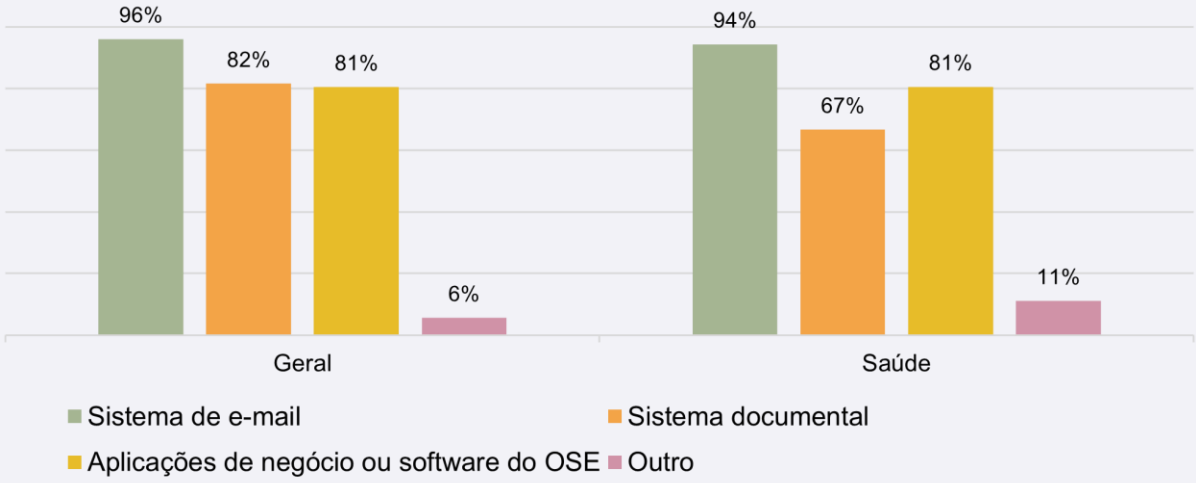
[19] Instituto Nacional de Estatística, “Inquérito à Utilização das TIC nas Empresas”, 2023, 3.

Gráfico 22 - 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%). O setor da saúde é um dos nos quais ainda se registaram exceções. Ainda assim, pelo menos 92% dos OSE nestes setores fornecem acesso remoto a esses sistemas aos seus colaboradores.
Voltando a comparar com os dados do IUTICE de 2022, há uma maior percentagem de Operadores de Serviços Essenciais a fornecer acesso remoto ao sistema de e-mail do que na generalidade das empresas em Portugal. Enquanto 95% dos OSE indicaram dar esse acesso remoto, no contexto empresarial geral apenas 74,7% das empresas fornecem acesso remoto ao sistema de e-mail[20].

Gráfico 23 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores



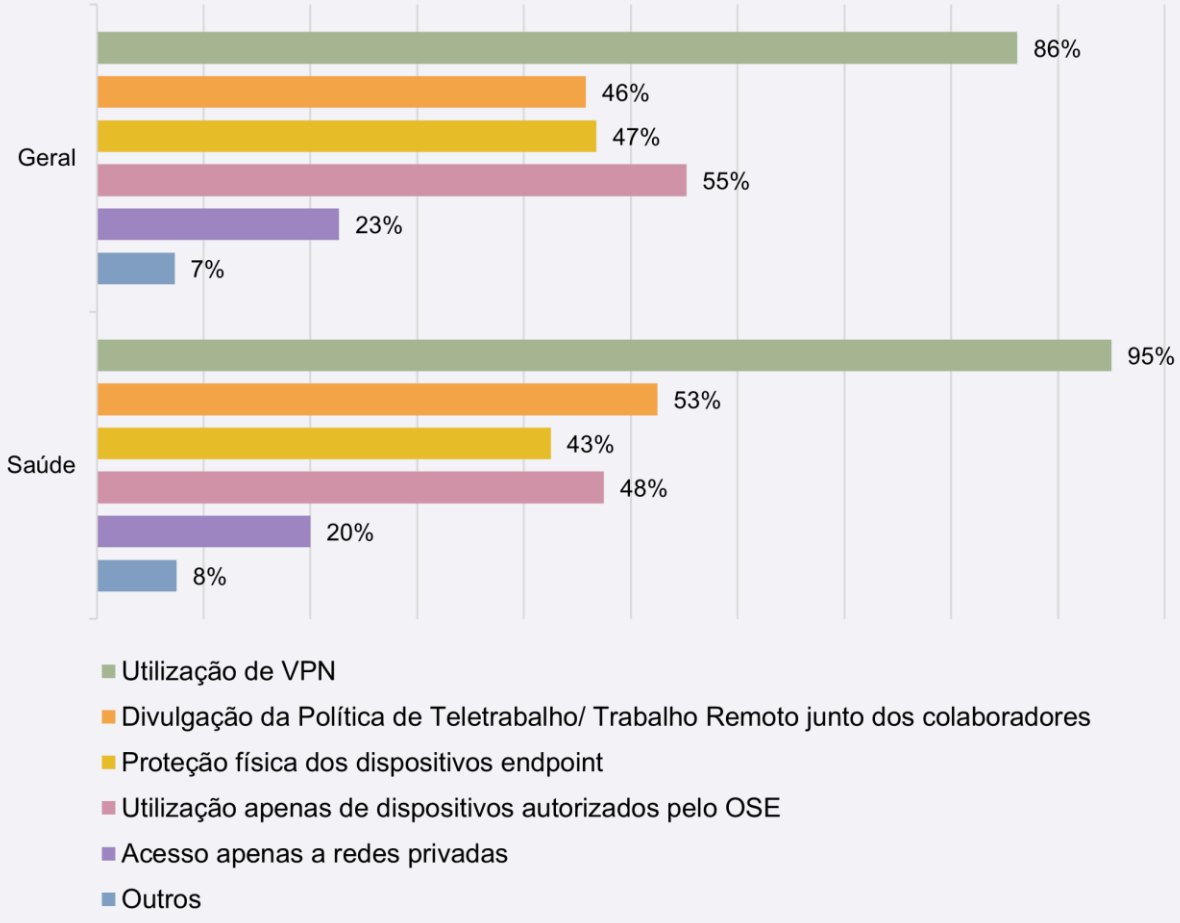
Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

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

No setor da saúde, os sistemas de e-mail podem ser acedidos por 94% dos colaboradores, sistemas documentais por 67% e aplicações de negócio por 81%.

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%)[21].

Gráfico 24 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE

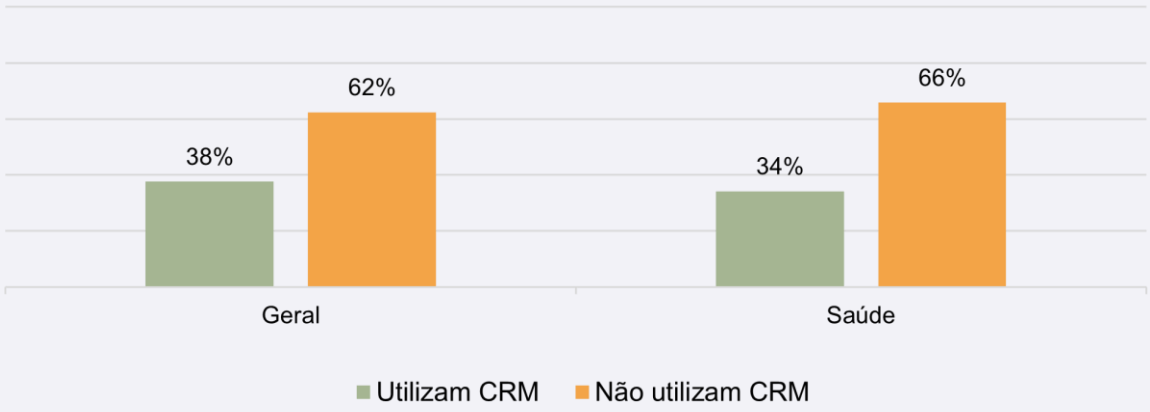


No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança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

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

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*).
No setor da saúde a divulgação da política de teletrabalho supera a proteção física dos dispositivos *endpoint*.
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.

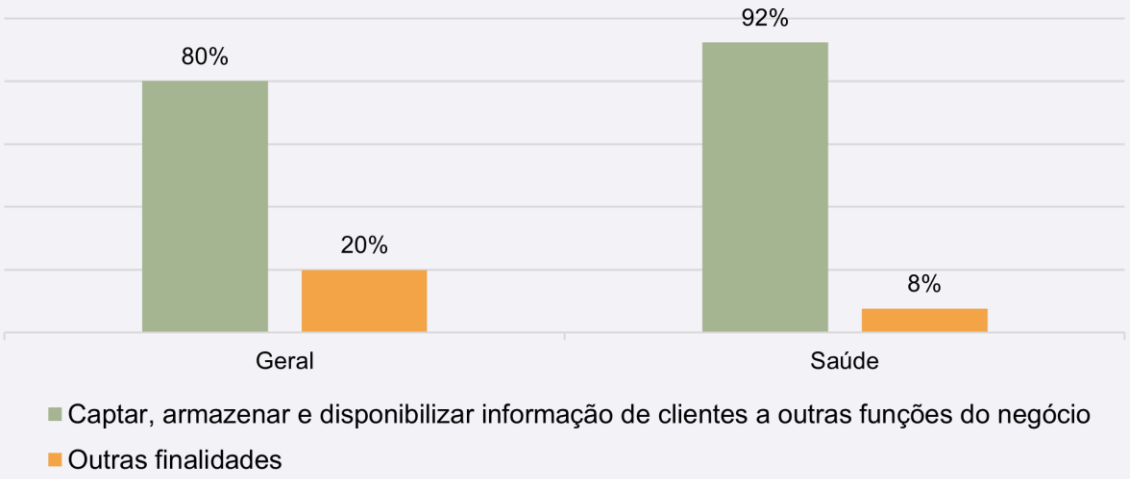
Gráfico 25 - OSE que utilizam Customer Relationship Management software (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)[22] - 62% - do que aqueles que utilizam - 38%. Quanto ao setor da saúde predominam os operadores que não utilizam CRM: praticamente dois terços, 66%.

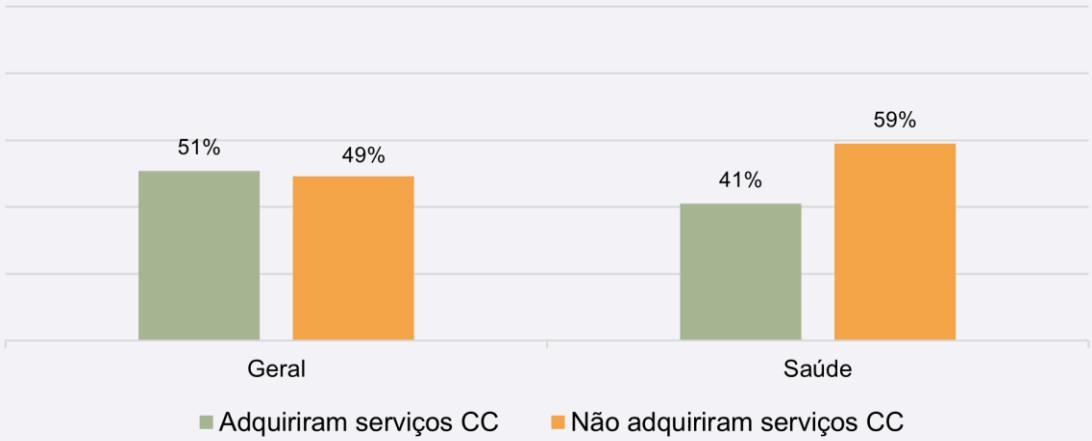
[22] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

Gráfico 26 - 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 em que mais OSE utilizam CRM para as funções especificadas é o da saúde, com 92%.

Gráfico 27 - OSE que adquiriram serviços de Computação Cloud (CC)

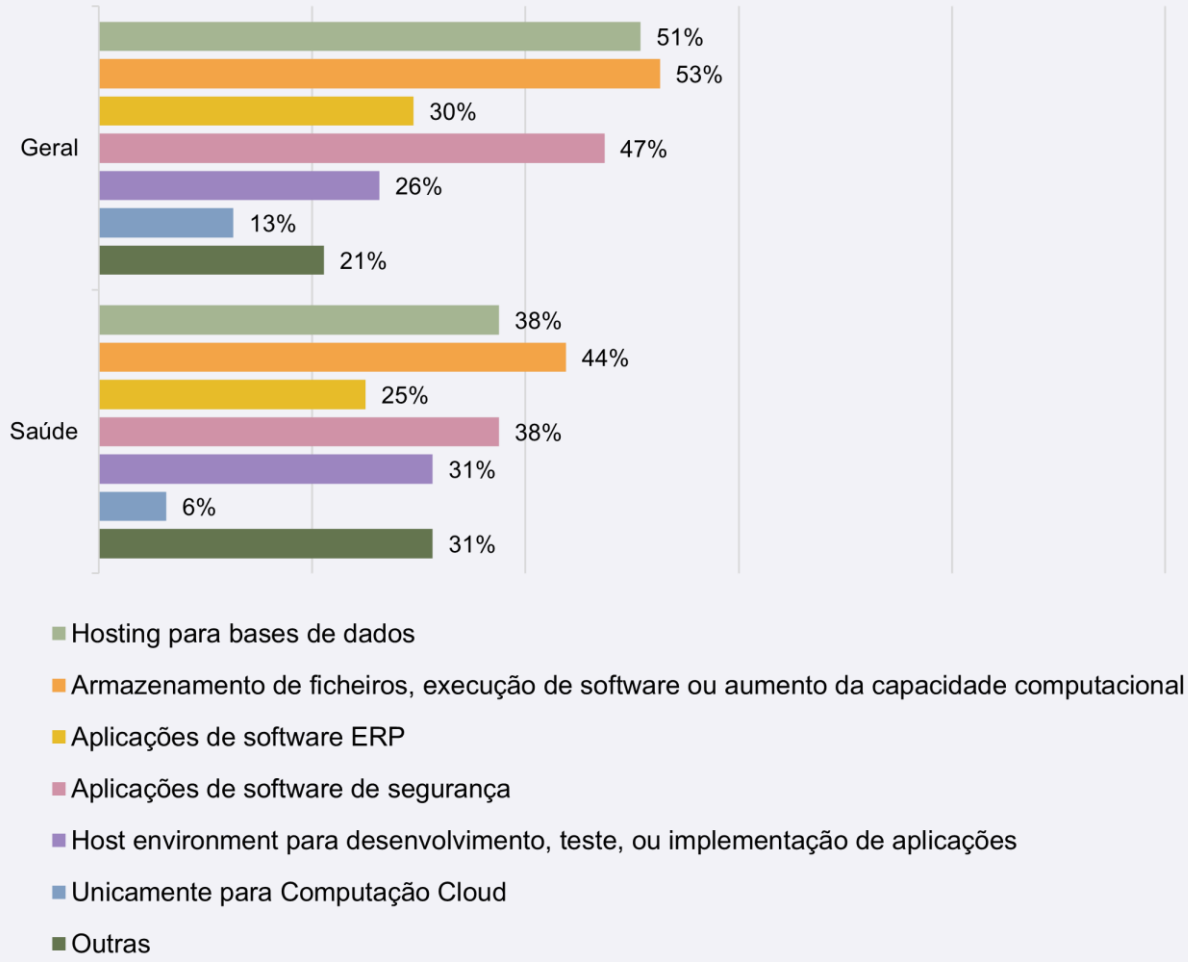


À data do estudo, 52% dos operadores tinham adquirido serviços de Computação *Cloud* (CC) para a sua organização.

Um dos setores onde menos de 50% dos OSE inquiridos adquiriram serviços *cloud* é o da saúde. 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[23]. Em 2023, este tipo de serviços continuou a ser uma das áreas onde os OSE mais aumentaram o seu investimento (49% dos OSE inquiridos pela ENISA em 2023 indicaram ter aumentado os seus investimentos em plataformas *cloud*)[24]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[25].

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

Gráfico 28 - Finalidades dos serviços de Computação Cloud adquiridos



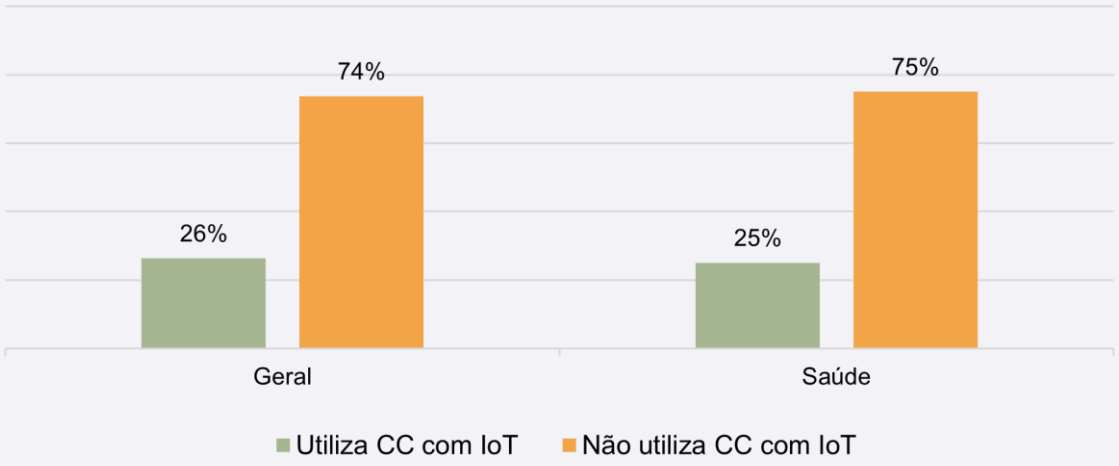
As finalidades dos serviços de Computação Cloud são múltiplas, variando entre *hosting* para bases de dados; armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional; aplicações de *software* ERP[26] aplicações de *software* de segurança; *host environment* para desenvolvimento, 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. A nível setorial, o setor da saúde, a ordem das finalidades mais indicadas mantém-se praticamente igual, embora com diferenças nas percentagens, e com exceção da opção "Outras", que no caso da saúde foi apontada por tantos OSE quanto a finalidade de *host environment* para desenvolvimento, teste ou implementação de aplicações.

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

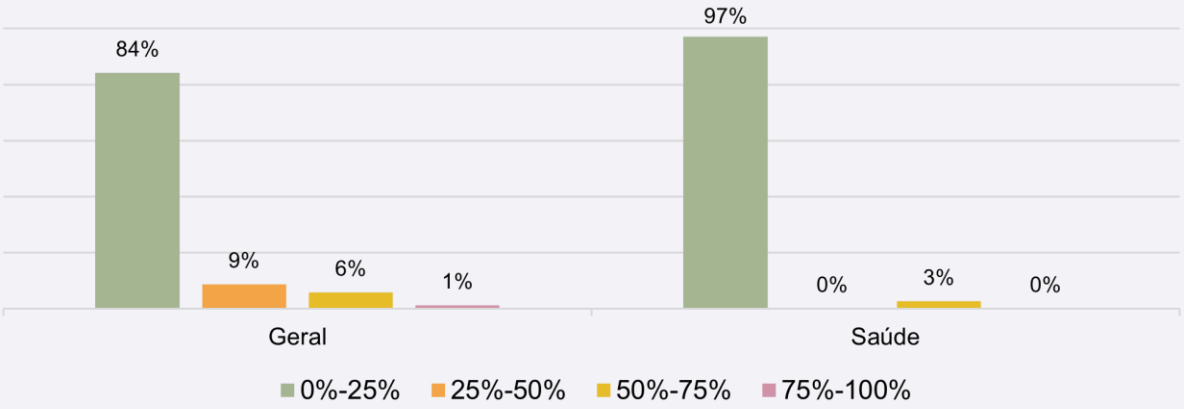
Comparando com dados do IUTICE de 2023, os serviços de computação *cloud* foram adquiridos pelas empresas em Portugal tendo em vista o funcionamento do serviço de correio eletrónico (91,1%), o armazenamento de ficheiros (73,7%), o funcionamento de *software* de aplicações de segurança (67,2%) e *software* de escritório (66,1%)[27].

Gráfico 29 - Utilização de serviços de CC em conjunto com *Internet of Things* (IoT)



De modo geral, não é frequente, entre os OSE, a utilização de serviços de Computação *Cloud* (CC) em conjunto com a *Internet of Things* (IoT), embora alguns operadores o façam (26%).
O setor da saúde é um dos setores em estudo onde os operadores mais utilizam os serviços CC em conjunto com *Internet of Things*, ultrapassando os 20% de utilização.

Gráfico 30 - Percentagem de sistemas core em *cloud*

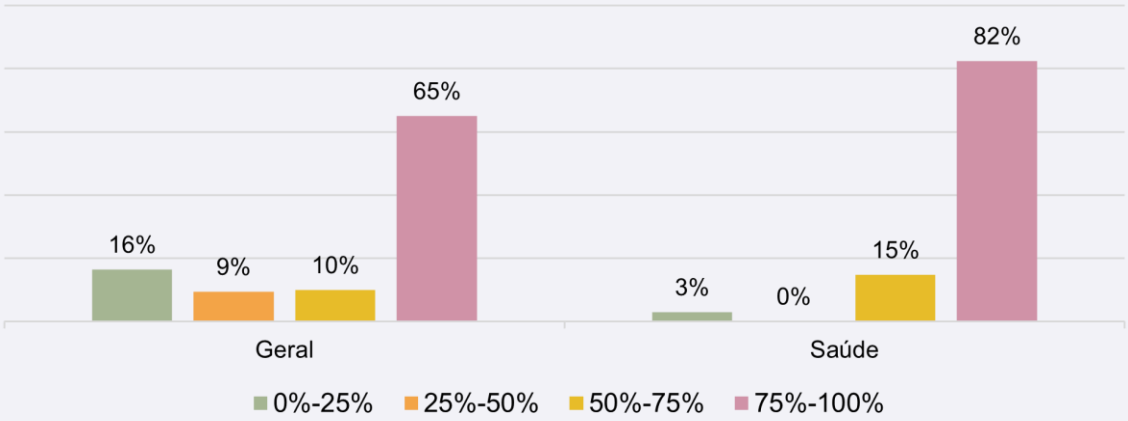


Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos.

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

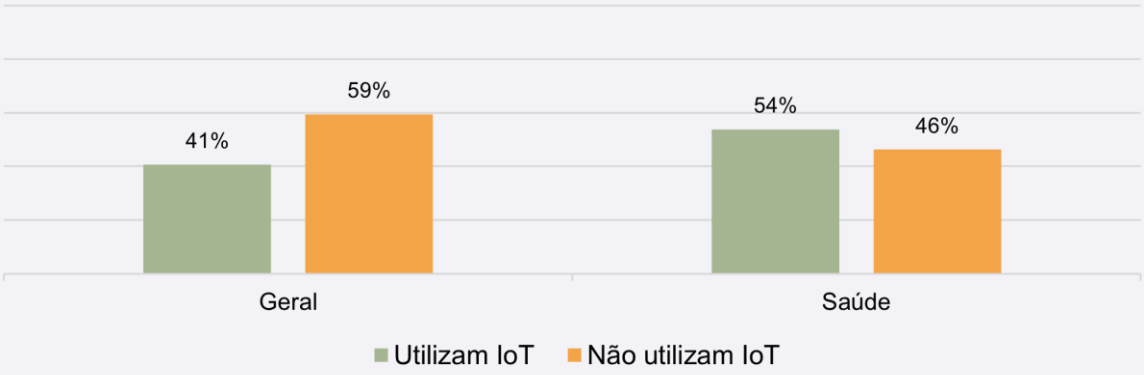
Há, no entanto, exceções. Por exemplo o setor da saúde, registam-se OSE cuja percentagem de sistemas *core* em *cloud* se encontra no intervalo de 50%-75%.

Gráfico 31 - 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, sendo que no setor da saúde essa percentagem passa a 82%.

Gráfico 32 - Utilização de IoT pelos OSE

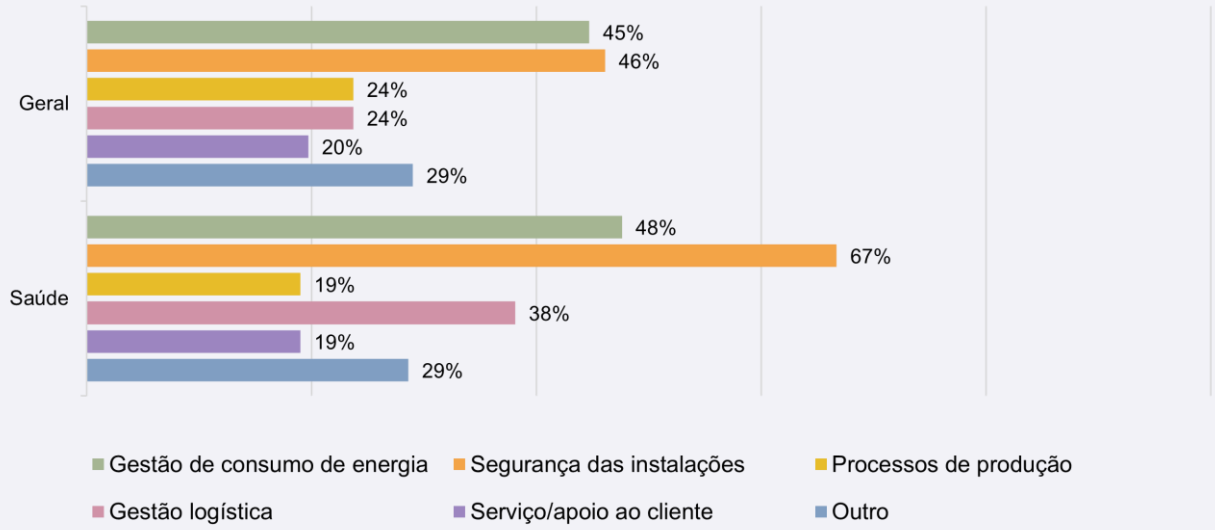


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. Destacam-se os setores bancário e das IMF, onde a totalidade dos inquiridos respondeu não utilizar de todo IoT.
Em contraste, no setor da saúde, são mais os operadores que utilizam IoT do que aqueles que não utilizam, embora essa 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%[28].

[28] 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 33 - 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 dos inquiridos, ao contrário da utilização de IoT para serviço/apoio ao cliente, que tem menos expressividade, cerca de 20%. No setor da saúde, a utilização de IoT é mais frequente no contexto de segurança das instalações.

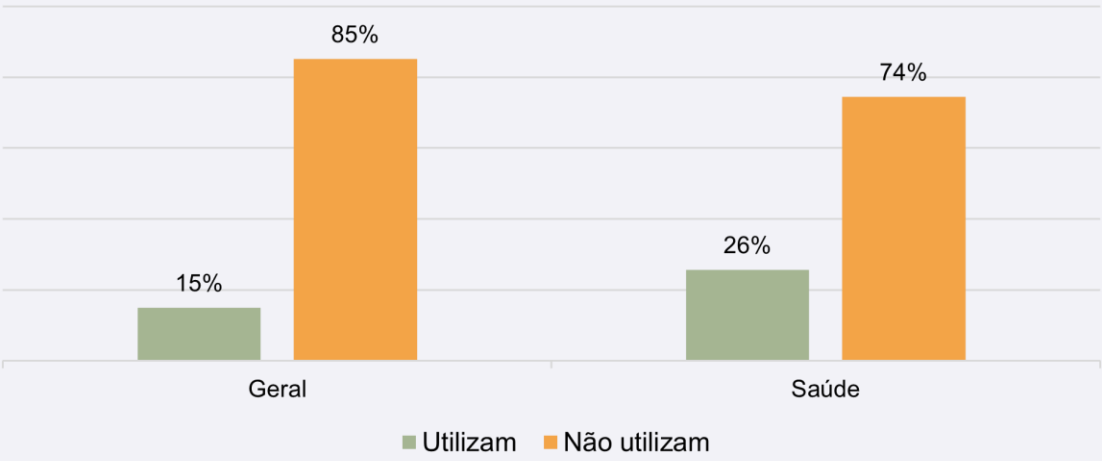
O mesmo estudo da ANACOM mencionado no gráfico anterior indica que "os equipamentos IoT foram sobretudo utilizados para segurança das instalações (86%), gestão do consumo de energia (32%), gestão logística (21%), processos de produção (19%), monitorização das necessidades de manutenção (18%) e serviço ao cliente (13%)"[29].

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

Gráfico 34 - 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%). No setor da saúde nenhum OSE mencionou a dificuldade, disponibilidade ou qualidade de dados como motivo da não utilização de IoT.
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 35 - OSE que utilizam processos que recorrem a IA



A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.
Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. Apenas 26% dos OSE do setor da saúde menciona utilizar processos que recorrem a IA.

Comparando com dados do IUTICE de 2023, conclui-se que no universo dos Operadores de Serviços Essenciais há uma maior percentagem de empresas a já recorrer a Inteligência Artificial do que se se olhar para o panorama empresarial geral português. Enquanto 15% dos 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%)[30], 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%[31].

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

Gráfico 36 - Funções para as quais utilizam IA

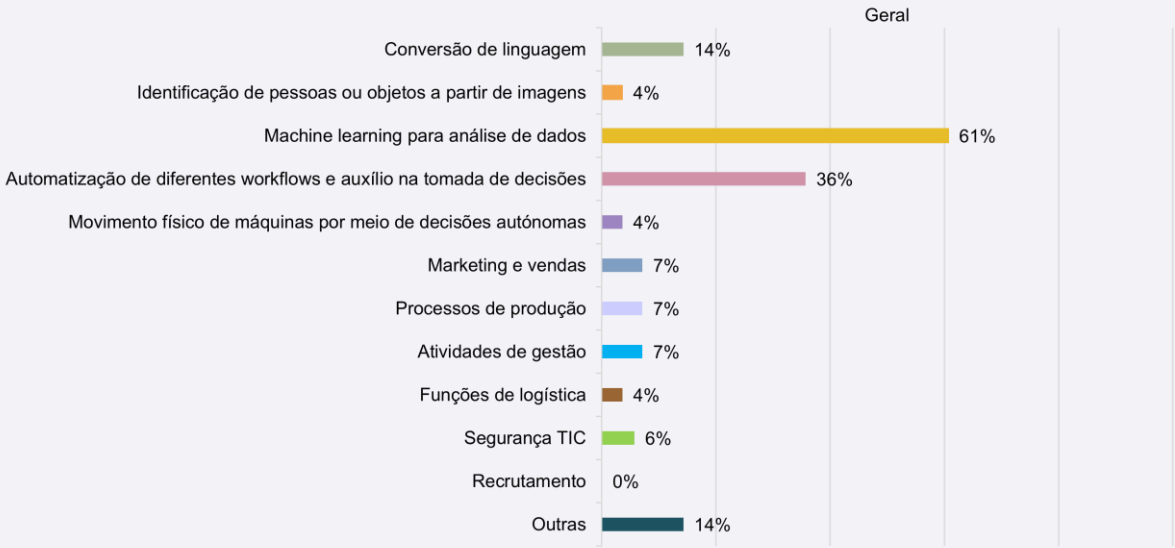
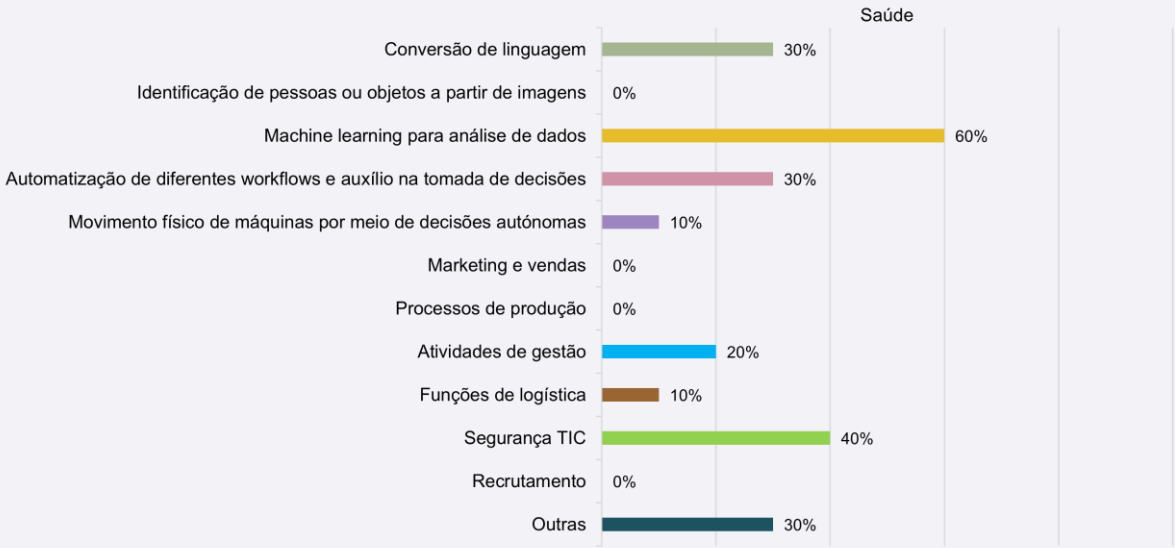


Gráfico 36.1 - Funções para as quais utilizam IA



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 OSE da saúde que recorrem a Inteligência Artificial. Destaca-se também a utilização de IA para a automatização de fluxos de trabalho e auxílio na tomada de decisões, indicada por 35% dos OSE que fazem uso de IA. As restantes funções surgem de forma mais residual, sendo indicadas por

apenas 15% ou menos dos OSE que já recorrem a IA. Curiosamente, não se registou o recurso a Inteligência Artificial em processos de recrutamento entre os OSE inquiridos.

De acordo com os dados do IUTICE de 2023, entre as empresas que utilizam tecnologia de IA, 44,7% delas utilizam-na para identificar objetos ou pessoas através de imagens. Em seguida, 40,8% das empresas utilizam tecnologias que automatizam fluxos de trabalho ou auxiliam na tomada de decisão. Tecnologias para análise de linguagem escrita são utilizadas por 35% das empresas, apresentando um ligeiro. Já as tecnologias de aprendizagem automática para análise de dados, incluindo *deep learning*, são adotadas por 26,2% das empresas. A tecnologia de IA menos utilizada pelas empresas é a que permite a movimentação física de máquinas através de decisões autónomas baseadas na observação do meio ambiente, com apenas 8,3% de adoção. No entanto, no setor da Indústria e Energia, essa tecnologia é mais prevalente, sendo utilizada por 15,3% das empresas que empregam IA[32].

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"[33]. 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%[34].

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

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

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

Gráfico 37 - Medidas de proteção contra ameaças de cibersegurança – Geral

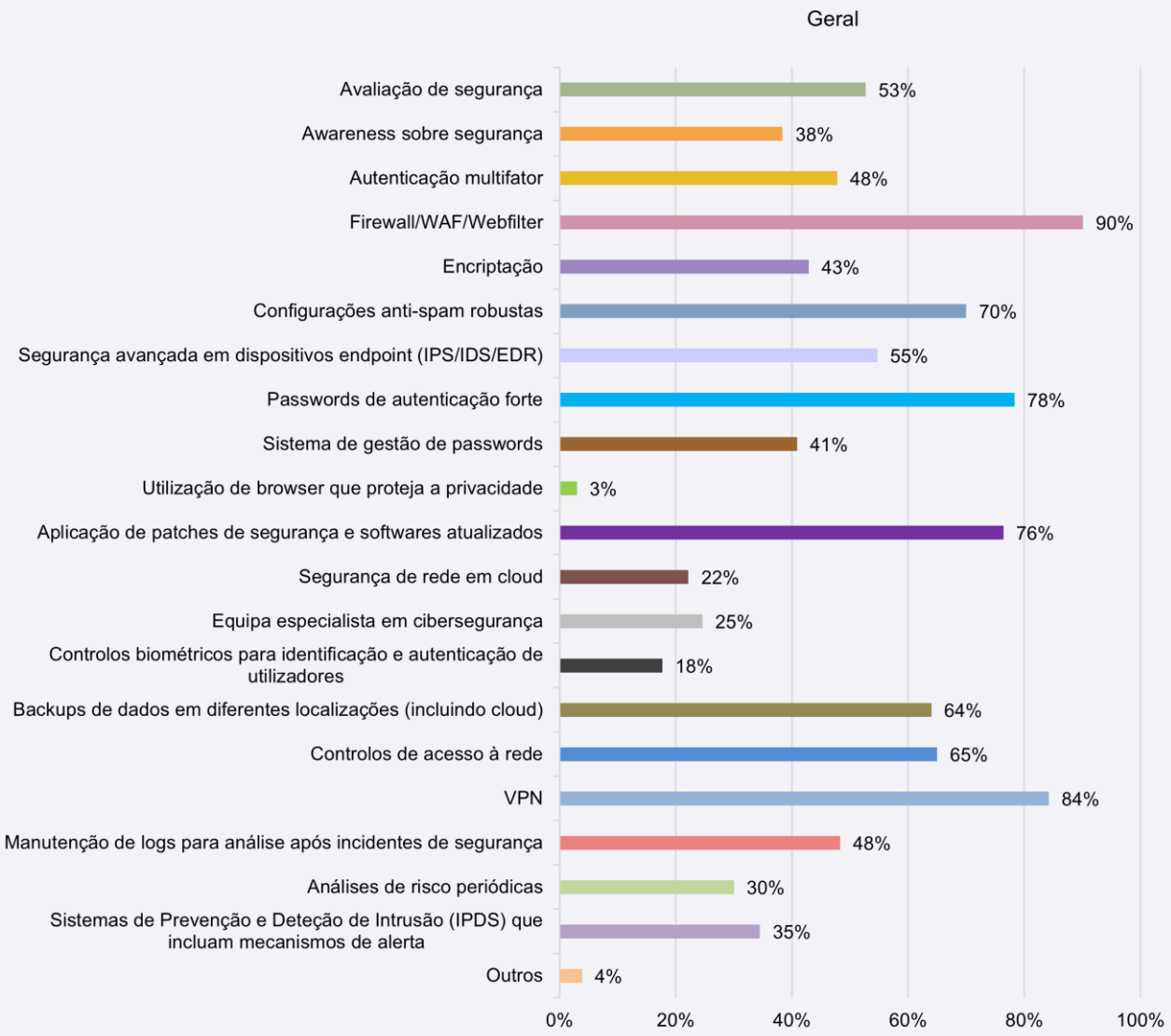


Gráfico 37.1 - Medidas de proteção contra ameaças de cibersegurança - Saúde

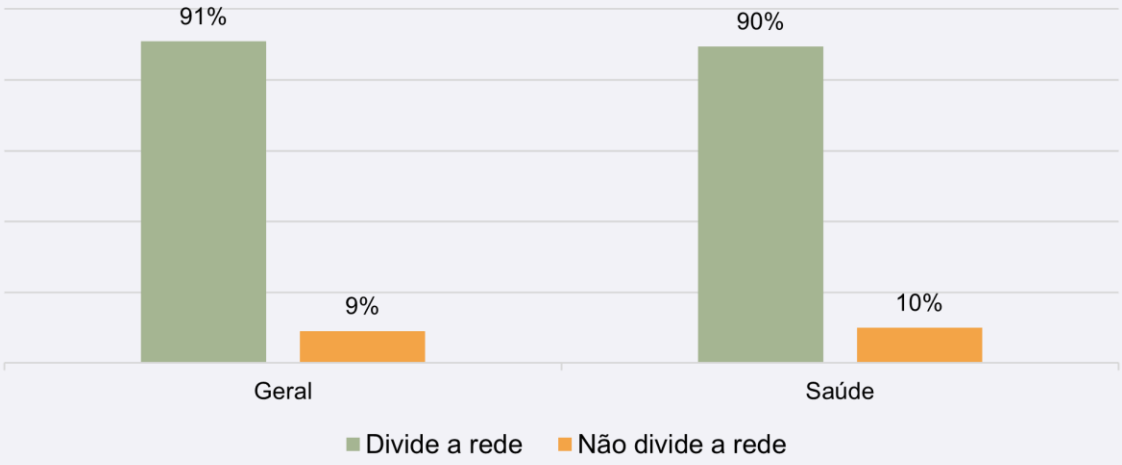
Na análise geral das medidas de segurança utilizadas pelos OSE, é possível verificar que medidas técnicas como a utilização de *Firewall/WAF/Webfilter*, utilização de VPN, palavras-passe de autenticação forte, aplicação de *patches* de segurança, a atualização dos *softwares* e *backups* de dados em 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 OSE 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. No setor da saúde, essas medidas são também pouco verificadas. Por exemplo, a realização de avaliações de segurança, a utilização de encriptação, de sistemas gestão de *passwords* ou a realização de análises de risco periódicas são todas medidas implementadas por menos de 50% dos OSE do setor.

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%[35].

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

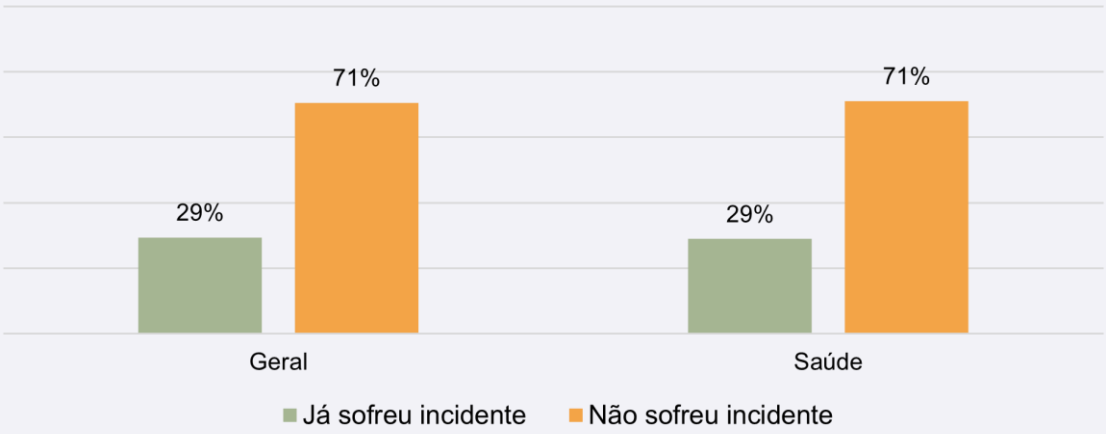
Gráfico 38 - Divisão entre rede dos colaboradores e rede para guests



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%. O setor da saúde apenas varia em 1 p.p. face à generalidade.

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

Gráfico 39 - OSE que já sofreram incidentes de segurança em contexto TIC



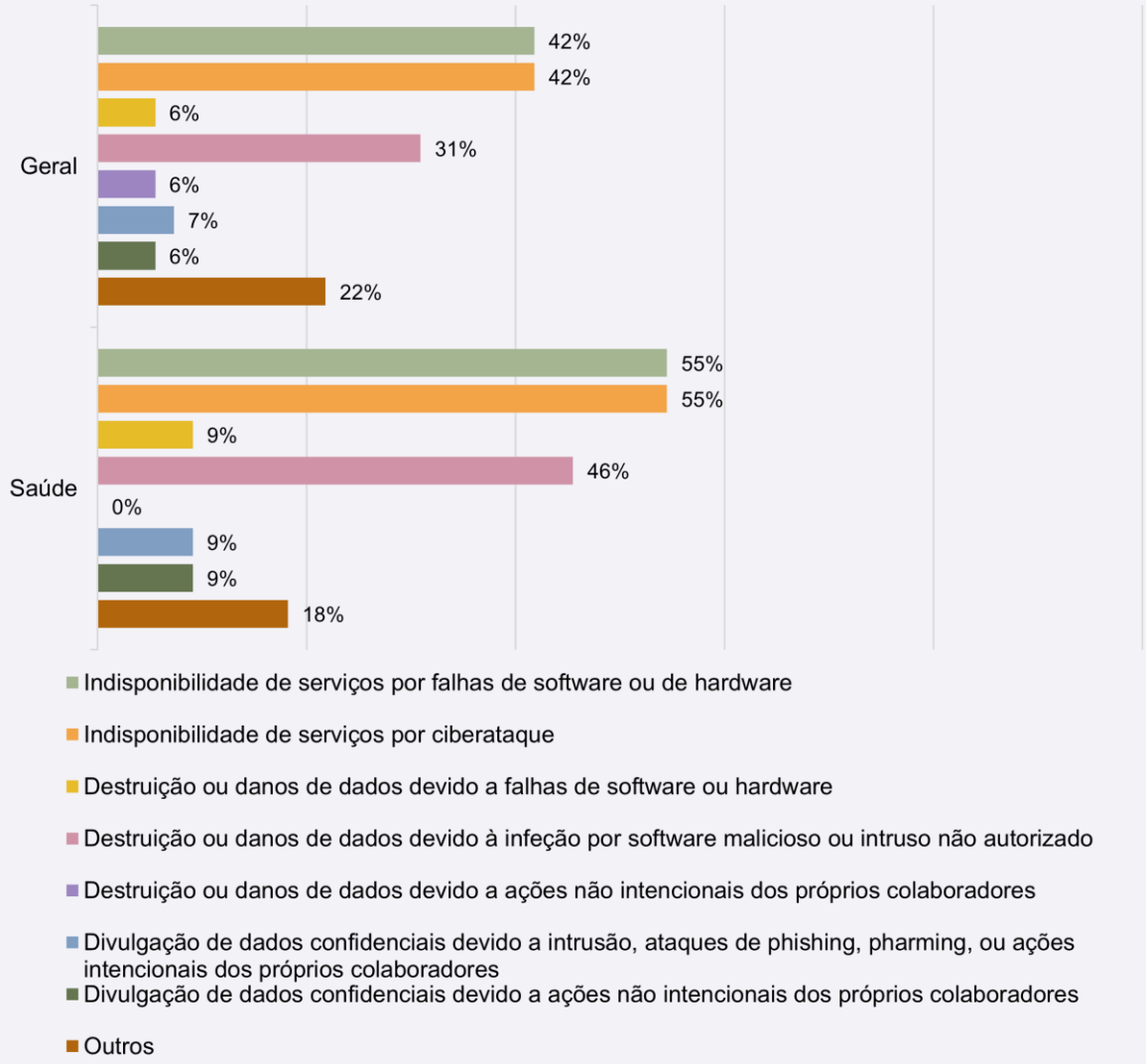
Em contexto TIC, pelo observado no gráfico, conclui-se que a maioria dos OSE inquiridos (71%) não sofreu incidentes neste contexto. O setor da saúde apresenta os mesmos resultados da generalidade, sem variações percentuais.

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)[37].

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[38].

[37] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 18.
[38] Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", janeiro de 2024, 5, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf.

Gráfico 40 - Tipos de incidentes ocorridos



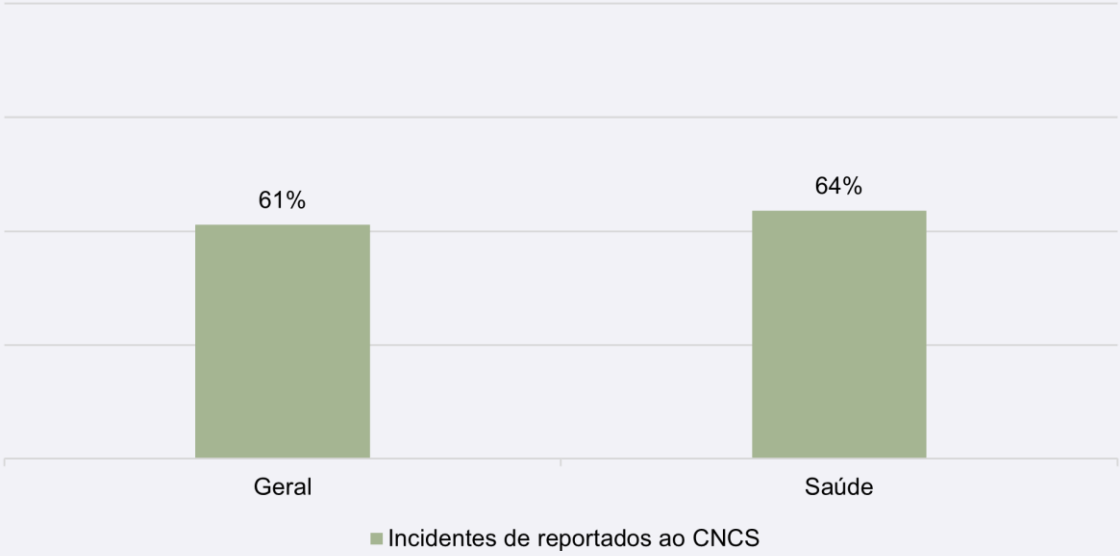
A grande maioria dos incidentes ocorridos afetou a disponibilidade dos serviços, quer por falha de *software* ou de *hardware*, quer por ciberataque. Depois destes, seguem-se os incidentes que resultaram na destruição de dados devido à infeção por *malware* ou devido a intrusão. Os operadores que referiram ter sofrido outros tipos de incidentes indicaram o comprometimento das contas de e-mail, a indisponibilidade de serviços por ataque a terceiros/prestadores de serviços e ainda tentativas de extorsão através de engenharia social. No setor da saúde, os três tipos de incidentes mais ocorridos prenderam-se com a indisponibilidade de serviços por falha de *software* ou *hardware*, indisponibilidade de serviços por ciberataque e com a destruição ou danos causados a dados por infeção com *malware* ou intrusão.

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)[39].

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[40].

Gráfico 41 - Incidentes de cibersegurança reportados pelos OSE ao CNCS

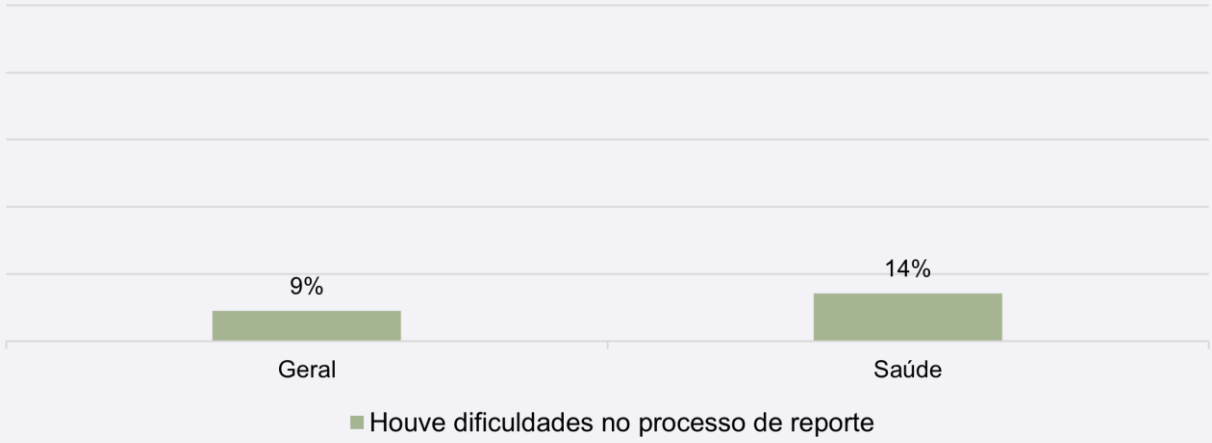


De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n.º 1 do artigo 16.º da Lei n. º46/2018 (RJSC), os OSE estão apenas obrigados à 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 46**.

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

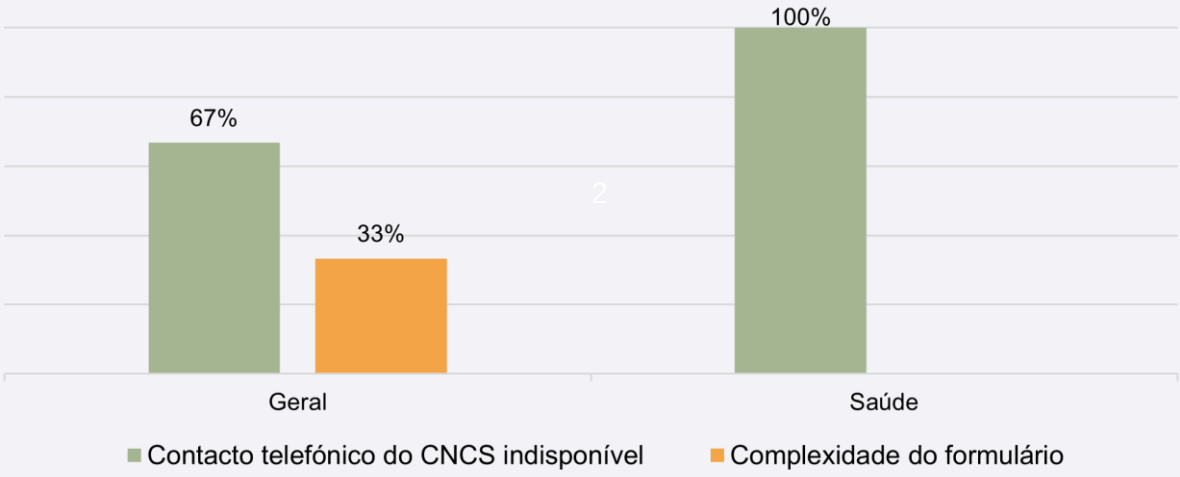
No setor da saúde, observa-se a mesma tendência que na generalidade, onde a maior parte dos operadores notificaram o CNCS. No entanto, como podemos verificar no **Gráfico 46,** em todos os casos onde o incidente não foi notificado, o impacto não foi relevante para a continuidade dos serviços.

Gráfico 42 - Dificuldades no processo de notificação ao CNCS



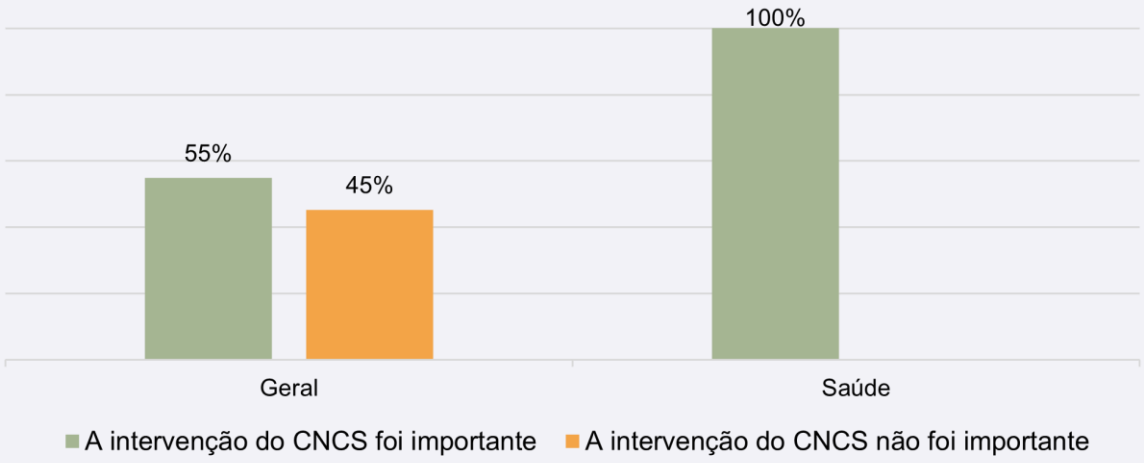
De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação. Apenas 14% dos OSE do setor da saúde mencionaram ter dificuldades no processo de notificação.

Gráfico 43 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS



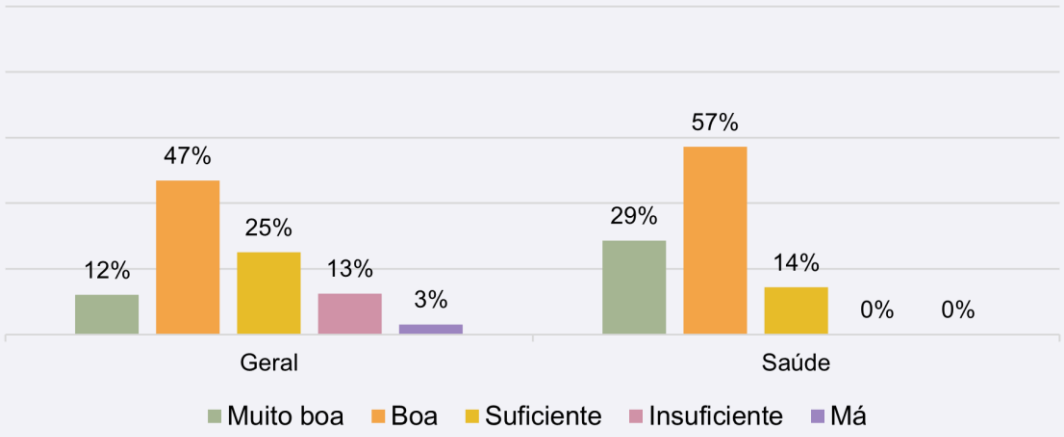
Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico. Note-se, estas percentagens são apenas relativas aos 9% (Geral) e 14% (Saúde) que indicaram ter havido dificuldades na notificação de incidentes.

Gráfico 44 - 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 saúde, é unânime (100%) a opinião de que a intervenção do CNCS foi importante na resolução do incidente notificado.

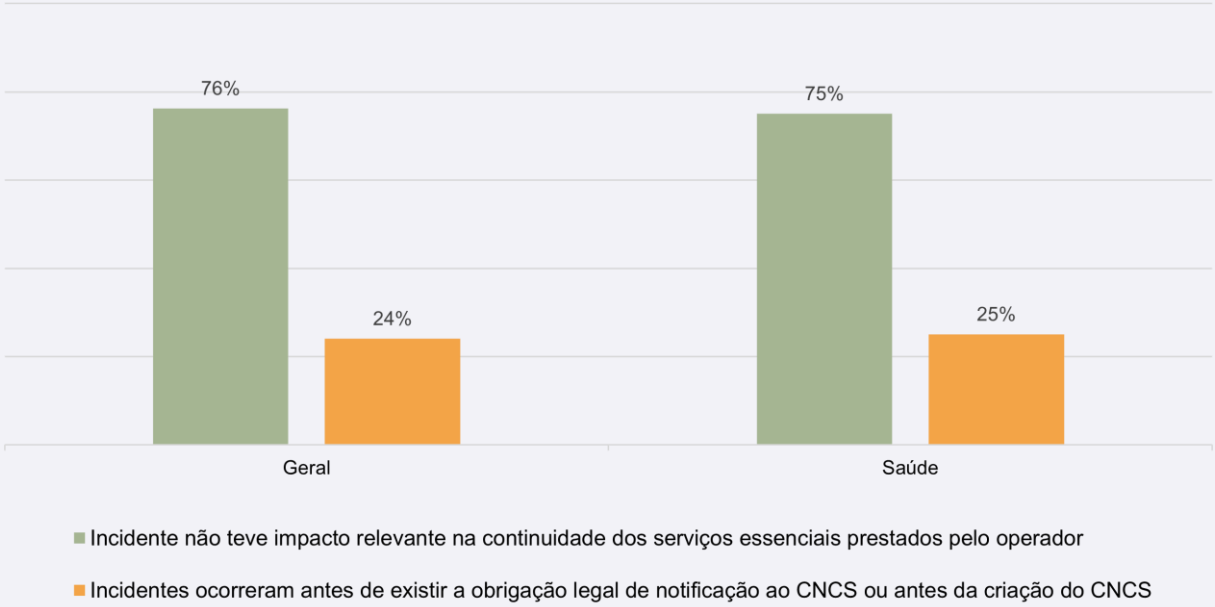
Gráfico 45 - Avaliação da resposta dada pelo CNCS



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%).

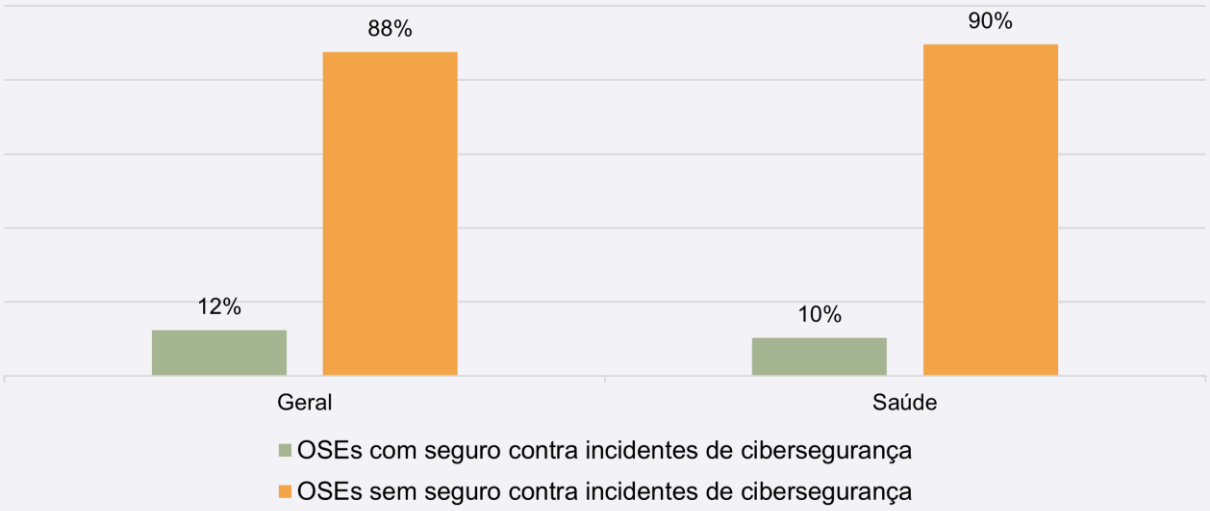
No setor da saúde, a perspetiva geral é novamente positiva, sendo que no caso do setor da saúde 86% classificaram a resposta como boa (57%) ou muito boa (29%) e nenhum OSE do setor classificou a resposta do CNCS como insuficiente ou má.

Gráfico 46 - Motivos para a não notificação de incidentes de cibersegurança ao CNCS



Como referido no **Gráfico 41**, a não notificação dos incidentes foi justificada. O principal motivo para a não notificação de incidentes de cibersegurança ao CNCS, segundo os OSE, foi o facto de o incidente não ter tido impacto na continuidade dos serviços essenciais por si prestados (76%). Nos restantes casos (24%) o incidente ocorreu antes de existir a obrigação legal de notificação ou até mesmo antes da criação do CNCS.

Gráfico 47 - Seguro contra incidentes de cibersegurança

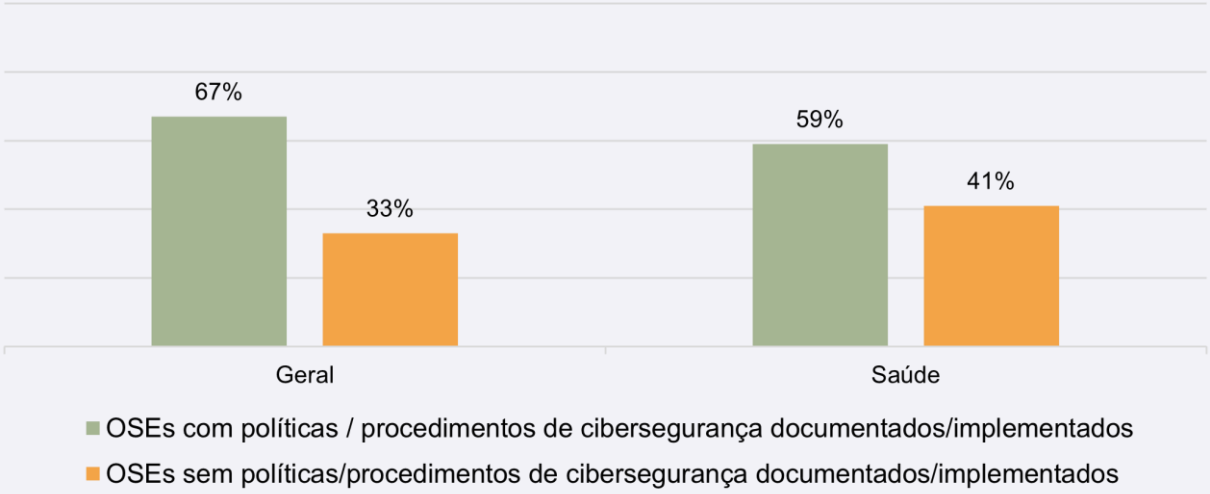


Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. A lógica geral mantém-se no setor da saúde, com a maior parte dos inquiridos a não possuírem este tipo de seguro.

Segundo dados da ENISA (Relatório *NIS Investments* de 2023), cerca de 58% dos inquiridos não tinham qualquer seguro relacionado com cibersegurança. A discrepância entre os valores da ENISA e os obtidos pelo questionário realizado poderá dever-se à composição da amostra, uma vez que a do estudo da ENISA inclui operadores de serviços essenciais e prestadores de serviços digitais. Já o questionário realizado pelo CNCS contemplou apenas operadores de serviços essenciais[41].

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[42].

Gráfico 48 - Documentação/implementação de políticas e procedimentos de cibersegurança

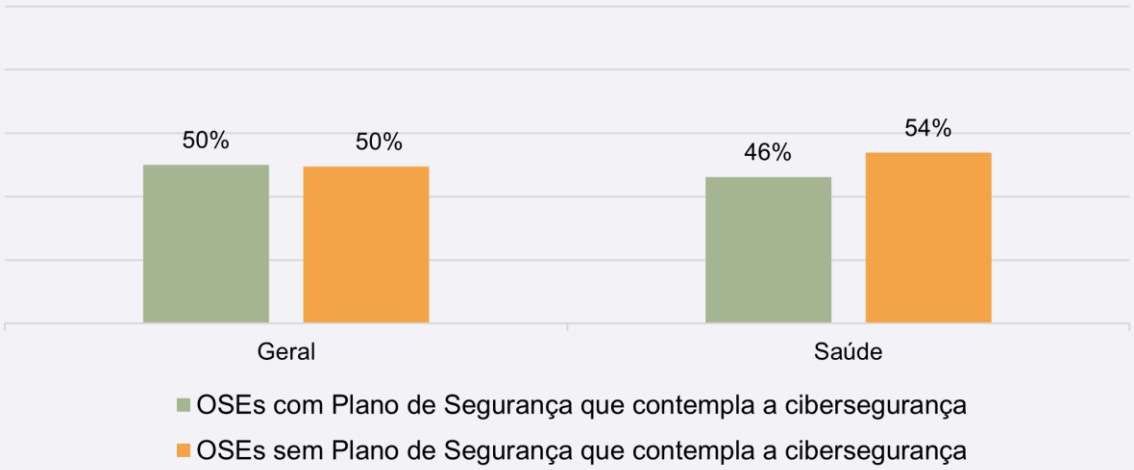


Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados.

No setor da saúde, menos OSE têm políticas e procedimentos de cibersegurança documentados ou implementados do que na generalidade. Ainda assim, a maioria dos operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados. Segundo dados do IUTICE, em 2022, cerca de 54.4% do total de empresas tinha documentos sobre medidas, práticas ou procedimentos em matéria de segurança[43].

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

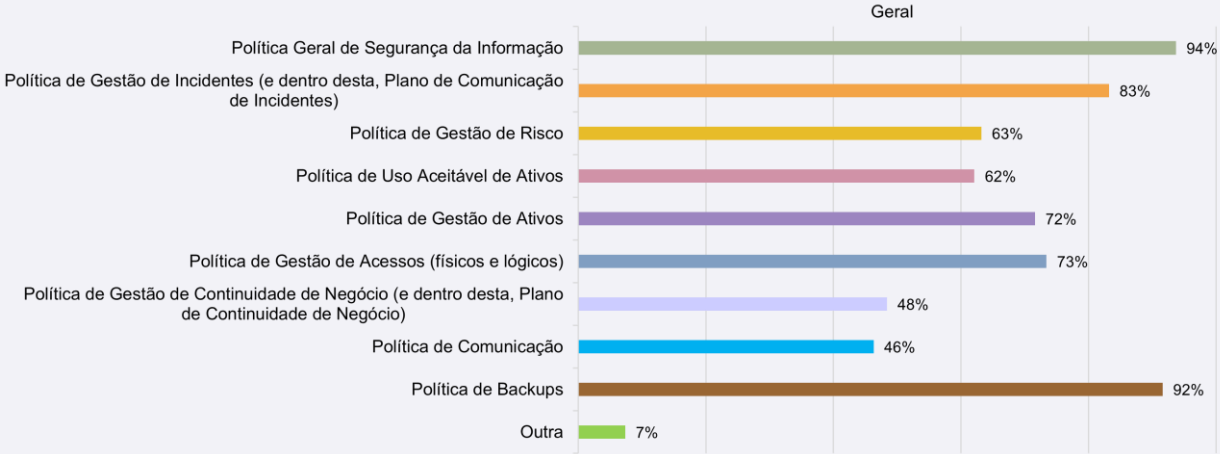
Gráfico 49 - Existência de Plano de Segurança que contemple a cibersegurança



O plano de segurança é obrigatório ao abrigo do decreto-lei n.º 65/2021, de 30 de julho. No entanto, metade dos operadores inquiridos, 50%, ainda não tem um plano de segurança que contemple a área da cibersegurança. O setor da saúde apresenta uma percentagem de OSE com plano de segurança acima dos 40%, mas aquém dos 50%.

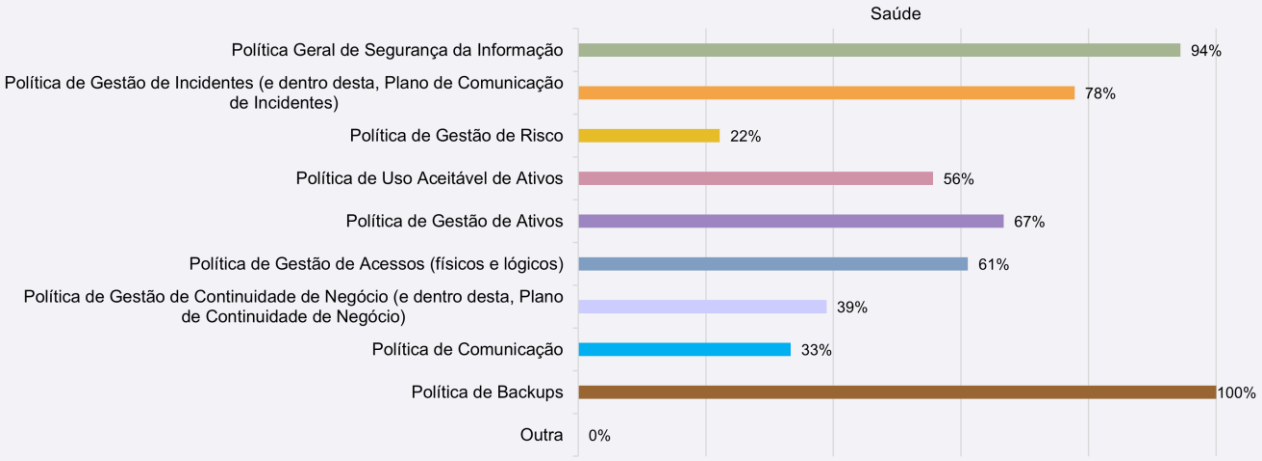
Segundo um estudo realizado pela Microsoft, mais de 40% das empresas inquiridas têm projetado um investimento em cibersegurança. Destas empresas, cerca de 69% irá investir em avaliações regulares de risco de cibersegurança e 66% em auditorias de segurança e monitorização de ameaças em tempo real[44].

Gráfico 50 - Políticas incluídas no Plano de Segurança



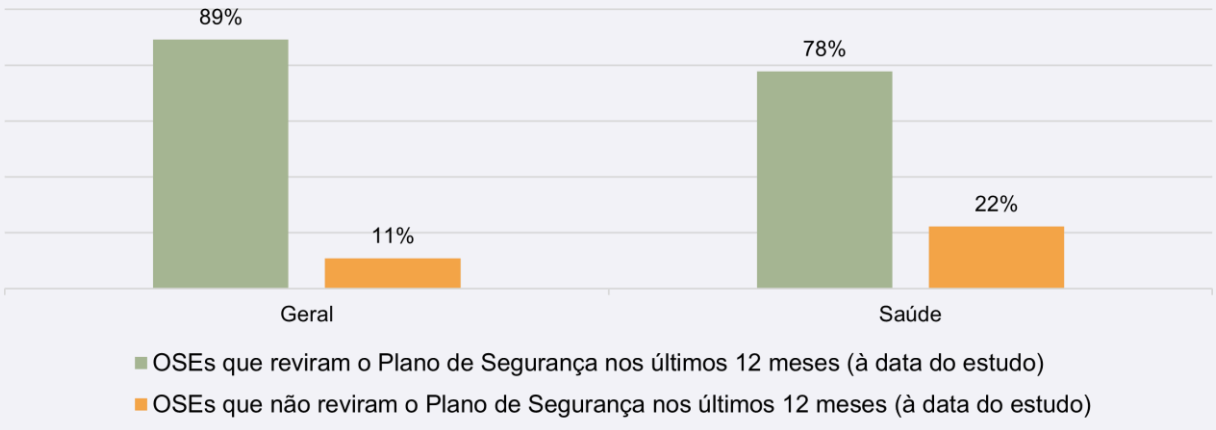
[44] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 5.

Gráfico 50.1 - Políticas incluídas no Plano de Segurança



Os gráficos acima representam a percentagem de operadores com plano de segurança que têm as diversas políticas elencadas elaboradas no âmbito desse mesmo plano.
As políticas mais comuns são a Política de Geral de SI (94%), a Política de Backups (92%), a Política de Gestão de Incidentes (83%), a Política de Gestão de Acessos (73%), a Política de Gestão de Ativos (72%), a Política de Gestão de Risco (63%) e a Política de Uso Aceitável de Ativos (62%). As políticas menos adotadas entre os operadores são a Política de Continuidade de Negócio (48%) e a Política de Comunicação (46%).
Entre as "outras" políticas (7%), contam-se a Política de Utilização de Correio Eletrónico, Política de *Passwords*, Política de Teletrabalho, Política de Classificação e Manuseamento de Informação, Política de Segurança Física, Política de Gestão de Alterações, Política de Criptografia, Política de Recursos Humanos para a Cibersegurança e Política de Privacidade e Proteção de Dados.
No caso do setor da saúde, todos os OSE inquiridos indicaram ter Política de *Backups*, 94% ter Política de Segurança da Informação e 78% ter Política de Gestão de Incidentes. Já menos de 50% têm Política de Gestão de Continuidade de Negócio (39%), Política de Comunicação (33%) ou Política de Gestão de Risco (22%).

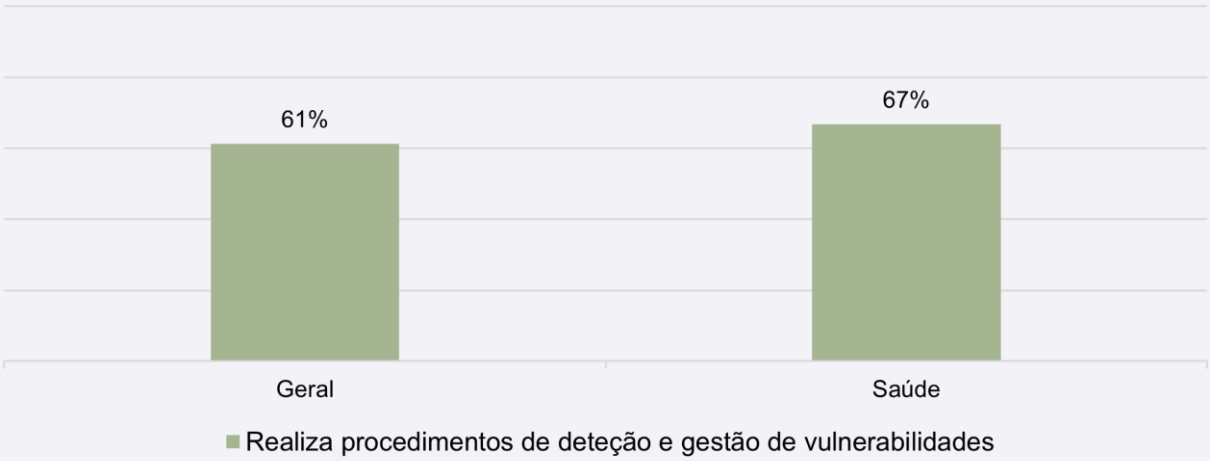
Gráfico 51 - Revisão do Plano de Segurança



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 setor da saúde (e o segundo o da energia), houve menos de 80% dos OSE a rever o seu Plano de Segurança nos últimos 12 meses, nomeadamente 78% à data do estudo.

Ainda assim, a revisão dos Planos de Segurança por parte dos OSE apresenta melhores resultados do que quando comparados com o restante tecido empresarial português. 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[45].

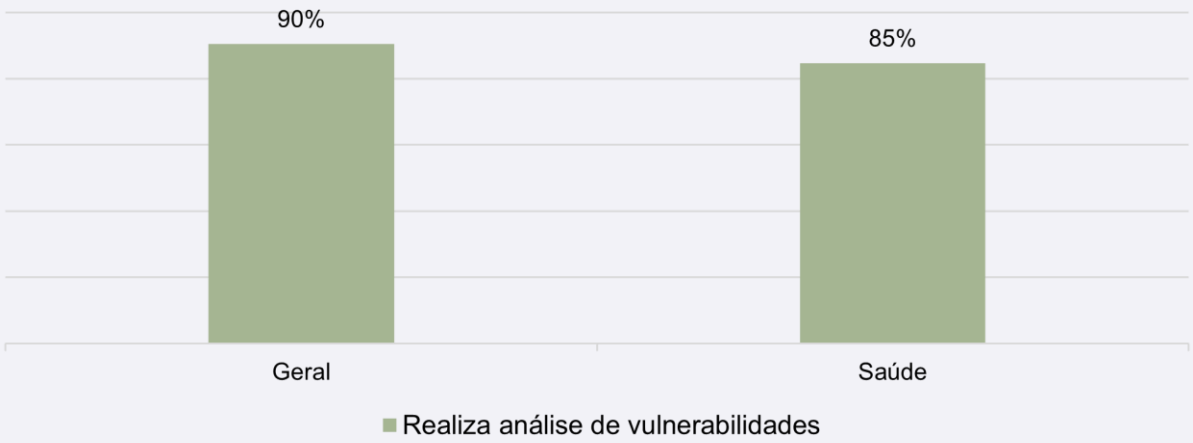
Gráfico 52 - OSE que realizam procedimentos de deteção e gestão de vulnerabilidades



Mais de 60% dos operadores inquiridos dos diferentes setores referem realizar procedimentos de deteção e gestão de vulnerabilidades. No setor da saúde, a percentagem de operadores que realiza estes procedimentos ultrapassa os 60%.

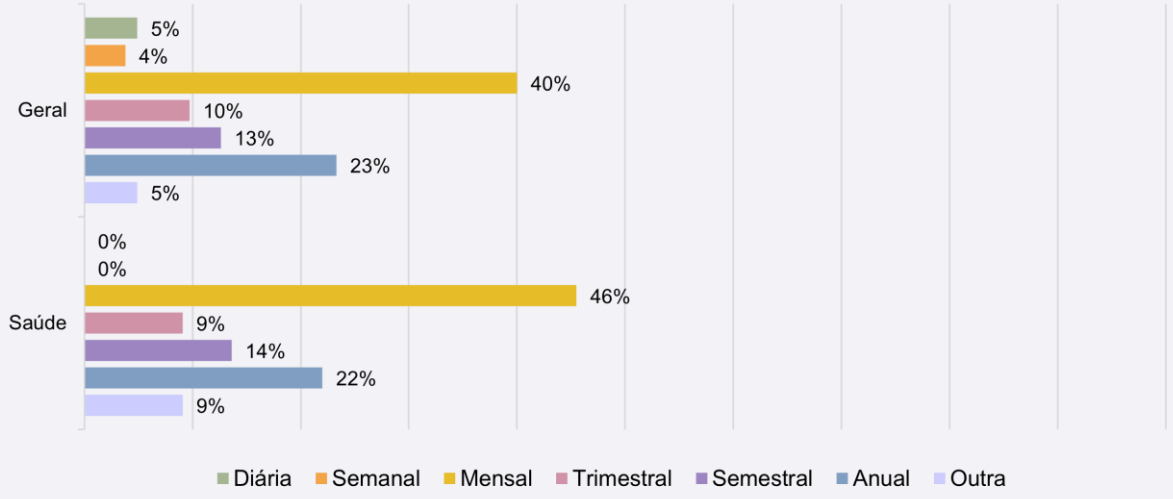
[45] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

Gráfico 53 - OSE que dentro dos procedimentos de deteção e gestão de vulnerabilidades realizam análise de vulnerabilidades



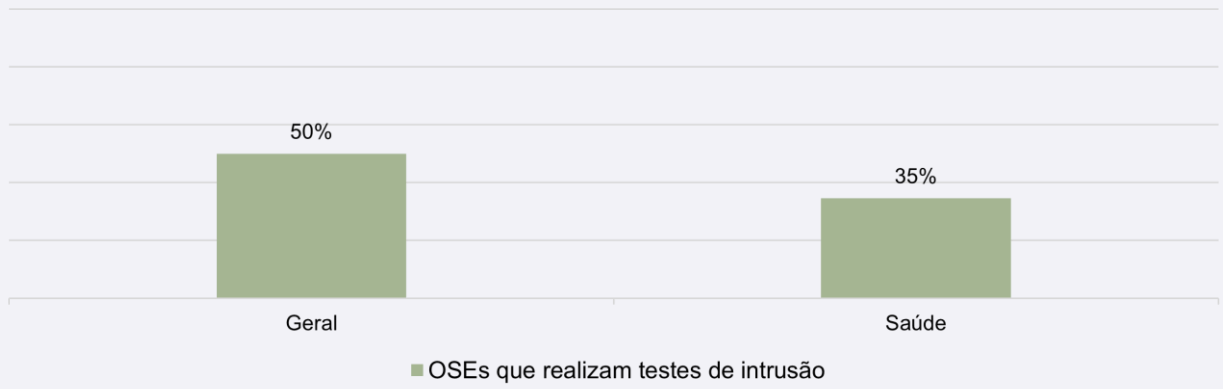
Entre os operadores que realizam procedimentos de deteção e gestão de vulnerabilidades, a vasta maioria (90%) faz também a análise das mesmas. No setor da saúde, embora a análise de vulnerabilidades não seja realizada por todos os operadores de cada setor, esta é realizada por pelo menos 85% dos operadores inquiridos.

Gráfico 54 - Frequência da análise de vulnerabilidades



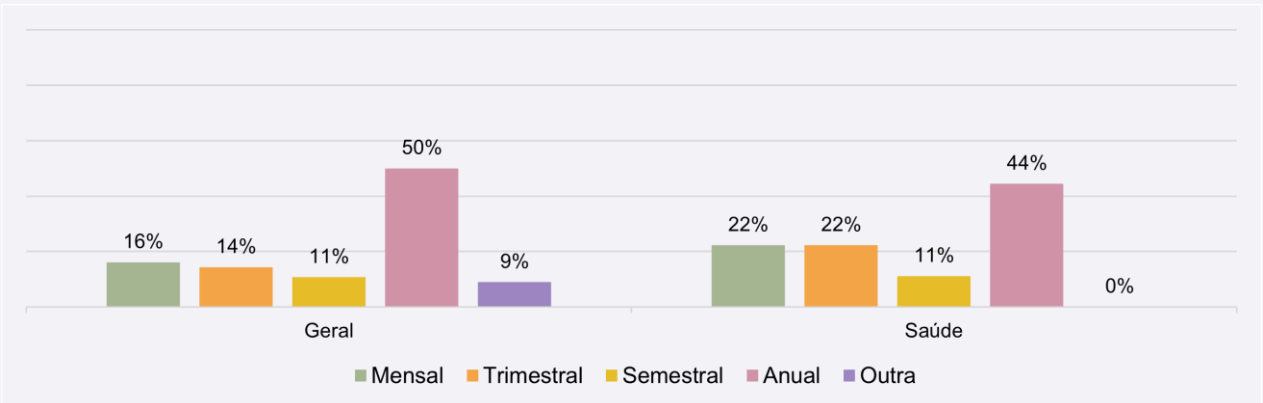
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral. No setor da saúde, nenhum OSE referiu realizar análises de vulnerabilidades de frequência diária ou semanal.

Gráfico 55 - Realização de testes de intrusão



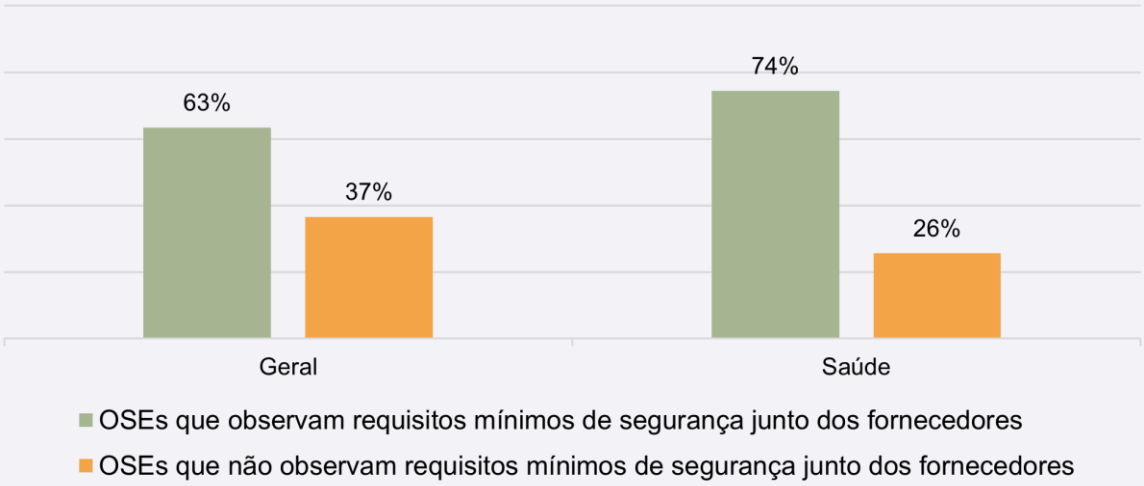
Na apreciação geral, é possível verificar uma igual divisão entre os OSE que realizam testes de intrusão e os que não realizam esses testes (50%-50%). Já no setor da saúde, os OSE que realizam estes testes encontram-se em minoria, não ultrapassando os 35%.

Gráfico 56 - Frequência de testes de intrusão



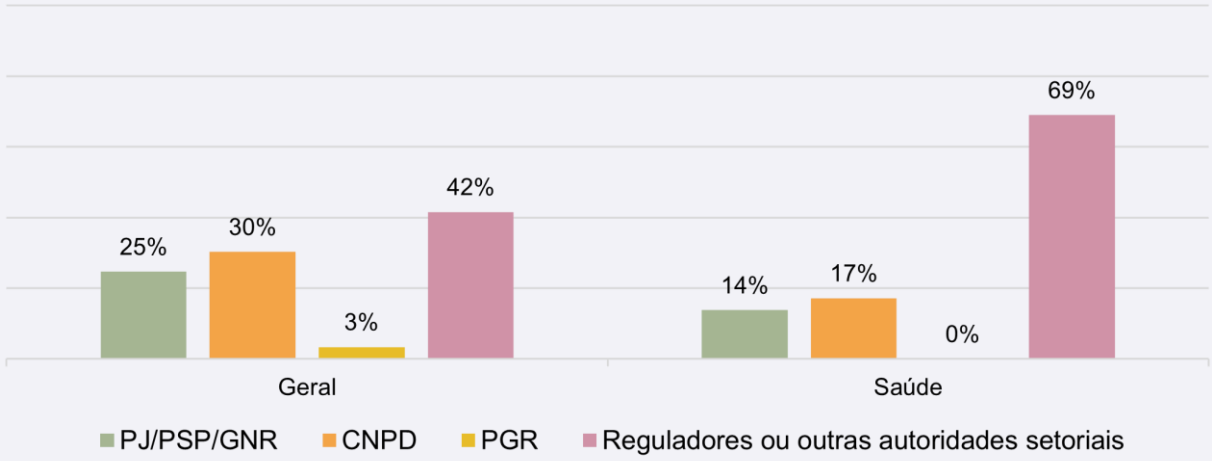
Pelo menos 50% dos OSE inquiridos realiza testes de intrusão anualmente. No setor da saúde prevalece também a frequência anual para estes testes, embora ainda haja OSE a realizarem-nos mais frequentemente (mensalmente, trimestralmente e semestralmente).

Gráfico 57 - Observação de requisitos mínimos e segurança por parte dos fornecedores em contexto de cadeia de abastecimento



Na generalidade, a maioria dos OSE (mais de 60%) procura que os seus fornecedores estejam alinhados com os requisitos mínimos de segurança por si exigidos. O setor da saúde apresenta, neste ponto, melhores resultados que a generalidade dos OSE, com quase 75% dos OSE do setor a procurarem ter os seus requisitos de segurança cumpridos pelos seus fornecedores.

Gráfico 58 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS



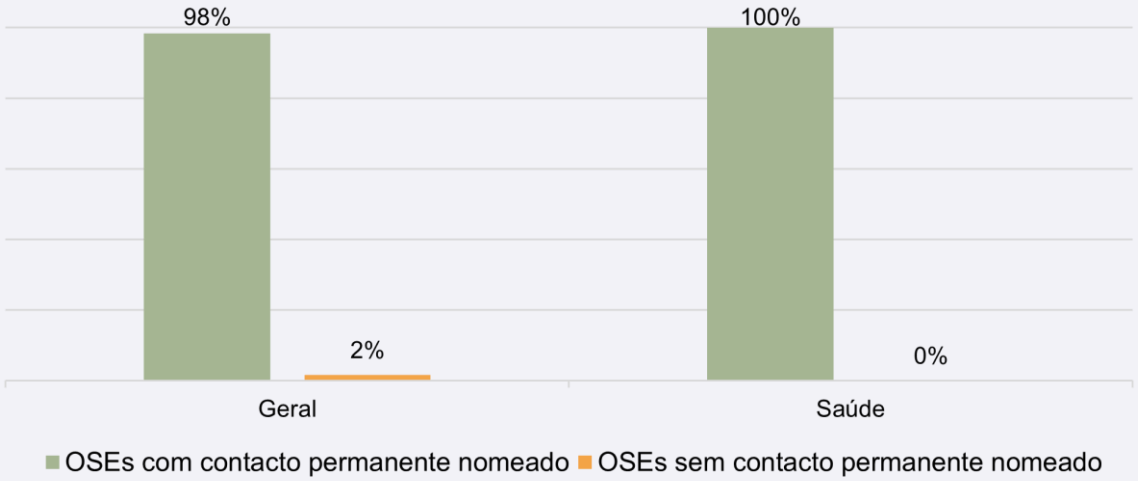
Embora não seja obrigatório em todos os setores, cerca de 40% dos operadores optam por notificar as entidades reguladoras do seu setor ou outras autoridades setoriais caso sofram um ciberataque ou incidente de cibersegurança.

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.

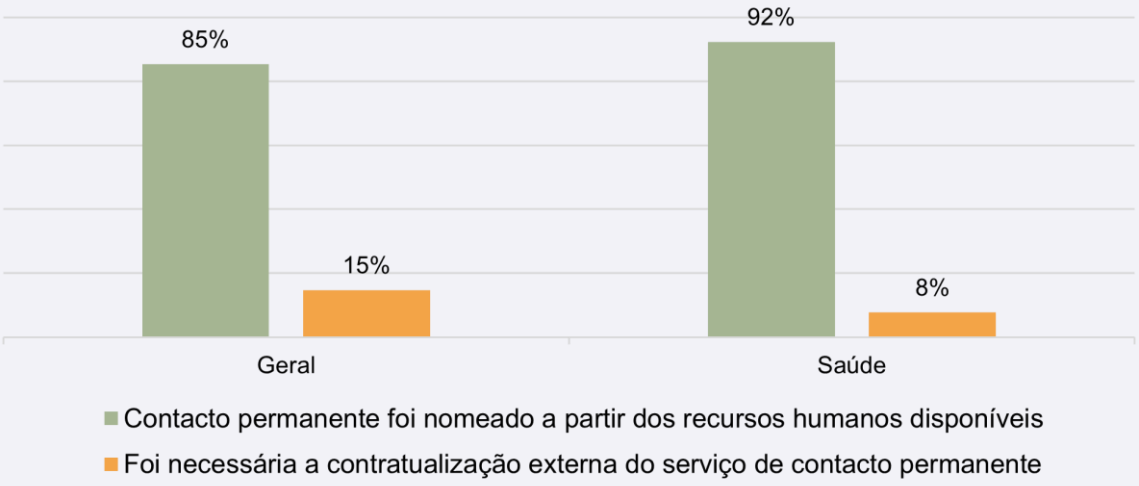
No setor da saúde, é notório que a maioria dos OSE (69%) optam por notificar as entidades reguladoras ou outras entidades setoriais. Já a notificação à CNPD ou às forças de segurança é feita por menos de 20% dos OSE do setor.

Gráfico 59 - Nomeação do contacto permanente que assegura os fluxos de informação de nível operacional e técnico com o CNCS



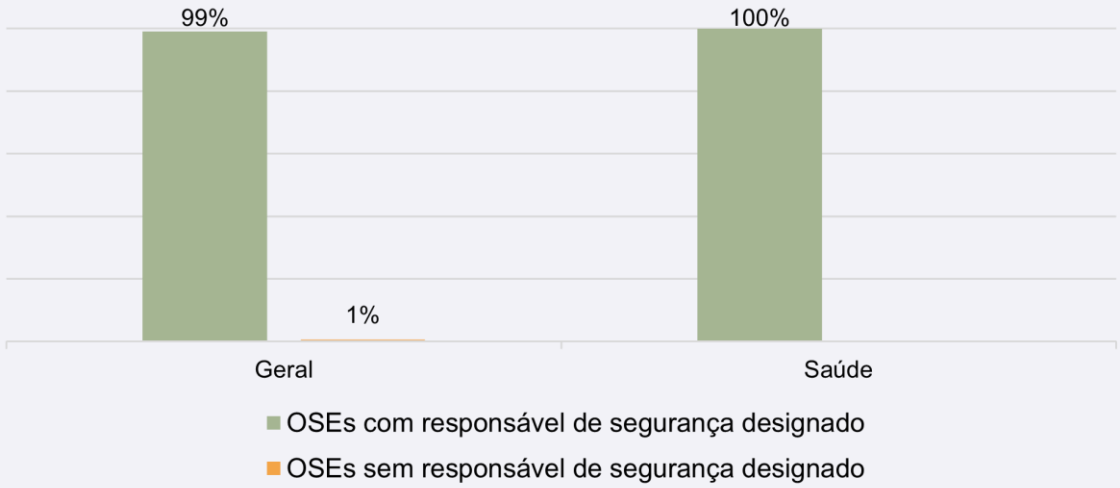
Praticamente todos os OSE inquiridos têm o seu contacto permanente com o CNCS nomeado. No setor da saúde, todos os inquiridos tinham nomeado o seu contacto permanente junto do CNCS.

Gráfico 60 - Designação do contacto permanente



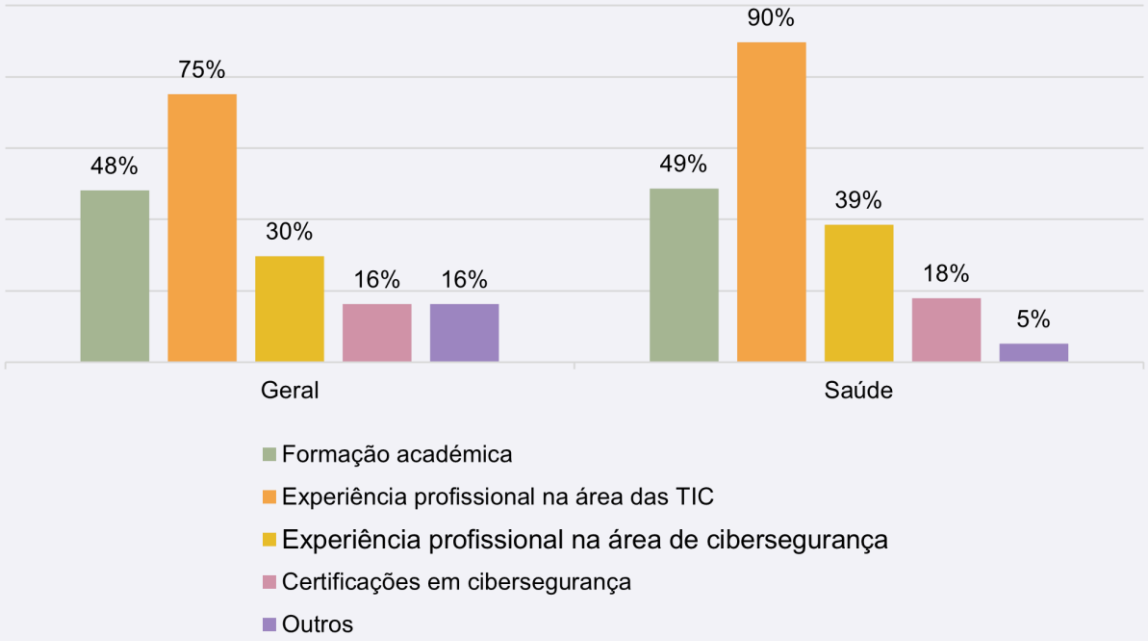
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No setor da saúde, a percentagem de OSE que nomearam o contacto permanente a partir dos seus recursos internos foi superior à da generalidade (92%).

Gráfico 61 - 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 e é totalmente cumprido pelos OSE do setor da saúde.

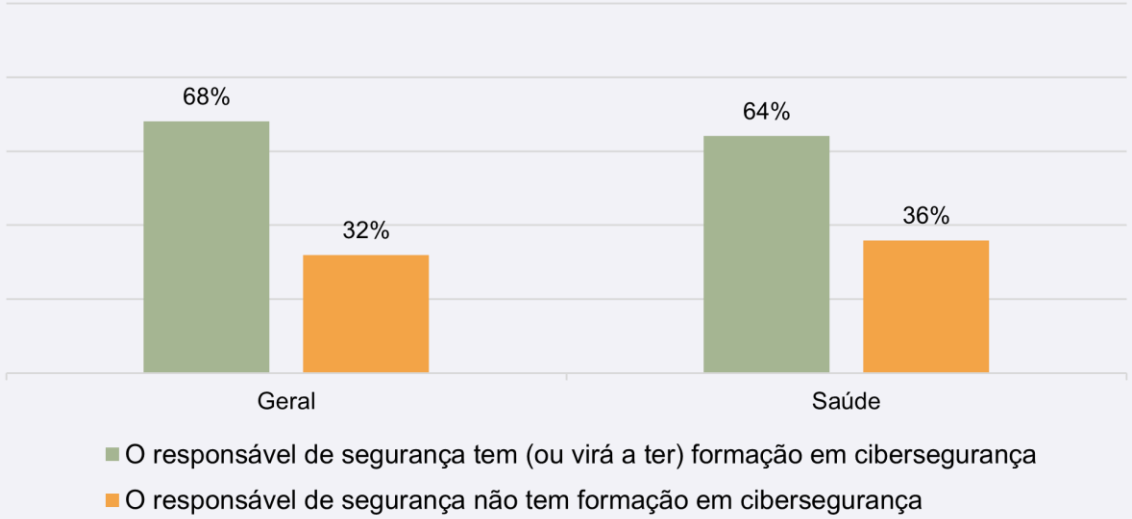
Gráfico 62 - Critérios utilizados para a designação do responsável de segurança



A formação académica e a experiência profissional na área das TIC e na área de cibersegurança foram os critérios mais importantes para a designação do responsável de segurança dos operadores. Na generalidade, a experiência profissional nas TIC foi um critério em 75% dos casos, a formação académica foi um critério em 43% dos casos e a experiência profissional em cibersegurança foi também critério em 30% dos casos. No setor da saúde predomina a experiência profissional na área das TIC como critério utilizado.

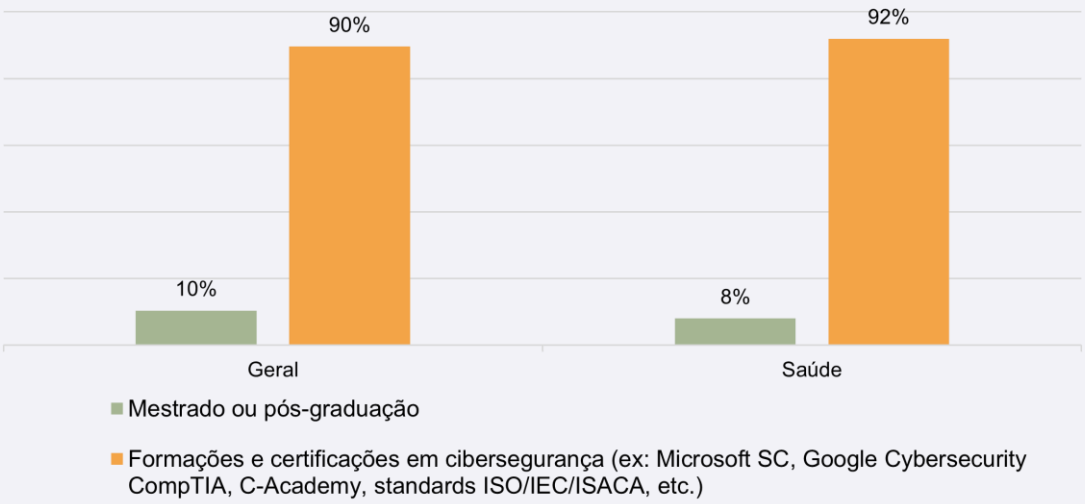
É também importante referir que se verificaram, casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de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

Gráfico 63 - 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. Nos setores bancário e das infraestruturas do mercado financeiro, todos os responsáveis de segurança designados têm ou virão a ter formação nesta área.
O setor da saúde é um dos quais onde mais se verificam operadores cujo responsável de segurança não tem formação em cibersegurança. Mais de 30% dos responsáveis de segurança não têm formação na área, nem está planeado que venham a ter proximamente.

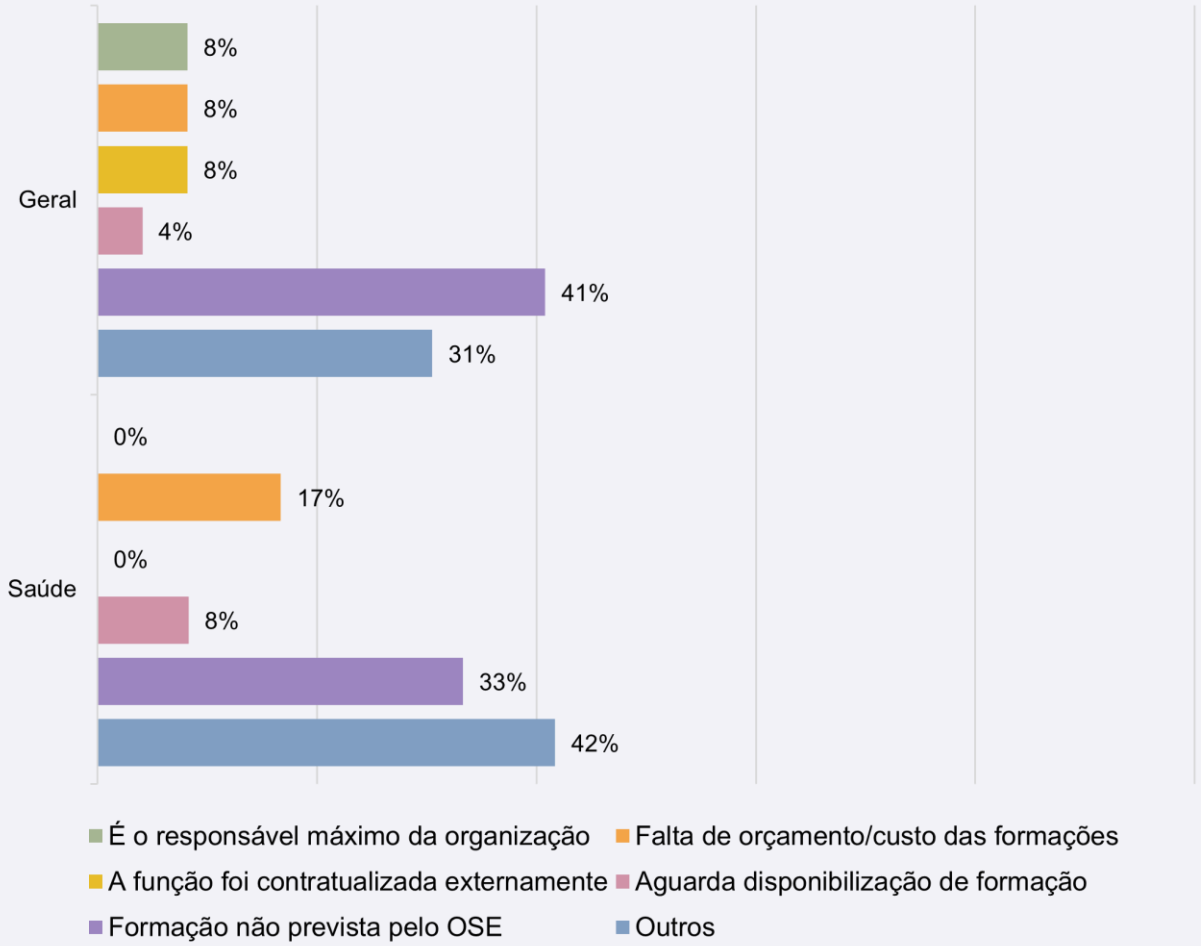
Gráfico 64 - Tipo de formação específica em cibersegurança



As formações e certificações em cibersegurança, tais como as formações *Microsoft Security Certifications, Google Cybersecurity, CompTIA*, da *C-Academy* do CNCS e em normas internacionais como a ISO/IEC 27001 são visivelmente mais comuns entre os responsáveis de segurança do que as formações universitárias como mestrados ou pós-graduações em cibersegurança. Cerca de 90% dos responsáveis de segurança tem uma mais das formações do primeiro tipo.

No setor da saúde apenas 8% é referente a mestrados ou pós-graduações.

Gráfico 65 - 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.

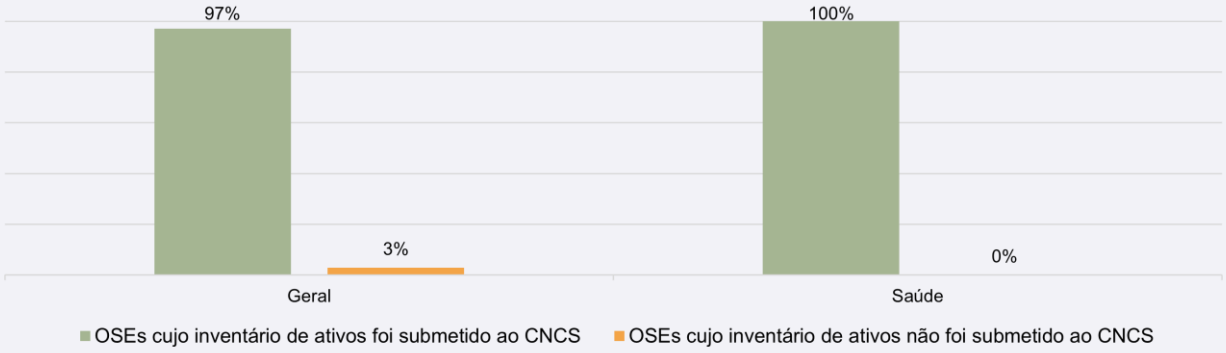
No setor da saúde, as principais motivações para que o responsável de segurança não tenha formação específica em cibersegurança são o facto de ainda não ter completado as formações necessárias, estar em fase de recrutamento, a formação não estar prevista, falta de orçamento/custo das formações e aguardar a disponibilização de formação.

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 66 - Inventário de ativos essenciais elaborado e atualizado

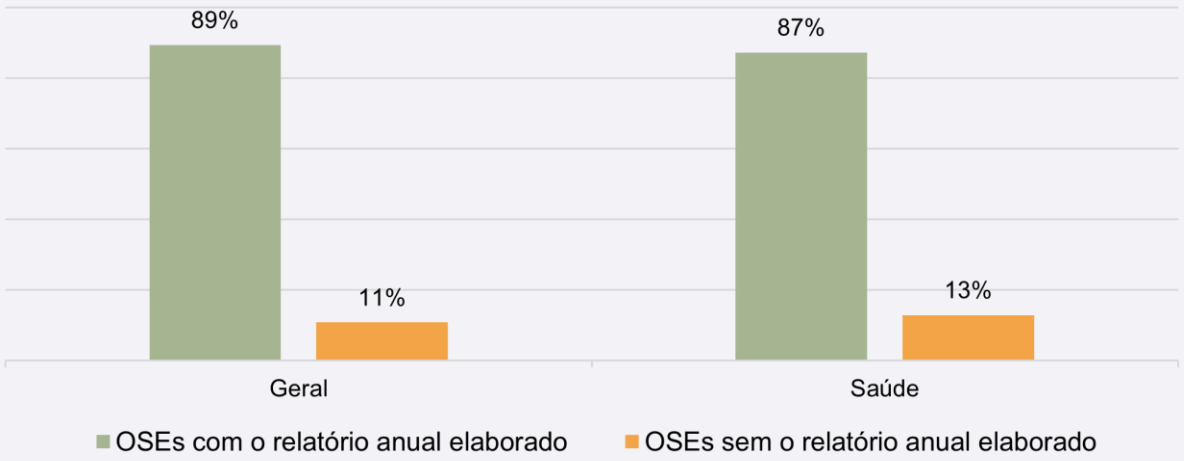
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. Destacam-se os setores da energia, o bancário e o setor das infraestruturas do mercado financeiro, nos quais todos os operadores têm o seu inventário elaborado e atualizado. Verificam-se exceções no setor da saúde, onde a percentagem de operadores cujo inventário de ativos essenciais é elaborado

Gráfico 67 - Submissão do inventário de ativos ao CNCS



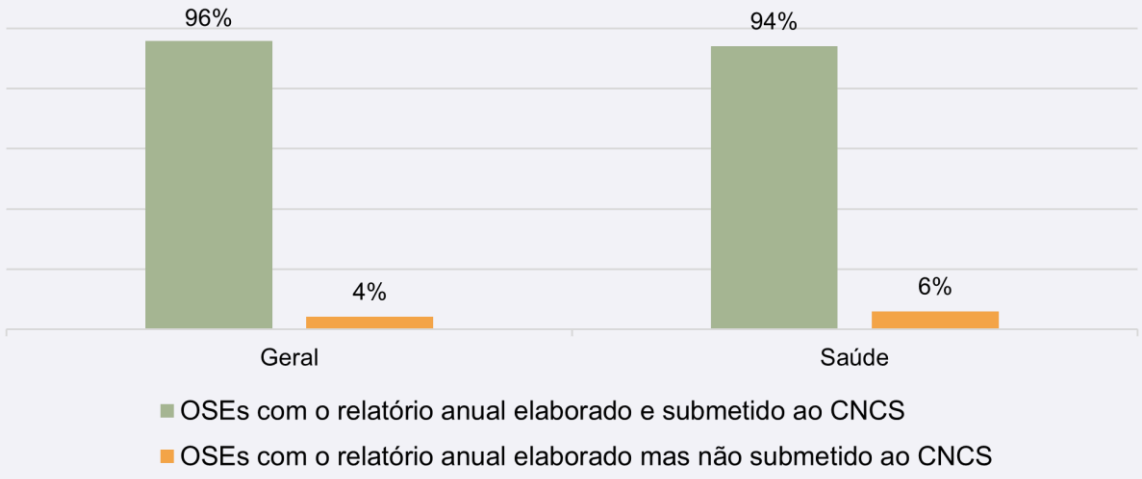
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. No setor da saúde, todos os operadores com inventário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

Gráfico 68 - Elaboração do relatório anual previsto pelo Decreto-Lei n.º 65/2021, de 30 de julho



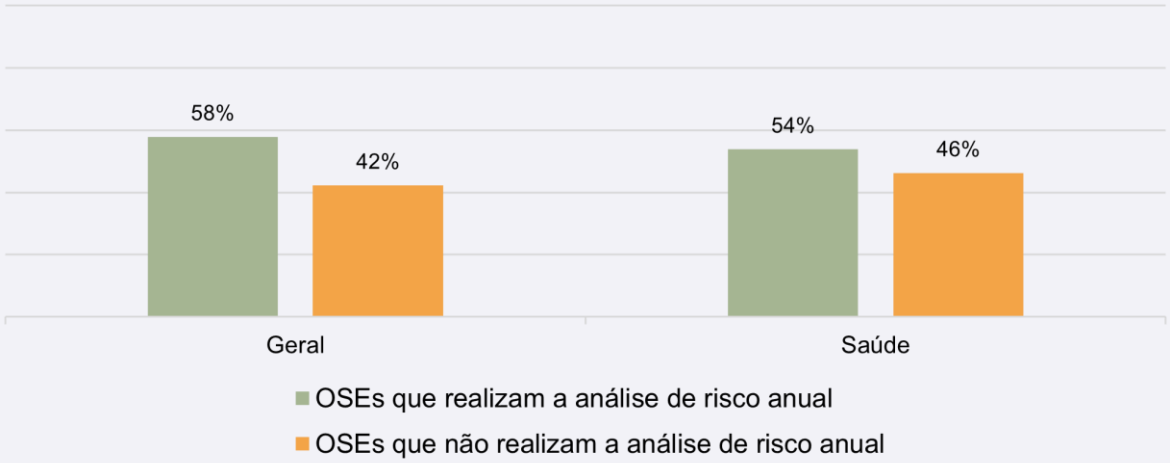
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo Decreto-Lei n.º 65/2021. No setor da saúde, 13% dos OSE não apresenta relatório anual elaborado.

Gráfico 69 - Submissão do relatório anual ao CNCS



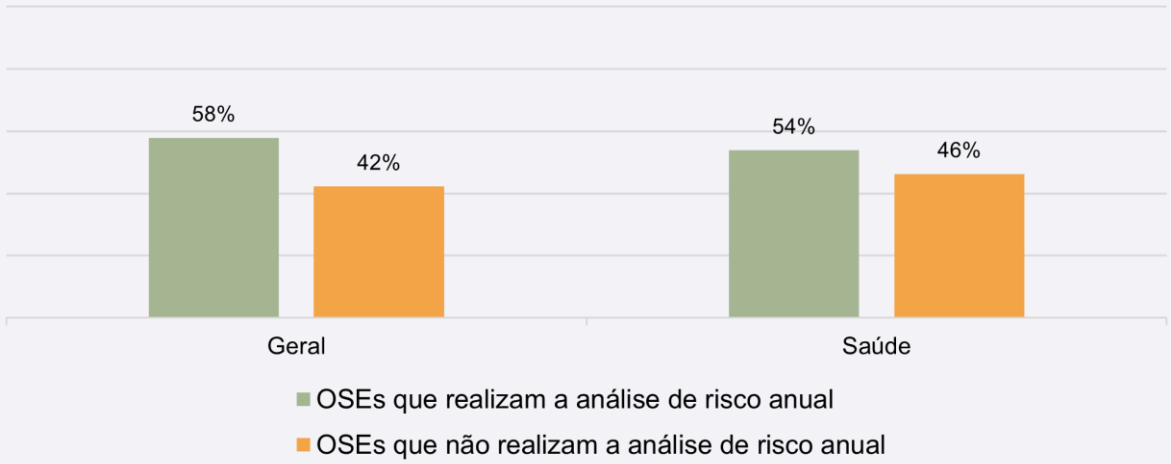
Entre os operadores que elaboraram o relatório anual exigido pelo Decreto-Lei, 96% submeteram-no ao CNCS. No setor da saúde esta percentagem foi de 94%.

Gráfico 70 - Realização de análise de riscos anual no âmbito de cibersegurança



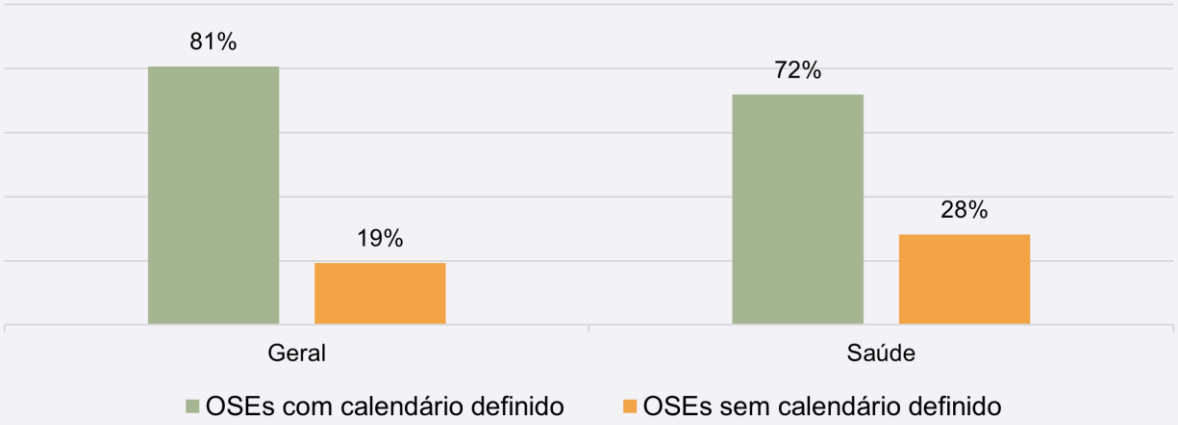
A realização anual de uma análise dos riscos relativa a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos OSE é uma outra obrigação legal decorrente do Decreto-Lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. No setor da saúde, a percentagem de OSE que não realiza a análise de risco é superior à da generalidade, fixando-se nos 46%.

Gráfico 71 - Plano de Resposta a Incidentes de Cibersegurança



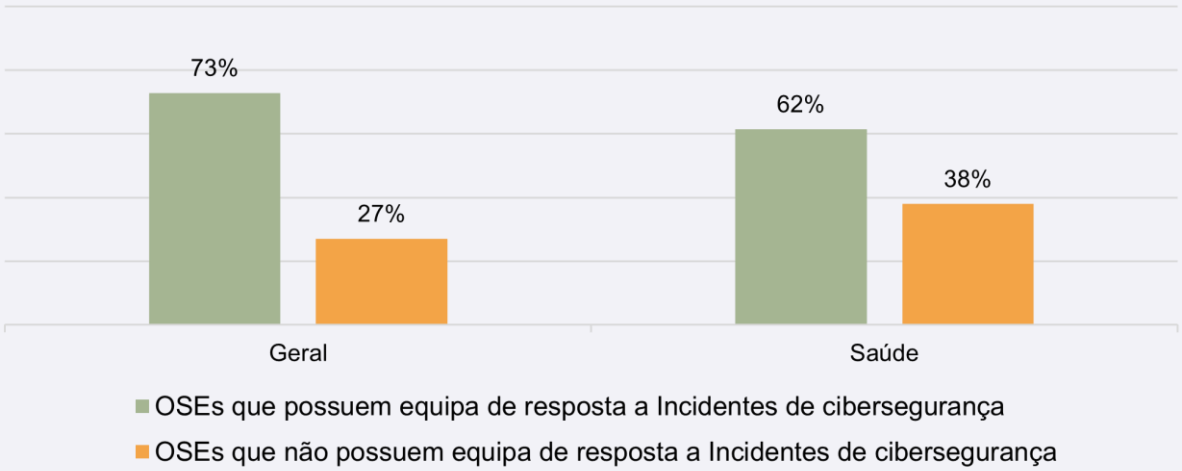
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. No setor da saúde verificam-se mais de 50% dos operadores com plano de resposta a incidentes.

Gráfico 72 - Definição de calendário para cumprimento das obrigações decorrentes do Decreto-Lei n.º 65/2021, de 30 de julho



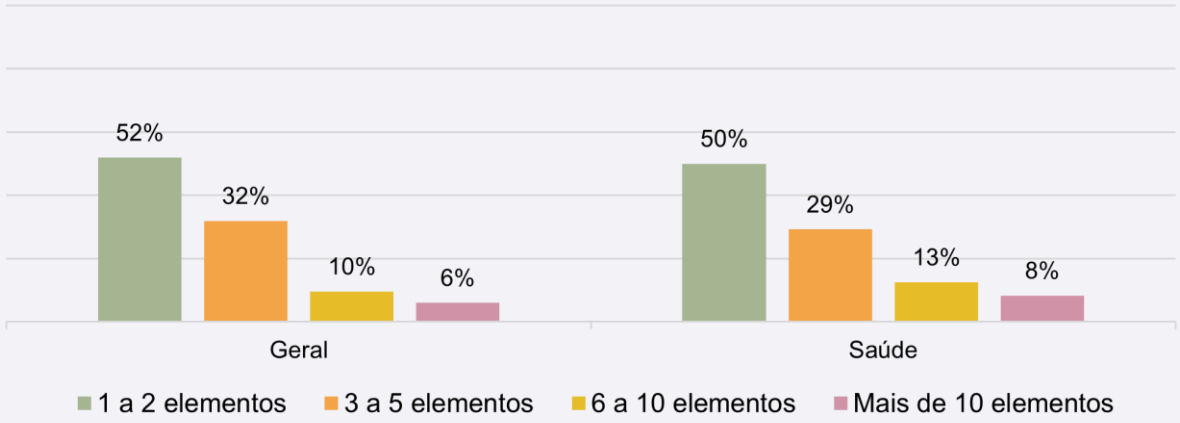
A maioria dos OSE (81%) procura definir um calendário para auxílio no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. O setor da saúde foi o setor onde menor percentagem de OSE define esse calendário, chegando ainda assim aos 72%.

Gráfico 73 - Equipa de resposta a incidentes de cibersegurança



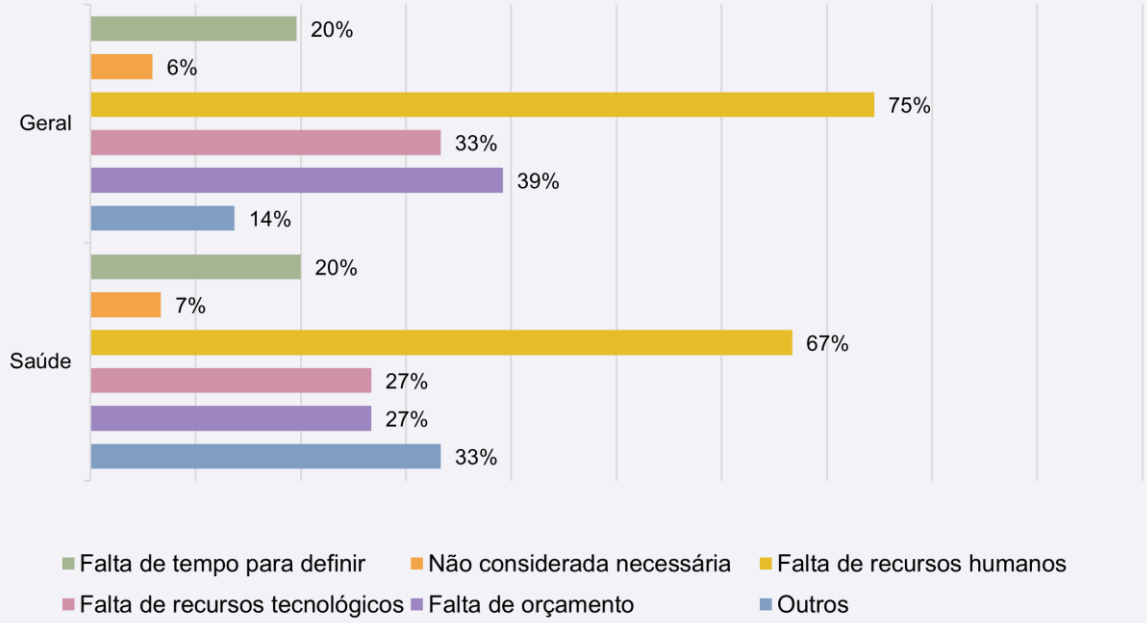
A nível geral, 73% dos OSE possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de OSE que possui tal equipa é sempre superior a 60%. O setor da saúde é aquele onde menos OSE têm equipa de resposta a incidentes, fixando-se nos 62%.

Gráfico 74 - Composição da equipa de resposta a incidentes de cibersegurança



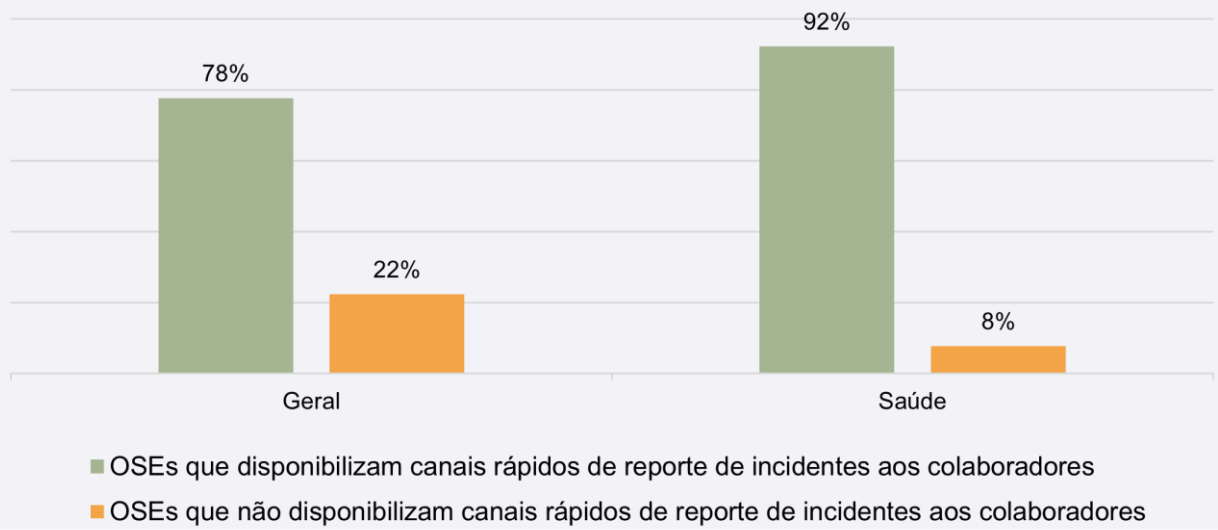
Na visão geral, 52% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, a prevalência de equipas de resposta a incidentes com 1 a 2 elementos repete-se no setor da saúde (50%). O setor da Saúde é também um dos setores que mais diversidade apresenta na composição das equipas.

Gráfico 75 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança



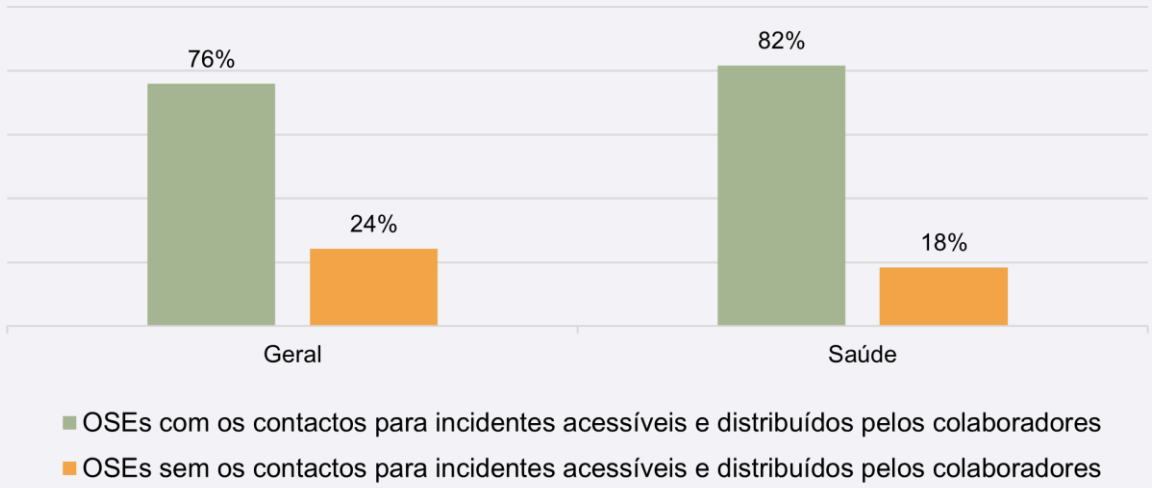
O principal motivo para que os OSE não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores sem equipa de resposta a incidentes. Os OSE que não consideram necessária uma equipa de resposta a incidentes necessária são, no cômputo geral, menos de 10%. Os OSE 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. O setor da saúde reflete os resultados da generalidade com algumas variações percentuais e com a exceção de haver uma percentagem mais elevada de OSE a indicar “Outros” motivos para a não existência de equipas de resposta a incidentes de cibersegurança.

Gráfico 76 - Disponibilização aos colaboradores de canais rápidos para reporte de incidentes



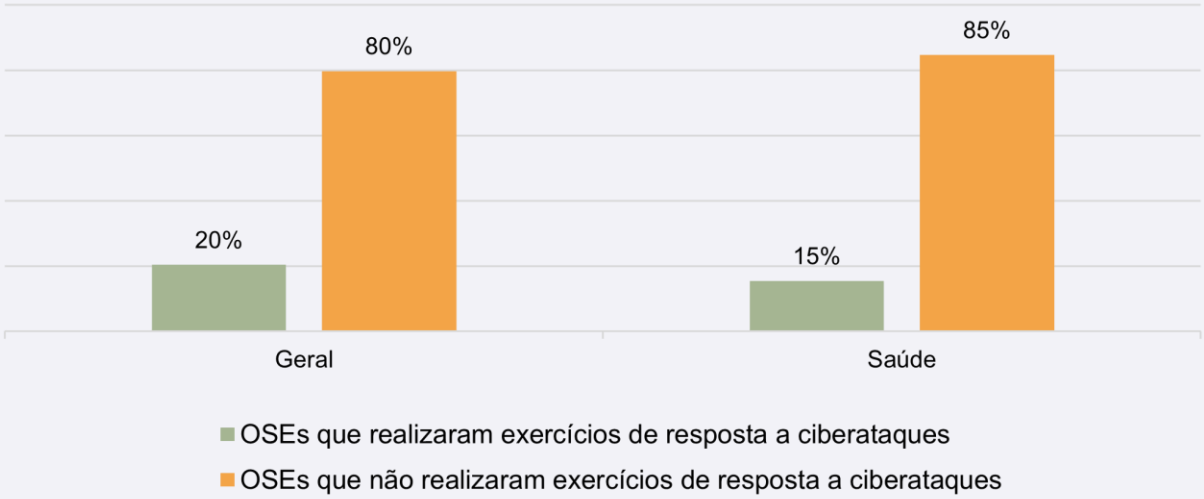
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. No setor da saúde 92% de operadores que disponibiliza estes canais.

Gráfico 77 - Acessibilidade e distribuição por todos os colaboradores dos contactos a utilizar em caso de incidente de cibersegurança



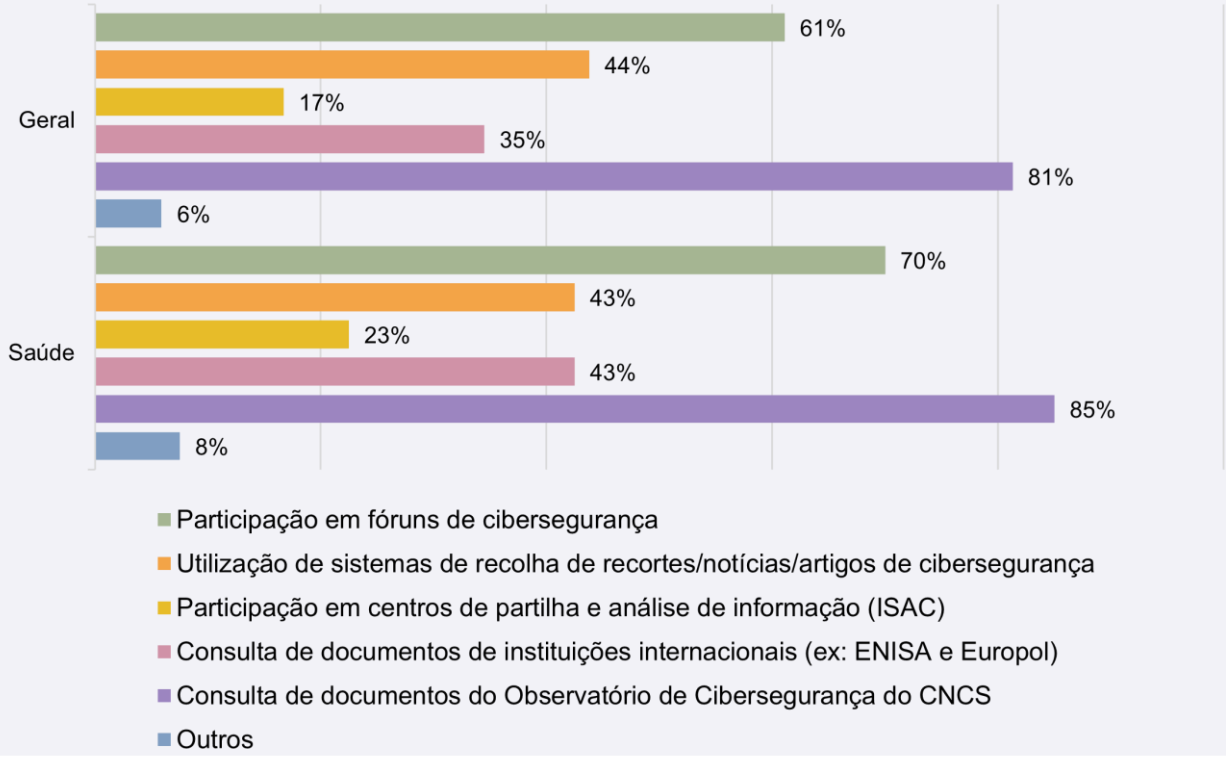
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. Sectorialmente, na saúde, 82% dos operadores têm estes contactos distribuídos e acessíveis por todos os colaboradores.

Gráfico 78 - 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 saúde, a percentagem de OSE que realizam estes exercícios é inferior à da generalidade, com apenas 15% a realizarem-nos.

Gráfico 79 - 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[46]. No setor da saúde, verificam-se variações percentuais positivas nos hábitos de recolha de informação sobre riscos e incidentes de cibersegurança face à visão geral, ou seja, percentualmente, há mais OSE a recorrer às diferentes fontes de informação elencadas do que na generalidade, com uma pequena exceção na utilização de sistemas de recolha de recortes/notícias/artigos, que no setor da saúde é 1 p.p. mais baixo do que na visão geral.

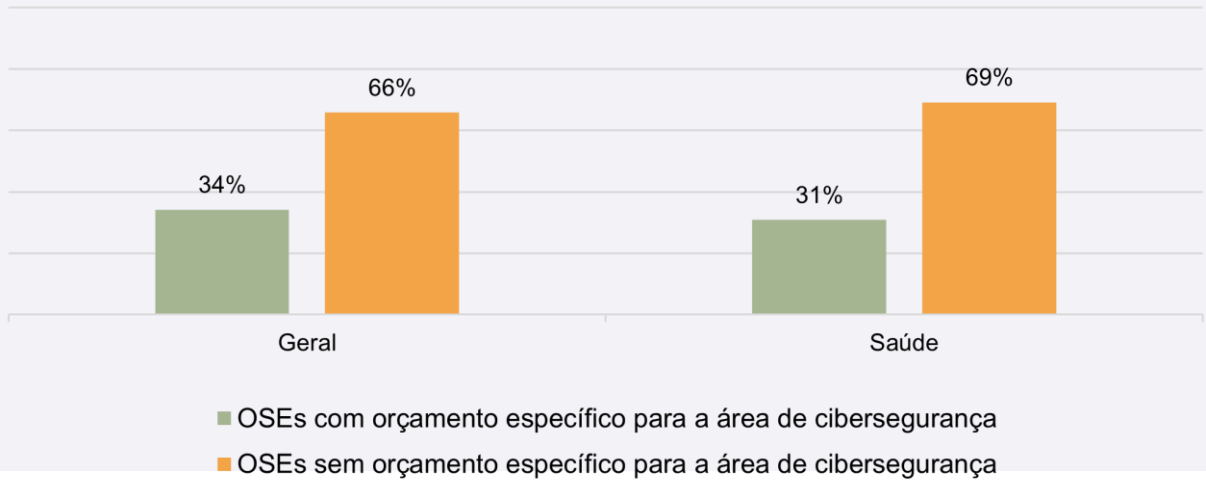
A baixa participação registada nos ISACs merece alguma reflexão. Estes centros de análise e partilha de informação "consistem em parcerias para troca de informação e experiência, assentes no pressuposto de que a partilha consistente de informação e análise de incidentes, ameaças, tendências e boas práticas favorece a resiliência digital individual e coletiva"[47].

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

O próprio CNCS dinamiza seis ISACs, nomeadamente nos seguintes setores: energia, águas, portos marítimos; *media*; retalho e distribuição; e saúde. O CNCS dinamiza também um ISAC regional na Região Autónoma dos Açores. Há ainda um outro ISAC do setor financeiro, do qual o CNCS é membro, mas não promotor[48].

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[49]. 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*)[50]. 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[51].

Gráfico 80 - Orçamento específico para a área de cibersegurança



Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. No setor da saúde, têm orçamento cerca de 31% dos operadores.

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

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

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

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

O Relatório *NIS Investments* de 2021 foi o último relatório da série da ENISA a analisar a questão de um orçamento específico para a cibersegurança, tendo os últimos dois relatórios, de 2022 e 2023, orientado o seu foco para orçamentos dedicados a riscos terceiros (*third-party risk*) e à formação em cibersegurança, respetivamente. No relatório de 2021, os resultados verificados ao nível da UE são próximos dos obtidos a nível nacional no questionário realizado pelo CNCS: na UE, apenas cerca de 38% dos OSE inquiridos tinham orçamentos dedicados à cibersegurança[52], próximo dos 33% registados pelo CNCS. O mesmo relatório indica que a maioria dos OSE aloca fundos à cibersegurança a partir do orçamento dedicado à parte informática.

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSE a ter orçamentos específicos para cibersegurança. No entanto, um estudo da Comissão Europeia e do Banco Europeu de Investimento (BEI) sobre a criação de uma plataforma de investimento em cibersegurança constatou que a ausência desses orçamentos específicos dificulta grandemente a análise do investimento realizado nesta área. Segundo o mesmo estudo, a própria UE não tinha, no ano de 2022, um orçamento dedicado ao financiamento da sua estratégia de cibersegurança[53]. 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[54]. 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[55].

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

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

[54] 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.

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

Gráfico 81 - Áreas de aplicação dos orçamentos específicos para cibersegurança

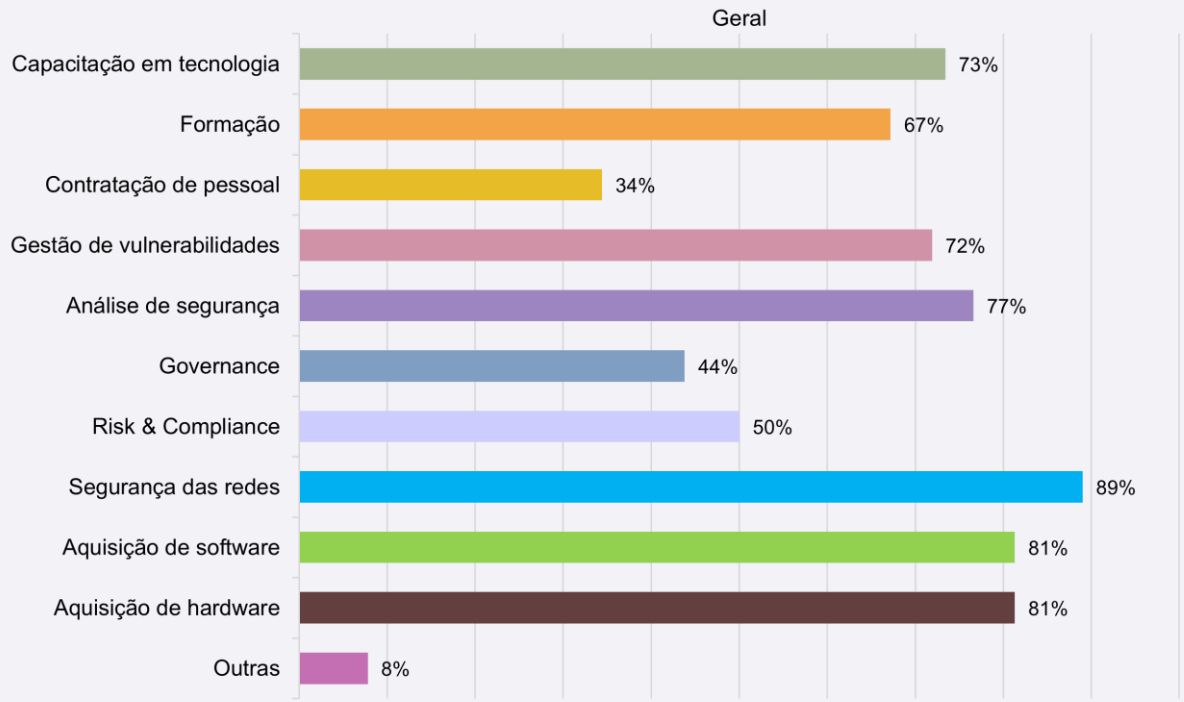
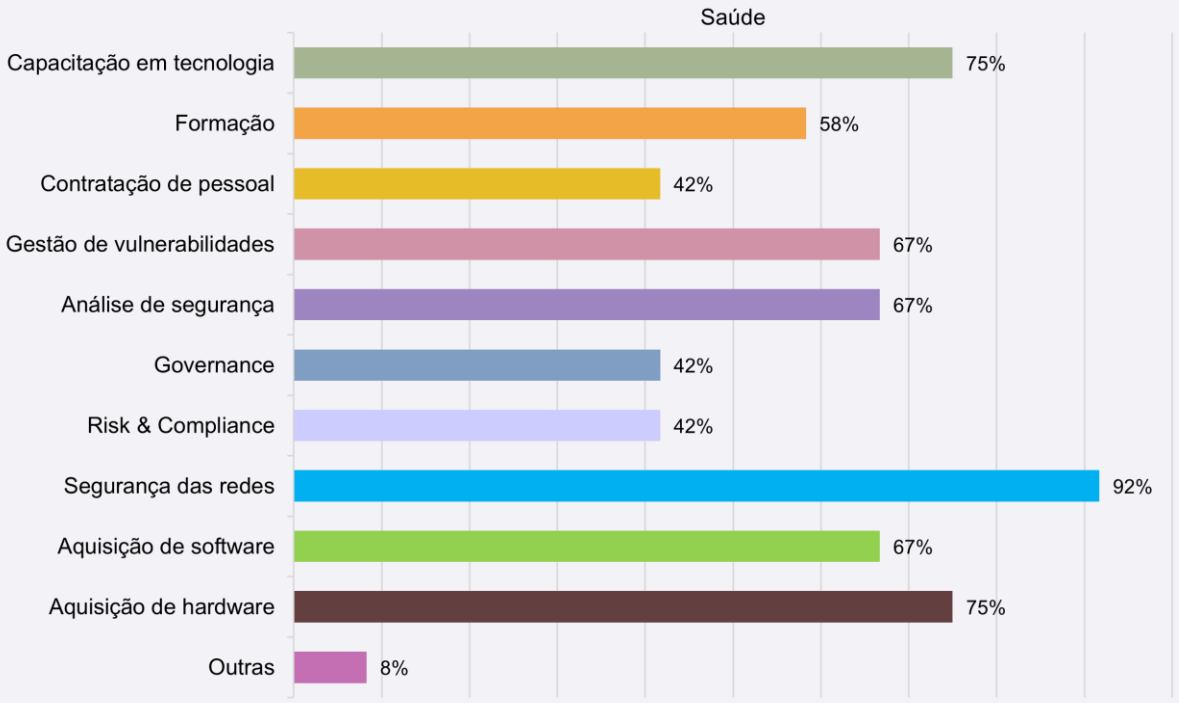


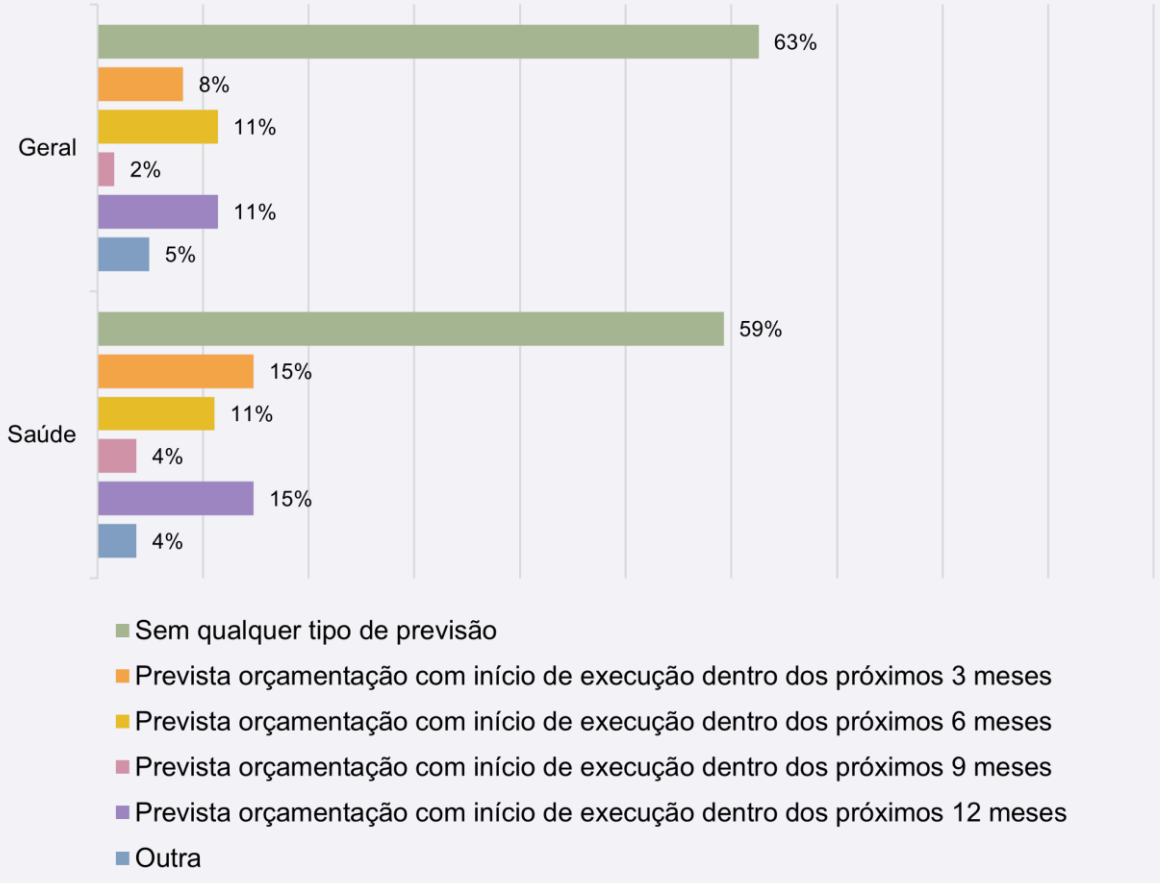
Gráfico 81.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança



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*. No setor da saúde, os resultados são semelhantes, com ligeiras variações percentuais, e verificando-se a mesma percentagem de OSE a aplicar parte do orçamento à gestão de vulnerabilidades e análises de segurança, bem como a mesma percentagem de OSE a direcionar parte do orçamento para as questões de *Governance* e de *Risk & Compliance*. 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[56]. 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[57].

Gráfico 82 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança



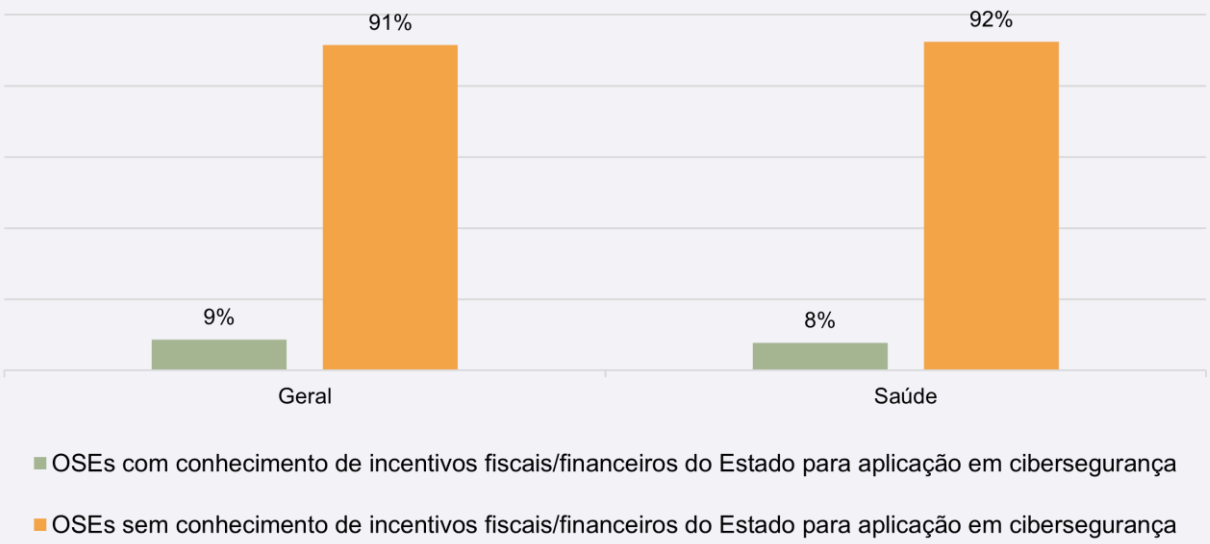
Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento.

[56] 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.

[57] ENISA, "NIS Investments", 2023

No setor da saúde a previsão de vir a iniciar a execução de um orçamento específico para cibersegurança ainda durante o ano de 2024 existia para entre 11% a 15% dos operadores. Quanto às "outras" respostas, estas corresponderam globalmente a situações em que os orçamentos atribuídos à cibersegurança se incluem ou decalcam dos orçamentos dedicados à área de informática.

Gráfico 83 - Conhecimento de incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança

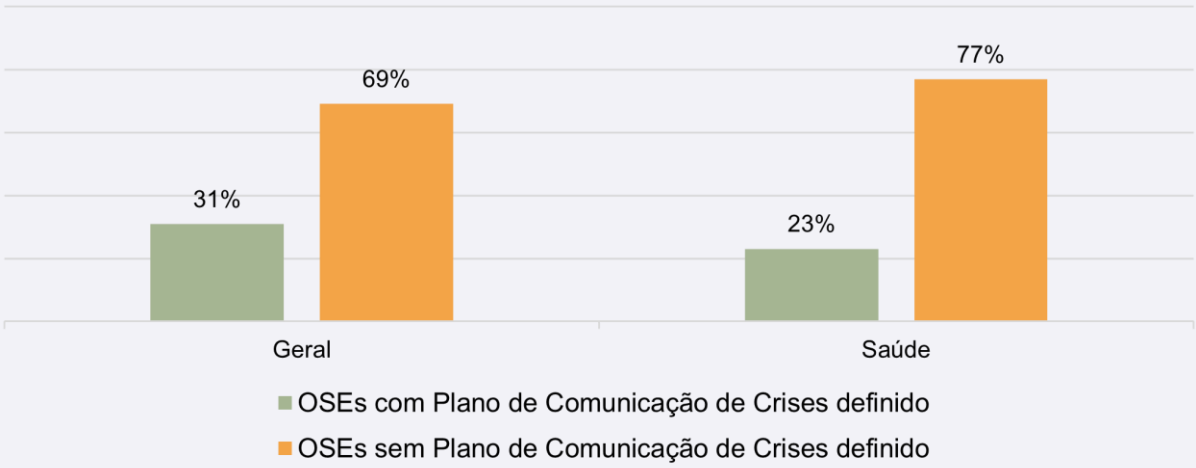


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No setor da saúde, essa percentagem é ligeiramente superior (+1 p.p.), atingindo os 92%.

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[58].

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

Gráfico 84 - 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. Nos setores bancário e das infraestruturas do mercado financeiro todos os inquiridos declaram ter plano de comunicação de crises definido. Tal deve-se ao facto de existir legislação setorial em vigor que obriga os operadores destes setores a terem este plano definido. No setor da saúde a percentagem de operadores com plano de comunicação de é de 23%.

Gráfico 85 - Secções definidas no Plano de Comunicação de Crises

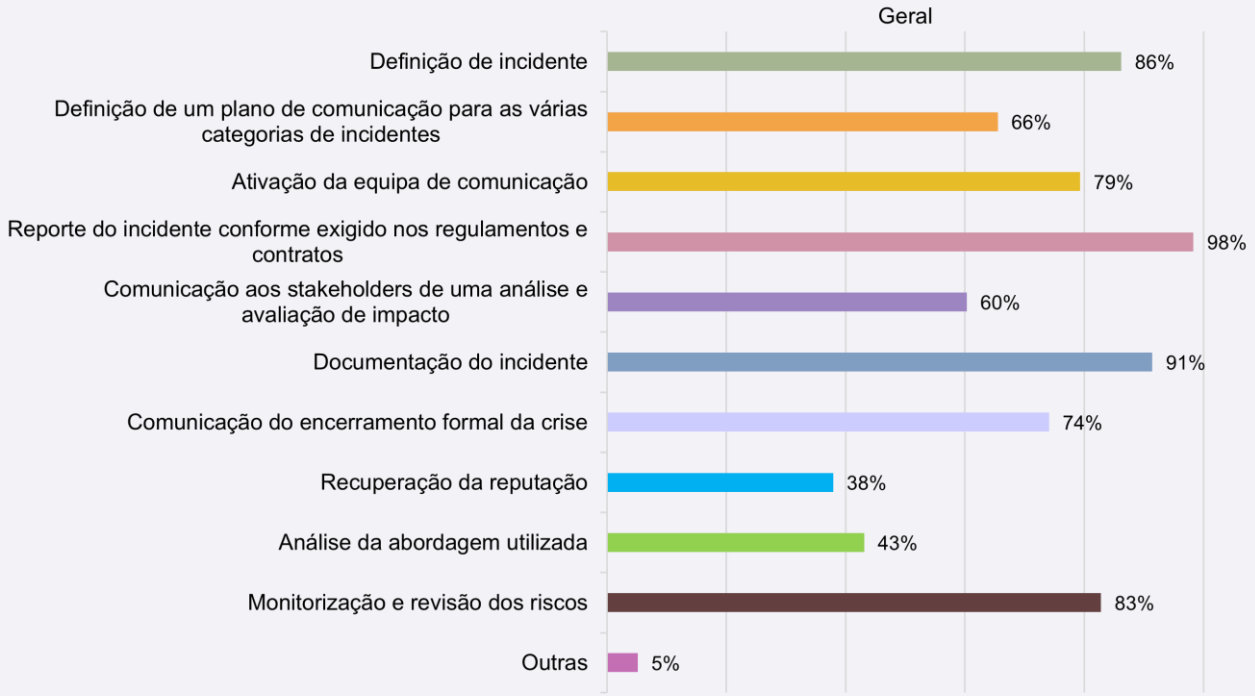
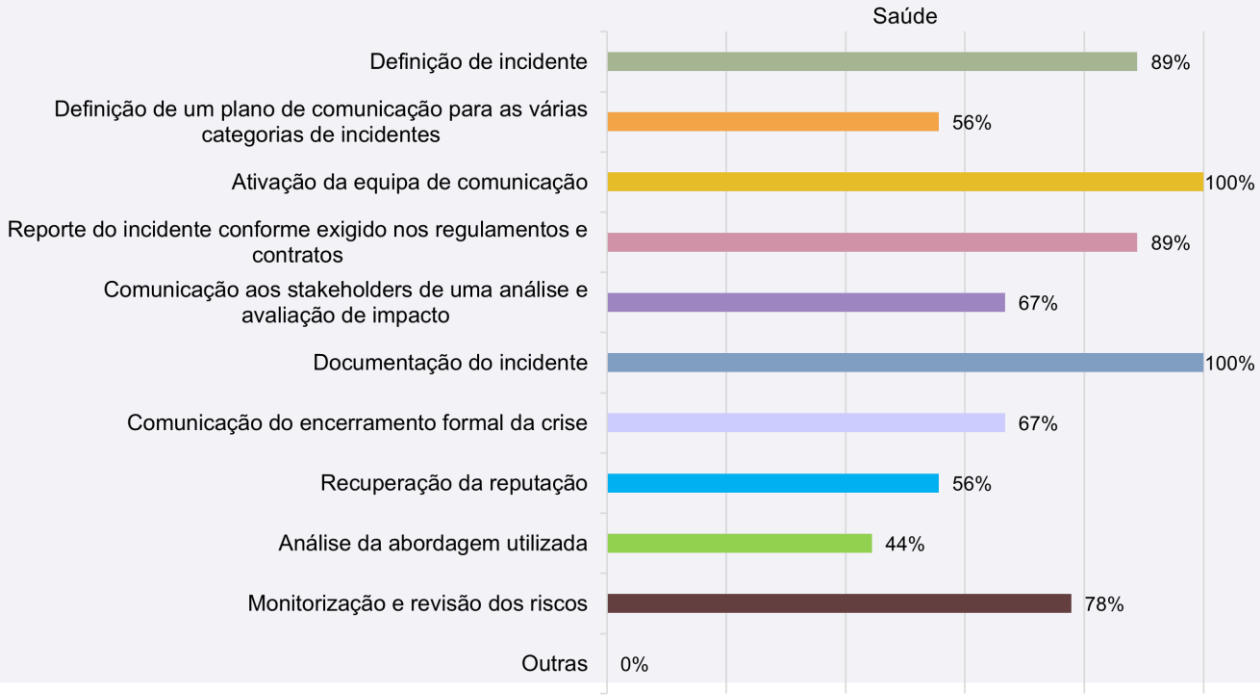


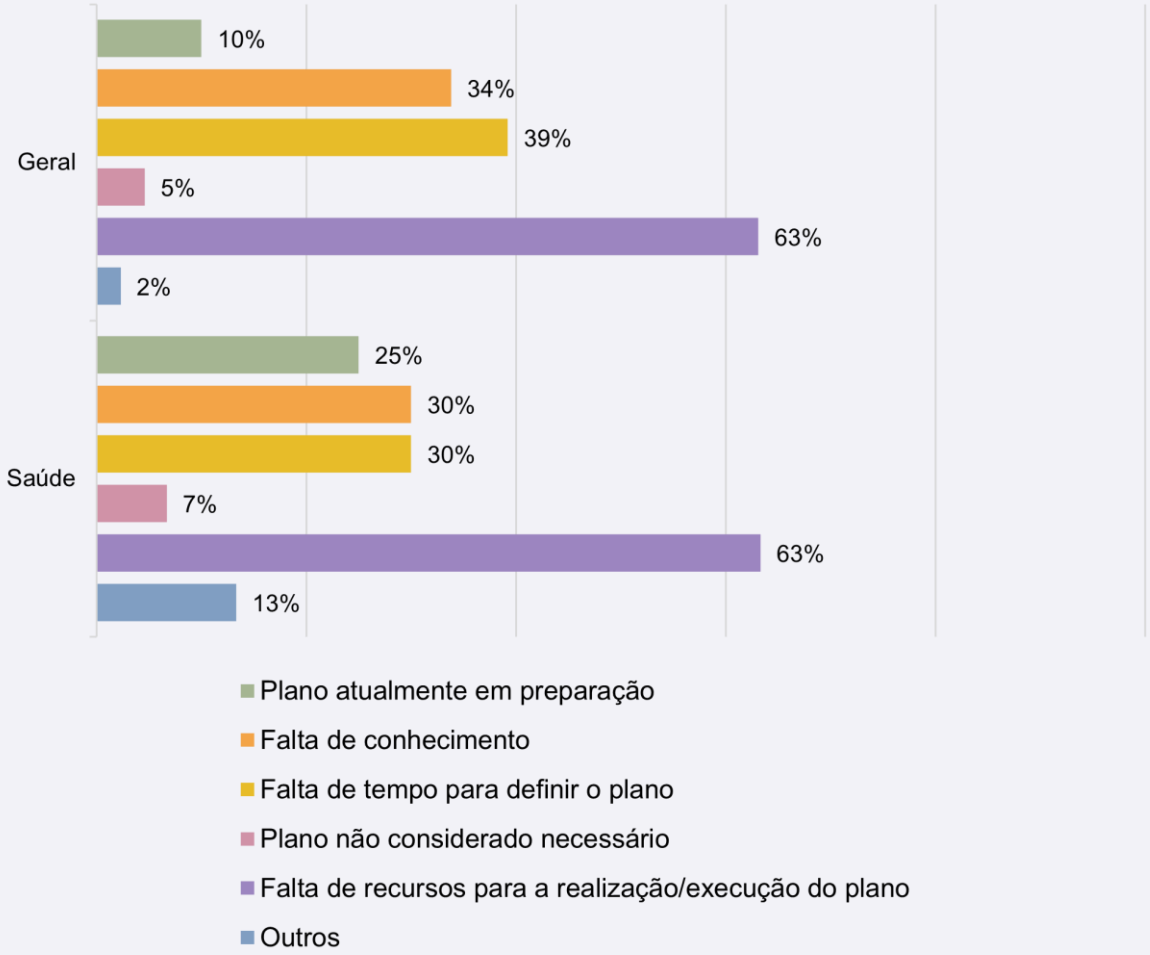
Gráfico 85.1 - Secções definidas no Plano de Comunicação de Crises



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.
O setor da saúde, foi um dos setores onde mais OSE tinham incluído nos seus planos as diversas secções elencadas no questionário.

Gráfico 86 - 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.

No setor da saúde, verificou-se a mesma percentagem de OSE que na generalidade a indicar a falta de recursos para a execução do plano. Face à generalidade, havia também no setor da saúde uma maior percentagem OSE a preparar Planos de Comunicação de Crises (25% no setor da saúde contra 10% na generalidade).

Análise Setorial

1. Saúde

1.1. Contextualização setorial

Em Portugal, "a saúde constitui matéria de governação política pelo menos desde o século XVI, ainda que o seu financiamento não tenha, durante alguns séculos, sido assumido pelo poder governativo"[59]. Tal só viria a acontecer verdadeiramente depois do 25 de Abril de 1974, com a consagração do direito à proteção da saúde "através de um serviço nacional de saúde [SNS] universal e geral e (...) tendencialmente gratuito"[60] na Constituição de 1976.

Durante o Estado Novo (1933-1974), os cuidados de saúde estavam a cargo das famílias, das instituições privadas ou da previdência[61] [62]. A criação do SNS mudou esse paradigma, transformando o Estado no principal prestador de cuidados de saúde em Portugal.

O SNS foi então formalmente criado em 1979, através da Lei n.º 56/79, de 15 de setembro, enquanto instrumento do Estado para assegurar o direito à proteção da saúde, nos termos da Constituição. O acesso é garantido a todos os cidadãos, independentemente da sua condição económica e social, bem como aos estrangeiros, em regime de reciprocidade, apátridas e refugiados políticos, e envolve todos os cuidados integrados de saúde, compreendendo a promoção e vigilância da saúde, a prevenção da doença, o diagnóstico e tratamento dos doentes e a reabilitação médica e social[63].

[59] Laurinda Abreu, "Pensar historicamente os cuidados de saúde em Portugal", *O Referencial: Revista da Associação 25 de Abril*, 12, https://dspace.uevora.pt/rdpc/bitstream/10174/24717/1/REFERENCIAL%20130_bx_12_17.pdf.

[60] Constituição da República Portuguesa, art. 64.º: Saúde, https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx

[61] A previdência, ou a Previdência Social, era essencialmente composta por instituições corporativas, tais como os sindicatos nacionais obrigatórios, as Casas do Povo ou as Casas de Pescadores, que ofereciam alguma proteção aos trabalhadores em situações de doença ou de invalidez (fonte: BBVA, "História da Segurança Social (parte I)", 20 de novembro de 2013, https://www.aminhapensao.pt/blog/historia-da-seguranca-social-parte-i/).

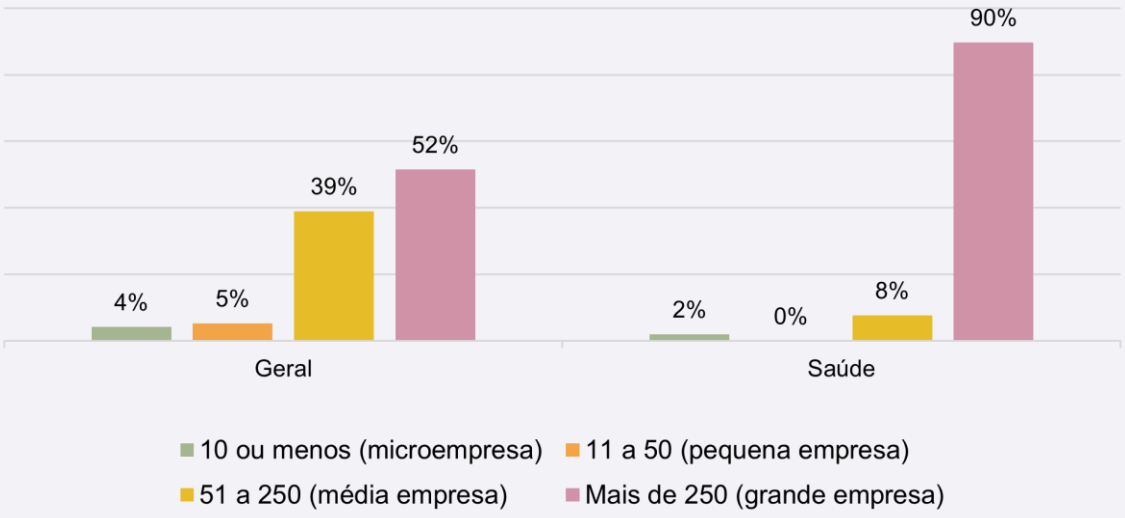
[62] Teresa Nicolau, "Da democracia nasceu o Serviço Nacional de Saúde", *RTP Ensina*, 2014, https://ensina.rtp.pt/artigo/da-democracia-nasceu-o-servico-nacional-de-saude/.

[63] "História do SNS", *SNS*, https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/.

Segundo os *rankings* mais recentes disponíveis, o SNS é considerado o 13º melhor SNS[64] entre 35 países europeus[65] e o 40º melhor entre 104 países do mundo[66].

De acordo com o questionário realizado, o tecido empresarial dos operadores de serviços essenciais (OSE) do setor da saúde é sobretudo composto por grandes organizações, com mais de 250 colaboradores, e as restantes são médias e micro-organizações (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



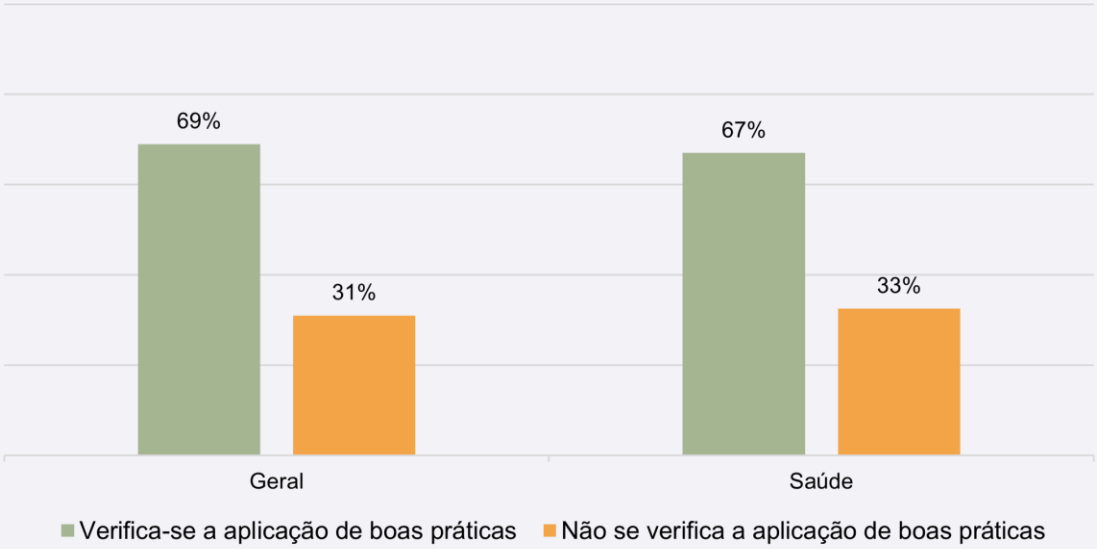
[64] Arne Björnberg e Ann Phang, "Euro Health Consumer Index 2018", *Health Consumer Powerhouse*, 2019, https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf

[65] "Euro Health Consumer Index by Country 2024", *World Population Review*, https://worldpopulationreview.com/country-rankings/euro-health-consumer-index-by-country.

[66] "The Best Healthcare in the World: Country Rankings", *International Citizens Insurance*, 2024, https://www.internationalinsurance.com/health/systems/.

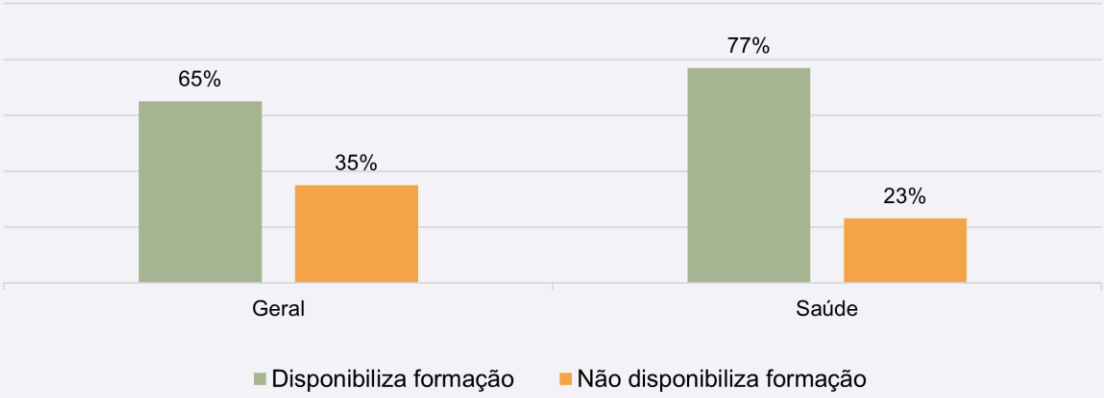
Dois terços dos operadores do setor da saúde referem aplicar boas práticas de segurança (**Gráfico 31**) sendo que o mesmo se verifica na generalidade dos setores.

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



Esta afirmação pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (vide **Gráfico 38**), este número corresponde a cerca de 77%, o que pode ser considerado um número elevado.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



As medidas de proteção contra ameaças de cibersegurança (**Gráfico 66.5**) também suportam a afirmação anterior e, nestas, as mais utilizadas são: A utilização de *Firewall* em cerca de 98% dos casos, a utilização de palavras-passe fortes em 73%, utilização de configurações de *anti-spam* em 70% dos casos, utilização de *VPN* e controlos de acesso à rede com 85% e 70%, respetivamente.

Gráfico 66.5 - Medidas de proteção contra ameaças de cibersegurança

Este é um setor onde a maioria dos operadores (92%) afirma existir falta de profissionais na área da cibersegurança (**Gráfico 44**), no entanto e segundo estes dados, é também um setor que tem demonstrado uma baixa incidência de ciberataques identificados pelos próprios (71% dos inquiridos nunca sofreu um incidente de segurança em contexto TIC) (**Gráfico 68**).

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

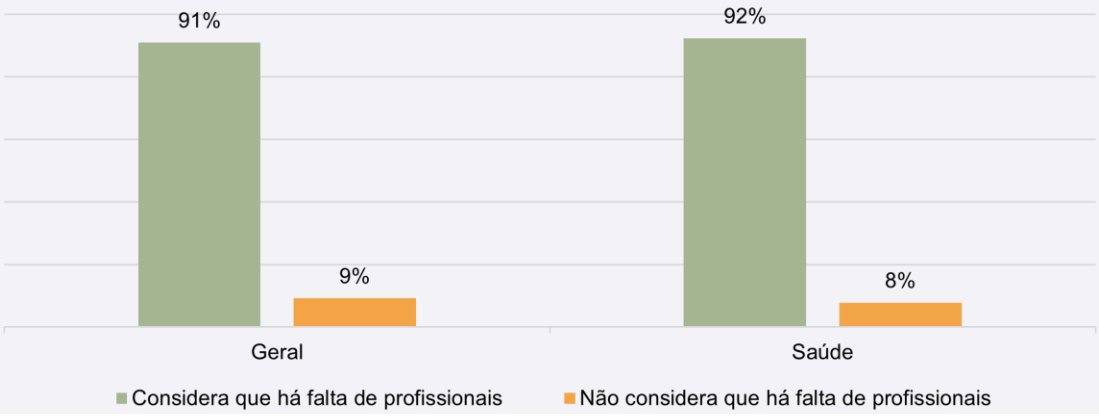
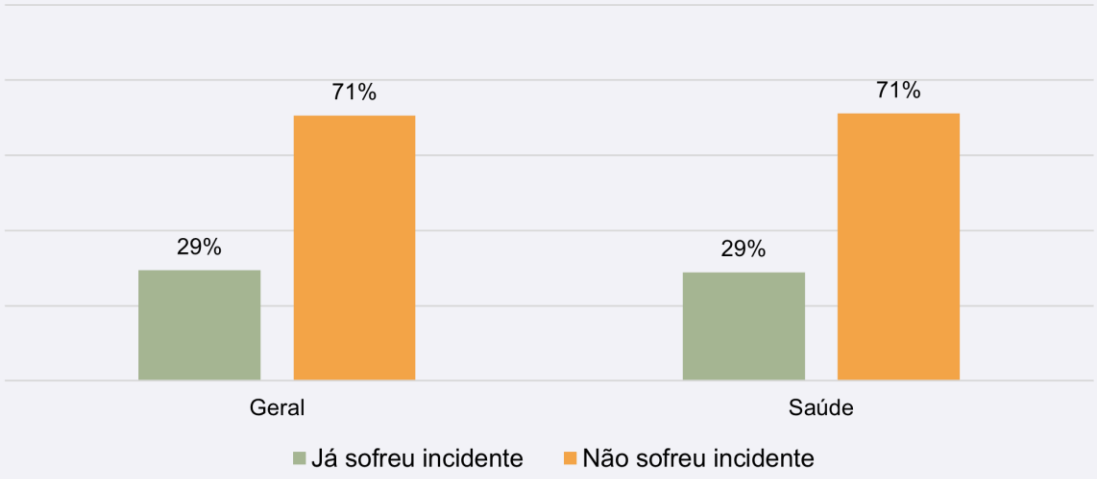


Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC



1.1.1. Impacto socioeconómico

O setor da saúde é um dos setores com mais peso na economia do país. A despesa corrente em saúde costuma representar cerca de 10% do Produto Interno Bruto (PIB) nacional, ou seja, mais de 20 mil milhões de euros em cada ano, de um PIB de aproximadamente pelo menos 200 mil milhões de euros desde 2018[67]. Este valor de despesa não se deve apenas ao setor público, mas também à despesa das entidades de saúde privadas. De um modo geral, o setor público costuma representar dois terços desta despesa (cerca de 14-15 mil milhões de euros) e o setor privado o restante terço (cerca de 6-7 mil milhões de euros)[68]. Em termos de Orçamento do Estado, cujo valor total se tem situado acima dos 100 mil milhões de euros (103 mil milhões em 2023 e 123 mil milhões em 2024)[69], a percentagem alocada à saúde para 2024 é de aproximadamente 12,7% (cerca de 15,5 mil milhões de euros de um orçamento global de 123,6 mil milhões)[70].

Em 2019, a despesa corrente em saúde foi de cerca de 20,4 mil milhões de euros, representando 9,5% do PIB. Em 2020, houve um aumento para 21,1 mil milhões de euros (10,5% do PIB), e em 2021 foi de 23,7 mil milhões de euros (11,2% do PIB), indicando um crescimento de 12,2% face a 2020[71]. Em 2022, a despesa corrente em saúde aumentou 6,3%, atingindo 25,4 mil milhões de euros, representando 10,6% do PIB. O regresso à normalidade nas atividades dos prestadores públicos e privados nas áreas não COVID-19 iniciado em 2021 continuou e, havendo mais entidades a retomar o seu normal funcionamento, houve também um aumento da despesa corrente nesse ano no orçamento. Os efeitos da pandemia persistiram em 2022, mas com impacto inferior na despesa corrente a 2020 e 2021[72].

Apesar de a prestação de cuidados de saúde ser em Portugal uma atividade que gera sobretudo despesa, uma vez que o Estado assume o papel de prestador de forma tendencialmente gratuita, o setor da saúde é, noutras vertentes, como a produção de preparações farmacêuticas e o fabrico de material médico-cirúrgico, uma força motriz da economia nacional e um gerador de receita. Agregando estas vertentes, a saúde representa, em Portugal, um volume de negócios anual na ordem dos 34 mil milhões de euros e um valor acrescentado bruto de cerca de 12 mil milhões de euros, envolvendo perto de 105 mil empresas[73].

---

[67] PORDATA, "Produto Interno Bruto (PIB): Quanta riqueza é criada em Portugal", Estatísticas, https://www.pordata.pt/pt/estatisticas/economia/crescimento-e-produtividade/produto-interno-bruto-pib.

[68] INE, "Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB", Informação à Comunicação Social, 4 de julho de 2023, 3, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=594883237&DESTAQUESmodo=2.

[69] Ministério das Finanças, "Orçamento do Estado 2024: Relatório - versão consolidada de 16 de outubro de 2023", 290 e 337, https://www.dgo.gov.pt/politicaorcamental/OrcamentodeEstado/2024/Proposta%20do%20Or%C3%A7amento/Documentos%20do%20OE/OE2024_doc16_Relatorio.pdf

[70] Ministério das Finanças, "Orçamento do Estado 2024: Relatório", 290.

[71] INE, "Estatísticas da Saúde - 2022", edição de 2024, 54, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=660521049&att_display=n&att_download=y.

[72] INE, "Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB", Informação à Comunicação Social, 4 de julho de 2023, 1.

[73] "Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões", *Health Cluster Portugal*, 27 de fevereiro de 2024, https://www.healthclusterportugal.pt/pt/noticias/exportacoes-em-saude-2023/.

Estima-se, também, que o setor da saúde empregue mais de 400 mil pessoas[74]. Cerca de 296 mil pessoas estão ligadas à prestação de cuidados de saúde. Entre médicos, enfermeiros, técnicos auxiliares de saúde e outros, o SNS emprega cerca de 150 mil profissionais[75], enquanto o setor privado emprega cerca de 146 mil[76].

Como referido, até à criação do SNS, os cuidados de saúde estavam sobretudo a cargo das famílias, das instituições privadas ou da previdência. Ao ser criado um serviço nacional, universal e geral, e tendencialmente gratuito, esse paradigma foi alterado. De um cenário em que o Estado assumia apenas o cuidado dos mais pobres, passou-se para um em que o Estado procura assegurar o acesso a cuidados de saúde por parte de todos os cidadãos. Por isso, o SNS conta hoje com mais 10,5 milhões de utentes inscritos, dos quais 65,9% se encontram inscritos em unidades de saúde familiar[77].

O número de médicos em Portugal sofreu também um grande aumento. Contrastando com os primeiros anos do SNS, o número de médicos por cada 100.000 habitantes triplicou. Em 1979, havia 186 médicos por cada 100.000 habitantes[78]. Em 2021, segundo dados do Eurostat, esse número atingiu os 562 médicos por cada 100.000 habitantes, sendo este rácio o segundo mais elevado da UE, atrás somente da Grécia (629 médicos por cada 100.000 habitantes)[79].

Há também mais hospitais. Em 1985, havia 94 hospitais públicos em Portugal[80]. Em 2021 havia 110. Tem também crescido o número de hospitais privados. Em 1999, por exemplo, existiam 97 hospitais privados[81]. Já em 2021, o número de hospitais privados supera o número de hospitais públicos, sendo que se contam 128 privados. Acrescem ainda 2 hospitais em regime de parceria público-privada (PPP). Ao todo, existem 240 hospitais em Portugal. Ressalva-se que, apesar de os hospitais públicos serem menos, estes têm maior capacidade de internamento instalada: de um total de 36,2 mil camas, em 2021, 23,9 mil estavam nos hospitais públicos, 11,6 mil nos hospitais privados e 705 nos hospitais em parceria público-privada[82].

O aumento do acesso aos cuidados de saúde, bem como o aumento do número de profissionais e de hospitais, reduziram grandemente a mortalidade infantil no país. Em 1979, a mortalidade infantil em crianças com menos de um ano era de 26 por mil[83] e, em 2022, de 2,6 por mil - 10 vezes menor[84]. Houve também aumentos consideráveis ao nível da esperança média de vida. Em 1979, a esperança média de vida em Portugal era de 71 anos[85]. Em 2023, a esperança média de vida chegou aos 84,75 anos[86].

---

74 "Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões".

75 Ana Ferreira et al., "Os Profissionais do SNS: Retrato e Evolução", *PLANAAP*: *Coleção Profissionais da Saúde* - n.º 2, março de 2024, 18, https://www.planapp.gov.pt/wp-content/uploads/2024/03/PlanAPP_ProfissionaisSNS-2.pdf.

76 "Empresas privadas do setor da saúde com valor acrescentado acima de 6,7 mil milhões", CIP, 20 de outubro de 2023, https://cip.org.pt/empresas-privadas-do-setor-da-saude-com-valor-acrescentado-acima-de-67-mil-milhoes/.

77 Conselho das Finanças Públicas, "Evolução do Desempenho do Serviço Nacional de Saúde em 2022 (Relatório n.º 7/2023)", junho de 2023, 4, https://www.cfp.pt/uploads/publicacoes_ficheiros/cfp-rel-07-2023.pdf.

78 Cátia Mendonça e Rita Costa, "40 anos do SNS. O que mudou?", *Público*, 14 de setembro de 2019, https://www.publico.pt/2019/09/14/infografia/40-anos-sns-mudou-340.

79 "Physicians and physiotherapists in the EU: how many?", *Eurostat*, 18 de agosto de 2023, https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230818-1.

80 Mendonça e Costa, "40 anos do SNS. O que mudou?", *Público*.

81 Mendonça e Costa, "40 anos do SNS. O que mudou?", *Público*.

82 INE, "Estatísticas da saúde 2021", edição de 2023, 4-5, https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=11677508&PUBLICACOESmodo=2

83 Mendonça e Costa, "40 anos do SNS. O que mudou?", *Público*.

84 INE, "Estatísticas Demográficas 2022", 16 de novembro de 2023, 1, https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637367953&att_display=n&att_download=y#.

85 Mendonça e Costa, "40 anos do SNS. O que mudou?", *Público*.

86 INE, "Estatísticas Demográficas 2022", 6 e 7.

1.1.2. Especificidades tecnológicas

O setor da saúde lida, necessariamente, com um grande volume de dados que lhe permite operar, indo do registo de marcação de consultas e cirurgias, ao histórico de saúde dos diversos utentes e à vigilância epidemiológica. Tem, por isso, ao longo dos anos, avançado significativamente na integração da tecnologia na sua infraestrutura, nomeadamente através dos Serviços Partilhados do Ministério da Saúde (SPMS).

As melhorias na segurança da tecnologia utilizada no setor são de extrema importância, uma vez que os dados de saúde são de grande sensibilidade. A partilha de dados pessoais de saúde, mesmo com um empregador, um familiar ou um amigo, pode gerar estigmas, formas de discriminação, ou simplesmente ser motivo de embaraço para a pessoa a quem esses dados pertencem. Num estudo de 2005, uma em cada oito pessoas admitiu adotar comportamentos que poderiam comprometer a sua saúde por terem dúvidas em relação a como os seus dados de saúde poderiam ser utilizados uma vez partilhados, tais como mentir aos seus médicos sobre sintomas e comportamentos, recusar dar informação ou dar informação incorreta a profissionais de saúde, e até mesmo chegar ao ponto de evitar recorrer a quaisquer cuidados de saúde[87]. Para melhor dar uma ideia de como a partilha de determinados dados de saúde pode gerar esses estigmas, apresentam-se, de seguida, alguns exemplos reais.

Em 2015, uma clínica de saúde em Londres, no Reino Unido, divulgou acidentalmente os dados de saúde de cerca de 780 pessoas com HIV positivo. Alguns indivíduos afetados pela divulgação destes dados reportaram terem sofrido discriminação nos seus locais de trabalho, terem tido as suas relações de amizade afetadas e terem sido socialmente ostracizados depois de a sua condição ter sido conhecida[88].

Também em 2015, um ataque ao Sistema de Saúde da UCLA (University of California,Los Angeles, EUA), afetou cerca de 4,5 milhões de pacientes. A exposição de dados de saúde, como os relativos à saúde mental de diversos pacientes, terão conduzido a discriminação no local de trabalho, micro-gestão junto dos trabalhadores cujos dados de saúde se tornaram conhecidos e até mesmo ao proferimento destes relativamente a promoções[89]. Casos como estes evidenciam a sensibilidade dos dados relativos à saúde

Os dados de saúde são também um alvo preferencial dos agentes de ameaça. E são um alvo preferencial porque podem ser utilizados por esses agentes de ameaça para cometer uma variedade de crimes: dados como o número do Cartão do Cidadão, de Segurança Social, morada fiscal, nome e data de nascimento podem ser utilizados para furtar a identidade de alguém e obter empréstimos ou cartões de alguém em seu nome.

---

87 Institute of Medicine Committee on Health Research and the Privacy of Health Information, "The Value and Importance of Health Information Privacy" em *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, ed. Sharyl Nass, Laura Levit e Lawrence Gostin (Washington DC: National Academies Press, 2009), https://www.ncbi.nlm.nih.gov/books/NBK9579/.

88 Cara McGoogan, "London HIV clinic accidentally leaks data of 780 patients", *Wired*, 2 de setembro de 2015, https://www.wired.com/story/56-dean-street-hiv-leak/.

89 Chad Turhune, "UCLA Health System data breach affects 4.5 million patients", *Los Angeles Times*, 17 de julho de 2015, https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html.

Os dados sobre o histórico de saúde de alguém podem também ser usados para cometer fraude de seguros ou obter medicamentos a que não conseguiriam normalmente aceder. Além disso, os dados de saúde podem ser usados indevidamente por longos períodos, ao contrário dos dados de cartões de crédito ou de débito cujo uso indevido pode ser rapidamente detetado e bloqueado[90].

Apresentam-se, de seguida, alguns dos sistemas utilizados no setor da saúde, bem como algumas das debilidades desses mesmos sistemas, apontadas por diversos profissionais do setor em análise.

SINAVE | Sistema Nacional de Vigilância Epidemiológica

O SINAVE (Sistema Nacional de Vigilância Epidemiológica) é um sistema integrado que tem como principais objetivos a vigilância, deteção precoce e resposta a surtos e epidemias de doenças transmissíveis de saúde pública. Este sistema pretende proteger a população contra riscos sanitários, melhorando assim a capacidade de resposta a emergências de saúde pública[91].

As principais características deste sistema são a notificação obrigatória de certas doenças por parte dos profissionais de saúde e dos laboratórios e o facto de utilizar uma plataforma de forma a facilitar a recolha e transmissão de dados em tempo real. Esta plataforma permite a monitorização contínua da incidência e prevalência de doenças transmissíveis fazendo assim análises epidemiológicas para identificar tendências e surtos.

O SINAVE tem vários componentes, tais como:

- **SINAVE Laboratorial**: Focado na notificação laboratorial de doenças transmissíveis;
- **SINAVE Clínico**: Baseado na notificação clínica feita por profissionais de saúde;
- **Plataforma de notificação**: permite a monitorização contínua da incidência e prevalência de doenças transmissíveis fazendo assim análises epidemiológicas para identificar tendências e surtos.

O SINAVE é crucial para a saúde pública em Portugal pois ajuda na deteção precoce de surtos, fornece dados para o planeamento de políticas de saúde e melhora a comunicação entre diferentes níveis do sistema de saúde[92].

BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários

O BI CSP é uma iniciativa do SNS e tem como objetivo melhorar a gestão, qualidade, eficiência e a transparência dos serviços de cuidados de saúde primários (CSP) e dados hospitalares. Este sistema permite ainda a monitorização e avaliação contínua das unidades de saúde, facilitando assim a tomada de decisões baseadas em dados concretos.

[90] Steve Alder, "Editorial: Why Do Criminals Target Medical Records", *The HIPAA Journal*, 2 de novembro de 2023, https://www.hipaajournal.com/why-do-criminals-target-medical-records/

[91] SPMS, "SINAVE | Sistema Nacional de Vigilância Epidemiológica", https://www.spms.min-saude.pt/2020/07/sinave-2/.

[92] Daniela Oliveira, "Desenvolvimento de um Sistema Eletrónico de Vigilância Epidemiológica (eVDmed): recolha, análise e publicação de informação" (dissertação de mestrado, Universidade do Minho, 2017), 3-4. https://repositorium.sdum.uminho.pt/bitstream/1822/49627/1/Daniela%20Pimentel%20de%20Oliveira.pdf

O sistema tem uma funcionalidade que permite avaliar o desempenho das unidades de saúde primários com base em diversos indicadores, ajudando assim a identificar áreas que precisam de melhorias e/ou implementar ações corretivas de forma eficiente. Com o BI CSP é ainda possível obter dados relevantes que podem ser úteis para profissionais de saúde, tais como: estatísticas sobre consultas, tempos de espera, cobertura vacinal e outros indicadores de desempenho[93].

Existem três componentes agregados ao BI CSP: portal com acesso público e acesso autenticado, ferramenta para a exploração da informação, ferramenta para a criação e monitorização dos planos de ação em contexto dos CSP[94].

PEM | Prescrição Eletrónica Médica

A PEM, Prescrição Eletrónica Médica tem como objetivo modernizar e agilizar todo o processo de prescrição de medicamentos, eliminando a necessidade de prescrições em papel, melhorando assim a eficiência do processo de prescrição e dispensa de medicamentos. Teve origem na Lei nº11/2012, de 8 de março, e na portaria n.º 137-A/2012, de 11 de maio e já funciona por DCI (Denominação Comum Internacional)[95].

Esta ferramenta permite que os médicos façam prescrições eletronicamente e que sejam enviadas para uma base de dados centralizada. Os utentes podem aceder às prescrições através do portal do utente (versão *web* ou aplicação móvel), esta aplicação é responsável por mais de 90% do total de prescrições registadas diariamente e apresenta a possibilidade de prescrição diferenciada de medicamentos, cuidados respiratórios domiciliários e dispositivos médicos[96]. As farmácias também têm acesso às prescrições, permitindo assim a dispensa dos medicamentos de forma rápida, reduzindo o risco de erros de transcrição[97].

A PEM também traz uma melhoria na segurança do processo de prescrição e reduz o risco de fraudes e falsificações, sendo que a plataforma está em conformidade com as normas e regulamentos de proteção de dados, garantindo assim a privacidade das informações de saúde dos utentes.

Exames Sem Papel

Exames Sem Papel é uma iniciativa do Ministério da Saúde e tem como objetivo modernizar e agilizar o processo de gestão de exames médicos, desde a requisição até à consulta dos resultados, promovendo a digitalização utilizando múltiplas plataformas de serviços centrais. As principais finalidades desta iniciativa são: reduzir o tempo necessário para a realização dos exames e obtenção dos resultados, minimizar os erros associados à transcrição manual de dados, facilitar o acesso tanto a utentes como a médicos e a redução de desperdício[98].

---

[93] Mafalda Simão, "A Prestação de Cuidados de Saúde em Função do Território", publicado no Repositório Científico da Universidade de Coimbra, 2022, 7-9, https://estudogeral.uc.pt/handle/10316/102463.

[94] SPMS, "BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários", https://www.spms.min-saude.pt/2020/07/bi-csp-bilhete-de-identidade-dos-cuidados-de-saude-primarios/.

[95] SPMS, "PEM | Prescrição Eletrónica Médica", julho de 2020, https://www.spms.min-saude.pt/2020/07/pem/.

[96] SPMS, "PEM | Prescrição Eletrónica Médica", julho de 2020.

[97] SPMS, "Prescrição Eletrónica Médica: Especificação dos Serviços para integração com o Sistema Central de Prescrições", janeiro de 2018, SPMS (min-saude.pt).

[98] SPMS, "Exames Sem Papel", julho de 2020, https://www.spms.min-saude.pt/2020/07/exames-sem-papel/.

As requisições de exames são feitas eletronicamente pelos médicos e enviadas diretamente para os laboratórios e centros de diagnóstico através de uma API, sendo que a faturação dos prestadores para o SNS também é efetuada por via eletrónica. É importante referir que esta iniciativa também garante a segurança e privacidade dos dados de saúde dos utentes, pois a iniciativa está em conformidade com as normas de proteção de dados e as informações são armazenadas e transmitidas de forma segura[99].

SClínico | Cuidados de Saúde Hospitalar

O SClínico Hospitalar é um sistema de informação evolutivo, este foi desenvolvido pela SPMS e está presente em 50 entidades do setor da saúde. Este sistema tem como principais objetivos melhorar a eficiência, a qualidade e a segurança dos cuidados de saúde prestados nos hospitais. Esta ferramenta permite a criação e gestão de registos clínicos eletrónicos, substituindo os registos em papel. Isto torna o acesso mais rápido e seguro às informações clínicas dos utentes, melhorando assim o funcionamento dos cuidados de saúde[100].

Nesta plataforma é possível gerir todos os processos clínicos, admitir pacientes, gerir consultas, prescrever medicamentos, requerer exames e elaborar relatórios clínicos, sendo este sistema interoperável com outros sistemas de saúde, permitindo assim a troca de informações entre diferentes unidades de saúde. Por fim, o SClínico conta com ferramentas de apoio à decisão clínica, fornecendo alertas e recomendações de forma a auxiliar os profissionais de saúde[101].

SClínico | Cuidados de Saúde Primários (CSP)

O SClínico Cuidados de Saúde Primários (CSP), tal como o SClinico Cuidados de Saúde Hospitalar, é um sistema de informação evolutivo onde a sua origem remonta duas aplicações: o SAM (Sistema de Apoio ao Médico) e o SAPE (Sistema de Apoio à Prática de Enfermagem). Este sistema tem crescido para ser uma aplicação única, comum a todos os prestadores de cuidados de saúde e centrada no doente. Os objetivos estabelecidos para este sistema são os mesmos do SClínico | Cuidados de Saúde Hospitalar, mas no âmbito dos cuidados de saúde primários[102].

Receita Sem Papel

A Receita Sem Papel tornou-se obrigatória para todas as entidades do SNS a 1 de abril de 2016, através do Despacho de 25 de fevereiro de 2016. O principal objetivo desta iniciativa é substituir as prescrições de medicamentos em papel por prescrições eletrónicas, de forma a simplificar o processo tanto para os profissionais de saúde como para os utentes[103]. Este novo modelo poderá incluir diferentes tipos de medicamentos, como medicamentos comparticipados e não comparticipados na mesma receita.

[99] SPMS, “Exames Sem Papel”.

[100] SPMS, “SClínico | Cuidados de Saúde Hospitalares (CSH)”, julho de 2020, https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/.

[101] SPMS, “SClínico | Cuidados de Saúde Hospitalares (CSH)”.

[102] SPMS, “SClínico | Cuidados de Saúde Primários (CSP)”, julho de 2020, https://www.spms.min-saude.pt/2020/07/sclinico-cuidados-de-saude-primarios-csp/.

[103] SPMS, “FAQs PEM - Receita sem papel”, novembro de 2015, https://spms.min-saude.pt/wp-content/uploads/2015/11/FAQs1.pdf.

No ato da dispensa nas farmácias, o utente poderá optar por despachar todos os produtos prescritos, ou apenas parte deles, sendo possível levantar os restantes em diferentes estabelecimentos e em datas distintas[104].

RNU | Registo Nacional de Utente

O Registo Nacional de Utente (RNU) figura-se como um dos pilares mais importantes do sistema de informação de saúde e visa proporcionar uma identificação única e centralizada de todos os utentes do SNS, melhorando assim a gestão dos serviços de saúde. Este sistema também facilita o acesso e a partilha de informações entre diferentes entidades do setor da saúde[105].

O RNU tem por base três componentes: uma aplicação *Web*, onde é possível a gestão dos dados de identificação dos utentes, uma plataforma na qual são disponibilizados serviços que permitem a consulta de dados e uma base de dados nacional. Esta última é alimentada diretamente pelos administrativos dos CSP, pelos hospitais do SNS, pelos processos do Cartão de Cidadão e pela integração de dados com as Regiões Autónomas. A estrutura do utente tem três campos: "Identificação", onde consta toda a informação relativa à identificação do utente, "Entidades Responsáveis", referente à informação das entidades financeiras responsáveis pelo utente e "Benefícios", que contém a informação sobre os benefícios de saúde aplicáveis ao utente[106].

O RNU também tem um *WebService* onde é possível efetuar uma chamada passando o número de SNS do utente ou a EFR (Entidade Financeira Responsável), de seguida, o *WebService* irá devolver o campo do Utente (caso os dados enviados sejam corretos) e uma mensagem com um código e uma descrição do mesmo. Este código funciona como uma garantia de correspondência entre a informação de referência no RNU e nos sistemas locais[107].

Dispositivos médicos

Segundo o decreto-lei n.º 145/2009, de 17 de junho, um dispositivo médico é "qualquer instrumento, aparelho, equipamento, *software*, material ou artigo utilizado isoladamente ou em combinação, incluindo o *software* destinado pelo seu fabricante a ser utilizado especificamente para fins de diagnóstico ou terapêuticos e que seja necessário para o bom funcionamento do dispositivo médico, cujo principal efeito pretendido no corpo humano não seja alcançado por meios farmacológicos, imunológicos ou metabólicos, embora a sua função possa ser apoiada por esses meios, destinado pelo fabricante a ser utilizado em seres humanos" para o diagnóstico, controlo e tratamento de doenças, compensações de lesões, substituição ou alteração da anatomia ou de processos fisiológicos e controlo da conceção[108].

[104] SPMS, "Receita Sem Papel", abril de 2019, https://www.spms.min-saude.pt/2019/04/receita-sem-papel-2/.
[105] SPMS, "RNU: Registo Nacional de Utentes", outubro de 2015, https://www.spms.min-saude.pt/2015/10/rnu/.
[106] DSI, "RNU - Registo Nacional de Utentes: Especificação Técnica", SPMS, 12 de novembro de 2015, SC_InfoSite_2015 (min-saude.pt).
[107] DSI, "RNU - Registo Nacional de Utentes: Especificação Técnica", SPMS.
[108] Decreto-Lei n.º 145/2009, de 17 de junho, https://diariodarepublica.pt/dr/detalhe/decreto-lei/145-2009-494558 .

No caso dos dispositivos médicos que possuem componentes eletrónicos, *software*, e capacidade de ligação à Internet, tem-se-lhes chamado dispositivos da *Internet of Medical Things* - IoMT. Incluem-se, nesta categoria, tanto dispositivos mais pequenos e simples, que podem ser implantados no corpo humano, como *pacemakers*, bombas de insulina e estimuladores de bexiga, como dispositivos maiores de uso hospitalar, como ventiladores, monitores de sinais vitais, máquinas de suporte vida ou até mesmo sistemas de cirurgia robótica potenciados pelas velocidades 5G. A crescente utilização e interconectividade destes dispositivos tem aumentado a superfície de ataque para cibercriminosos, algo que será explorado em maior profundidade em **1.2. Ameaças**.

No final de 2020, o INFARMED, I.P. lançou o novo Sistema de Informação para Dispositivos Médicos (SIDM). Este sistema, que já existia desde 2015, foi revisto de forma a otimizar toda a gestão da informação relacionada com dispositivos médicos, simplificando assim o seu registo. O SIDM, para além da componente de registo, possui uma componente de pesquisa pública dos dispositivos médicos (infoDM)[109] e uma área que permite a criação de notificações por parte de utilizadores com problemas em produtos de saúde. O principal objetivo do SIDM é gerir de forma eficiente os dispositivos médicos utilizados nos hospitais e outras unidades de saúde, ajudando assim a monitorizar o inventário, a manutenção, o uso e a rastreabilidade dos mesmos[110].

O SIDM permite o registo detalhado de todos os dispositivos médicos, como o tipo de dispositivo, número de série, fabricante, data de aquisição, localização atual, entre outros. A plataforma também monitoriza os cronogramas de manutenção e calibração dos dispositivos médicos, assim como mantém todo o histórico de uso do dispositivo, incluindo quem o utilizou e em que contexto[111].

Sistemas *legacy*

Tal como muitos outros setores, também o setor da saúde utiliza sistemas *legacy*. Estes sistemas consistem em *hardware* ou *software* antigo que ainda cumprem as funções para as quais foram adquiridos, mas que são difíceis de tornar seguros por já não receberem atualizações, por não poderem ser integrados com outras tecnologias ou sistemas mais recentes, ou até por não possuírem capacidades criptográficas, deixando-os vulneráveis[112]. De acordo com o livro *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices*, de Robert Seacord, Daniel Plakosh e Grace Lewis, um sistema torna-se *legacy* quando começa a resistir à modificação e evolução. A mesma obra indica também que se um sistema ainda dá algum valor relevante ao negócio, este deverá ser modernizado ou substituído[113].

---

[109] INFARMED, "Pesquisa de Dispositivos Médicos", https://www.infarmed.pt/web/infarmed/pesquisa-dispositivos#.

[110] INFARMED, "Sistema de Informação para Dispositivos Médicos (SIDM)", https://www.infarmed.pt/web/infarmed/infarmed?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=4088116&_101_type=content&_101_urlTitle=sistema-de-informacao-para-dispositivos-medicos-sidm-&inheritRedirect=false.

[111] INFARMED, "Dispositivos Médicos", Perguntas Frequentes, https://www.infarmed.pt/web/infarmed/perguntas-frequentes-area-transversal/novo-sistema-de-informacao-para-dispositivos-medicos-sidm.

[112] Melissa Chase et al., "Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks", MITRE, 15 de novembro de 2023, https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks.

[113] Robert Seacord, Daniel Plakosh e Grace Lewis, *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices* (Boston: Addison-Wesley, 2003), xiii.

A modernização destes sistemas pode ser, no entanto, difícil e, por isso, devem ser tidos em conta diversos fatores para o conseguir fazer, tais como: complexidade, tecnologia e processos de engenharia, risco, componentes comerciais e objetivos de negócio[114].

A utilização deste tipo de sistemas (*legacy*) é comum entre os setores que adquirem equipamentos com ciclos de vida relativamente longos, que podem durar, por exemplo, seis, 10, 20 ou ainda mais anos. Sublinha-se ainda que esta classificação de sistemas não se atribui apenas a grandes máquinas, como as utilizadas para realizar Tomografias Axiais Computadorizadas (TACs), mas também a dispositivos mais pequenos como os já referidos, como bombas de insulina e *pacemakers*.

Acresce ainda que a falta de modernização de alguns sistemas utilizados na saúde tem sido motivo de descontentamento entre os profissionais do setor. Segundo um estudo realizado pela Associação Nacional de Unidades de Saúde Familiar, onde foram inquiridos os coordenadores das 615 unidades, tendo sido reunidas 484 respostas, é notória a insatisfação dos profissionais de saúde com a qualidade dos sistemas utilizados na saúde em Portugal. Todas as unidades indicaram ter tido pelo menos uma falha informática nos 12 meses anteriores ao estudo e cerca de 96,5% dos inquiridos afirma que a falta de acesso às aplicações informáticas perturbou a qualidade dos cuidados prestados[115].

Um dos pontos mais críticos é a falta de interoperabilidade entre os sistemas informáticos levando, por vezes, à introdução da mesma informação várias vezes. Em entrevista ao jornal Expresso, foi indicado por médicos membros da direção da Associação Nacional das Unidades de Saúde Familiar (USF-AN), da Faculdade de Medicina da Universidade do Porto (FMUP) e membros do grupo de trabalho para a gestão da informação em Saúde da Associação Portuguesa de Administradores Hospitalares (APAH) que um dos maiores problemas dos sistemas informáticos é que são desenvolvidos por pessoas sem conhecimento da prática clínica. É expectável que com o investimento que será realizado entre 2021 e 2026, de 300 milhões de euros no âmbito do Plano de Recuperação e Resiliência (PRR), onde este montante tem como objetivo ajudar à transição digital na área da Saúde, a maioria destes problemas sejam resolvidos[116].

Estas falhas referidas acima ajudam a aumentar as ameaças no setor da Saúde. As ciberameaças inerentes aos dispositivos médicos e aos sistemas *legacy* utilizados na saúde serão exploradas em maior detalhe na subsecção seguinte.

[114] Seacord, Plakosh e Lewis, *Modernizing Legacy Systems*, 1.

[115] André Biscaia et al., "Síntese dos resultados do estudo 'O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023: Questionário aos coordenadores de USF'", Associação Nacional das Unidades de Saúde Familiar, https://usf-an.pt/sintese-dos-resultados-do-estudo-o-momento-atual-da-reforma-dos-cuidados-de-saude-primarios-em-portugal-2022-2023-questionario-aos-coordenadores-de-usf/.

[116] Biscaia et al., "O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023".

1.2. Ameaças

O setor da saúde é um dos setores mais apetecíveis para ciberataques por diversos motivos. Este setor contém uma grande riqueza de dados pessoais, desde números de identificação pessoal - como os números de identificação civil, fiscal, da segurança social e de utente, que podem ser utilizados para furto de identidade ou cometer fraudes de seguro -, aos problemas de saúde dos utentes, que podem ser utilizados contra os mesmos[117]. Existe, no setor da saúde, uma maior probabilidade de pagar um resgate quando afetado por *ransomware*[118], uma vez que parar as atividades na saúde pode significar a perda de vidas humanas e, por isso, a prioridade do setor passa por retomar o seu normal funcionamento o mais rápido possível[119].

Será por estes motivos que, no relatório *ENISA Threat Landscape: Health Sector*, publicado em julho de 2023, as duas ameaças mais prevalentes no setor da saúde a nível europeu são o *ransomware* (54% dos incidentes do setor entre 2021 e 2023) e as ameaças relativas a dados (46% dos incidentes também entre 2021 e 2023). Verifica-se uma grande discrepância entre a prevalência destas duas ameaças e quaisquer outras que possam afetar o setor da saúde. Tal demonstra-se pelo facto de a terceira ameaça que mais afetou este setor - a intrusão - ter sido 13% dos ataques, o que significa uma diferença de 33 pontos percentuais entre a segunda e a terceira ameaça mais prevalentes[120].

Os motivos por trás dos ataques de *ransomware* e de ameaças relativas a dados são normalmente os de ganho financeiro. Embora possa haver outros, tais como motivos ideológicos ou de espionagem, o mesmo relatório indica que na vasta maioria dos casos - 83% - os ciberataques realizados ao setor da saúde são motivados por ganho financeiro[121].

A realidade portuguesa não difere da apresentada pela ENISA no relatório referido. No Relatório Riscos e Conflitos de 2023, do Observatório de Cibersegurança do CNCS, evidenciou-se que o setor da saúde é um dos mais atacados em Portugal, e um dos que mais acaba por ter de notificar a CNPD por acessos indevidos a dados pessoais - cerca de 11% no setor privado e 13% no setor público das notificações recebidas pela CNPD vêm deste setor[122]. A par destes dados, é de notar que alguns dos ataques mais graves ocorridos no setor em Portugal foram ataques relativos a dados e de *ransomware*.

Um dos mais graves ciberataques no setor da saúde relativos a dados ocorreu em julho de 2020, em que milhares de credenciais de profissionais do SNS foram furtadas e divulgadas na Internet. No entanto, a lista de credenciais foi eliminada da hiperligação que permitia aceder à mesma algumas horas depois da sua divulgação[123].

---

[117] Richard Pallardy, "The Unique Cyber Vulnerabilities of Medical Devices", *Information Week*, 14 de novembro de 2023, https://www.informationweek.com/cyber-resilience/the-unique-cyber-vulnerabilities-of-medical-devices#close-modal

[118] Forma de ataque que afeta a disponibilidade da informação, bloqueando o acesso de utilizadores legítimos aos ativos de informação, exigindo um resgate - "*ransom*" - para devolver o acesso aos mesmos.

[119] ENISA, "ENISA Threat Landscape: Health Sector", 13, https://www.enisa.europa.eu/publications/health-threat-landscape.

[120] ENISA, "ENISA Threat Landscape: Health Sector", 11.

[121] ENISA, "ENISA Threat Landscape: Health Sector", 19.

[122] CNCS, "Relatório Riscos e Conflitos" (2023), 17, https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf.

[123] Hugo Séneca, "Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet", *Expresso*, 20 de julho de 2020, https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet.

Um outro ataque, de *ransomware*, ocorreu em agosto de 2023, tendo bloqueado o sistema informático do Serviço Regional de Saúde da Madeira, que forçou o regresso ao papel e ao modo analógico de forma a não fechar os hospitais e os centros de saúde. Foi assegurado que os dados clínicos fossem preservados, mas é possível que dados pessoais como números de telefone e números de utente tenham sido expostos[124].

A tabela seguinte faz uma breve apresentação das principais ameaças para o setor, bem como dos agentes de ameaça mais prováveis de concretizar essas ameaças. Esta tabela foi criada através do cruzamento da informação sobre ameaças setoriais recolhida pelo CNCS ao longo de vários anos, informação essa que tem vindo a ser espelhada nos relatórios Riscos e Conflitos[125], 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[126].
- **Agentes estatais:** Estes tipos de agentes caracterizam-se por uma maior sofisticação de meios, fruto da utilização, direta ou indireta, do aparelho de Estado. Atua com intuitos geopolíticos e geoestratégicos, procurando impactar a política interna e externa, bem como as questões da Defesa[127].
- ***Hacktivistas*:** Os *hacktivistas* são agentes de ameaça que se caracterizam por agir em função de uma ideologia, não procurando ganhos materiais ou estritamente reputacionais, embora a projeção mediática tenha importância na afirmação da sua causa. As suas ações são caracterizadas por arquiteturas técnicas de reduzida sofisticação; por uma forte elaboração ficcionada do ciberataque e das suas consequências; e pela propagação mediática dessa ficção em benefício da imagem pública do seu responsável[128].
- **Colaboradores internos:** são agentes que colocam em causa a cibersegurança da organização na qual trabalham. Podem assumir diversas formas quanto à intencionalidade: maliciosos, comprometidos ou negligentes. Malicioso quando colocam em causa a cibersegurança da organização intencionalmente (por motivos económicos, ideológicos ou ressentimento); comprometidos quando são manipulados de modo a agir contra organização, sem saberem que o estão a fazer; e negligentes quando o problema de cibersegurança é resultado da falta de cuidado ou atenção, levando o colaborador a comprometer, por exemplo, uma conta de e-mail ou a instalar *software* malicioso[129]. No caso, consideraram-se os colaboradores internos maliciosos.

[124] Marta Caires, "Serviço de Saúde da Madeira: ataque informático deixa utentes sem consultas e sem exames", *Expresso*, 7 de agosto de 2023, https://expresso.pt/sociedade/2023-08-07-Servico-de-Saude-da-Madeira-ataque-informatico-deixa-utentes-sem-consultas-e-sem-exames-e0cee143

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

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

[127] CNCS, "Relatório Riscos & Conflitos 2021", 75.

[128] CNCS, "Relatório Riscos & Conflitos 2021", 75-76.

[129] CNCS, "Relatório Riscos & Conflitos 2021", 76-77.

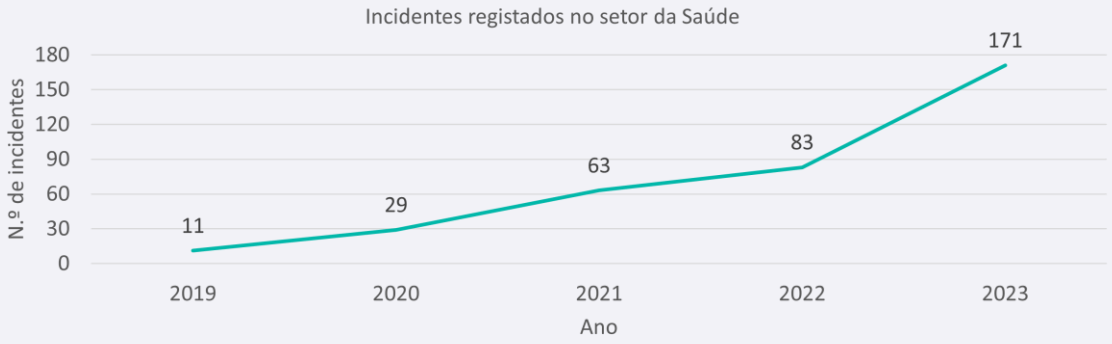
Tabela 2 - Agentes de ameaça mais prováveis

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

Legenda:
■ - Agente de ameaça provável

Segundo dados do CERT.PT, registaram-se, entre 2019 e 2023, 357 incidentes no setor da saúde[130]. Deve-se, no entanto, sublinhar que entre 2019 e 2022, se tinham registado apenas 186 incidentes, ou seja, 171 incidentes foram registados só no ano de 2023. Tal significa que entre 2022, ano em que só se tinham registado 83 incidentes, e em 2023, houve um aumento na incidência de incidentes de 106%[131].

Figura 1 - Número de incidentes no setor da Saúde anualmente



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

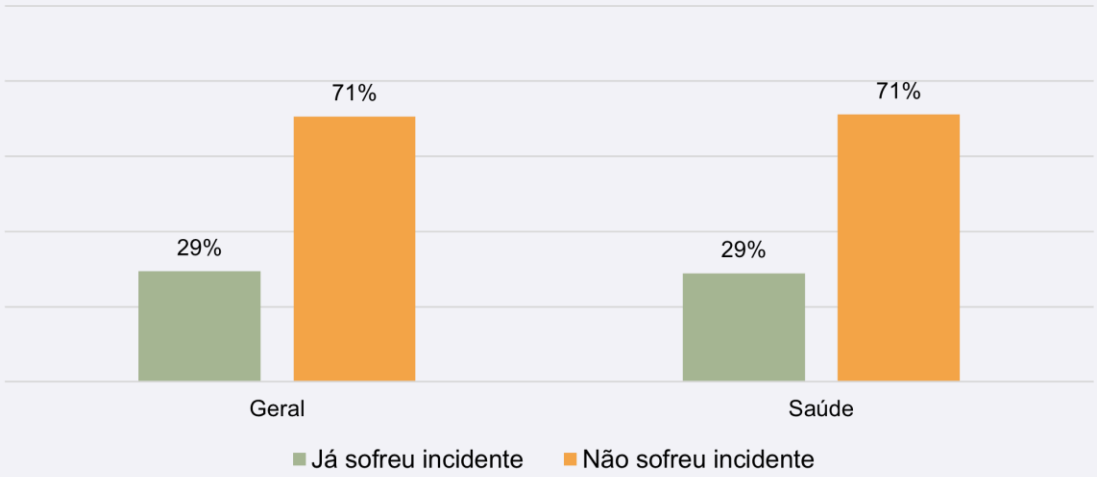
[130] CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024, https://www.cncs.gov.pt/pt/estatistica/.

[131] CNCS, "Relatório Cibersegurança em Portugal: Riscos e Conflitos", 5.ª edição, 2024, 25, https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf.

Os resultados do questionário realizado aos OSE corroboram estas conclusões, uma vez que colocam o setor da saúde entre um dos mais afetados por ciberataques, juntamente com os operadores da banca e dos transportes (**Gráfico 68**), sendo as principais consequências a indisponibilidade dos serviços/sistemas devido a infeção por *malware* (possivelmente, *ransomware*) e a destruição de dados pelo *malware* instalado ou intruso. Os valores deste setor andam a par com os valores gerais de todos os setores.

A estas questões, acresce o facto de pelo menos 448 Unidades de Saúde Familiar terem registado pelo menos uma falha no sistema informático no ano de 2022. Mais de 20% reportaram ter tido problemas mais de 50 vezes. O próprio sistema informático da área da Saúde torna-se uma ameaça por si só, pois um sistema que falha mais de 50 vezes por ano não é fidedigno[132].

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



Retomando o tema dos dispositivos médicos (IoMT e *legacy*) inicialmente abordado em **1.1.3. Especificidades tecnológicas**, importa sublinhar que segundo um relatório de dezembro de 2023 do Government Accountability Office do governo dos Estados Unidos da América (EUA), estes dispositivos têm, em média, 6 vulnerabilidades passíveis de serem exploradas por cibercriminosos[133]. Além disso, cerca de 40% dos dispositivos estarão no fim do seu ciclo de vida, sem *patches* ou atualizações disponíveis[134]. No pior cenário, ciberataques a dispositivos médicos podem afetar o bem-estar do paciente ou até mesmo causar perda de vida.

Nos casos dos dispositivos que são implantados no corpo humano, como *pacemakers*, bombas de insulina e estimuladores de bexiga, entre outros, essas vulnerabilidades devem-se, em parte, às próprias características desses dispositivos: o facto de terem de ser pequenos e leves para não impedirem outras funções fisiológicas e para que as baterias sejam duradouras, o espaço para *hardware* é muito limitado. Nalguns casos, não é necessário mais do que um sinal de rádio na frequência certa para interferir com estes dispositivos.

[132] Biscaia et al., "O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023".
[133] United States Government Accountability Office, "Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination", Report to Congressional Committees, dezembro de 2023, 6, https://www.gao.gov/assets/d24106683.pdf.
[134] "Hospitals' IoMT Device Security Risk Quantified in New Report", MedTech Dive, 23 de agosto de 2023, https://www.medtechdive.com/press-release/20230823-hospitals-iomt-device-security-risk-quantified-in-new-report/.

Noutros casos como, por exemplo, com dispositivos que possam ser controlados através de um *smartphone* ou que transmitam dados para bases de dados, estes podem servir como ponto de entrada noutros sistemas para obter outras informações[135].

Os dispositivos médicos, grandes e pequenos, são difíceis de substituir, no primeiro caso, porque a substituição de grandes máquinas é dispendiosa e pode obrigar a interromper o atendimento e a realização de exames urgentes aos utentes e, no segundo caso, porque substituir dispositivos implantáveis para os atualizar obrigaria a operar os pacientes que utilizam esses dispositivos e, em diversos casos, as operações acarretariam riscos que os pacientes não estão dispostos a aceitar, acabando assim por assumir um outro tipo de risco relativo à desatualização dos dispositivos implantados[136].

Embora seja mais provável que as escolhas dos alvos dos agentes de ameaça recaiam sobre as bases de dados de instituições maiores em vez de sobre indivíduos, os ataques a pessoas singulares que utilizam os dispositivos referidos não deixam de ser uma possibilidade e uma ameaça preocupante.

[135] Pallardy, "Cyber Vulnerabilities of Medical Devices", *Information Week.*

[136] Pallardy, "Cyber Vulnerabilities of Medical Devices", *Information Week*.

1.3. Capacitação

Em 2017, uma série de ciberataques, principalmente de *ransomware* (*WannaCry* e *Petya*), assolou vários países europeus, em particular a Ucrânia. O Banco Central Ucraniano, o sistema de comboios metropolitanos e a empresa estatal de energia da Ucrânia foram os principais afetados[137]. Em Portugal, face a esta série de ataques, a SPMS desligou preventivamente o sistema de *e-mail* do SNS, tendo na altura evitado que o SNS português se juntasse ao grupo de entidades afetadas pelos ataques de *ransomware*[138]. Na sequência destes eventos, o ano de 2017 foi particularmente rico em iniciativas que visavam o reforço da cibersegurança no SNS.

Entre as iniciativas mais recentes, contam-se:

- Estruturar o circuito para o registo de incidentes de segurança;
- Elaborar iniciativas de auditoria à utilização da Política de Segurança com base na ISO 27799;
- Promover e sensibilizar a importância da segurança de informação nos Sistemas de Informação da Saúde;
- Adotar as boas práticas em alinhamento com a *Framework ITIL V3 - Foundation*;
- Promover nas entidades do SNS um processo de melhoria contínua do nível da Cibersegurança[139].

A SPMS, responsável pela formação em matéria de cibersegurança no setor da saúde, tem criado campanhas de sensibilização para o tema, na qual se insere a criação de dicas mensais, manuais de cibersegurança, infografias[140] e de oportunidades de formação[141]. A mesma disponibiliza ainda uma ligação para uma página denominada “Alertas e Segurança”, onde é possível consultar informação referente a boas práticas[142].

[137] Christian Borys, “The day a mysterious cyber-attack crippled Ukraine”, *BBC*, 4 de julho de 2017, https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.

[138] SPMS, “Circular Normativa n.º 03/2017: medidas excecionais de segurança”, 19 de maio de 2017, 1, https://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA3-Medidas-Excecionais-de-Ciberseguran%C3%A7a.pdf.

[139] Agência para a Modernização Administrativa (AMA), “Cibersegurança na Administração Pública: O Imperativo da Conformidade Global no SNS”, *Encontros SAMA 2020* (Lisboa), 26 de abril de 2020, https://bo.tic.gov.pt/api/assets/etic/2e7a0cf7-68f5-4008-a95f-29594569d584/ .

[140] SPMS, “Cibersegurança”, abril de 2019, https://www.spms.min-saude.pt/2019/04/ciberseguranca-2/.

[141] SPMS, “Conteúdos de Sensibilização de Cibersegurança”, Academia SPMS, https://academia.spms.min-saude.pt/atis-de-sensibilizacao-de-ciberseguranca/.

[142] SPMS, “Alertas e Segurança”, https://www.spms.min-saude.pt/alertaseseguranca/.

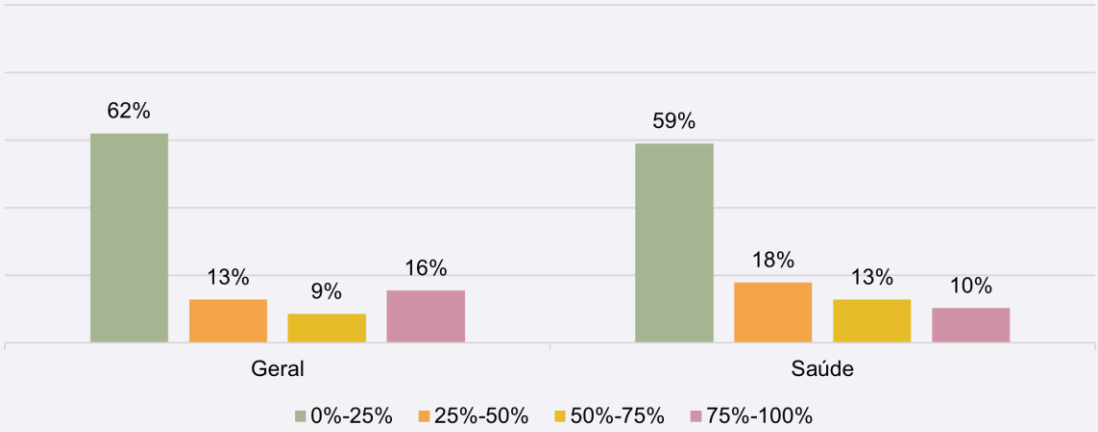
Adicionalmente, a 29 de janeiro de 2020, Portugal foi eleito como *Chair* do *Work Stream* criado para o setor da saúde, no âmbito do *NIS Cooperation Group*. Neste contexto o CNCS ficou responsável pela coordenação dos trabalhos, com o apoio da SPMS. Este evento decorreu em Bruxelas, na 14º reunião do *NIS Cooperation Group,* que foi criado pela Diretiva NIS no ano de 2016, cujo objetivo passava por garantir a cooperação estratégica e a partilha de informações entre os Estados Membros da UE acerca das temáticas de segurança da informação e cibersegurança. A criação do grupo *Work Stream for Health setor*, surgiu na sequência de uma proposta do *European Cybersecurity Health Group* (ECHG), do qual faz parte a SPMS, e decorreu da necessidade de harmonização das práticas e requisitos mínimos de proteção da informação da saúde, cada vez mais fundamental num contexto de saúde heterogéneo e interconectado. No decorrer da reunião, vários foram os países que encorajaram este trabalho, e prontificaram-se a participar ativamente nestas discussões, considerando que a cibersegurança em saúde não pode ser descurada, uma vez que, em última instância, estará em causa o risco de vida dos utentes[143].

Um outro momento marcante no setor foi o da pandemia de COVID-19, não só pelo enorme esforço exigido aos profissionais de saúde no combate à doença e à prestação de cuidados, mas também pelo grande aumento de ciberataques que houve nessa altura. Segundo um relatório da Check Point, a nível mundial, entre fevereiro de 2020 e abril de 2020, o número de ciberataques registados relacionados com a pandemia aumentou 40 vezes, de 5000 ataques por semana para 200 mil[144]. O confinamento e a rápida passagem ao teletrabalho de milhões de trabalhadores em todo o mundo sem que houvesse tempo para implementar medidas de segurança adequada nos seus dispositivos de trabalho foi uma oportunidade prontamente explorada pelos agentes de ameaças[145]. Este aumento exponencial dos ciberataques colocou a cibersegurança no centro das preocupações de pessoas individuais, empresas e governos. No entanto, o setor da saúde parece estar aquém do desejável em termos de capacitação em cibersegurança.

[143] SNS, "Portugal lidera Grupo Europeu criado para o setor da saúde", 30 de janeiro de 2020, https://www.sns.gov.pt/noticias/2020/01/31/saude-cibersegurança/.
[144] "Cyber Attack Trends: 2020 Mid-Year Report", *Checkpoint*, 22 de julho de 2020, 4, https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/.
[145] "Observatório de cibersegurança: nº 4/2021", CNCS, setembro de 2021, 1 https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf.

Embora seja possível verificar que o reforço da cibersegurança é uma preocupação e um objetivo estratégico do setor há vários anos, tanto através dos planos de atividades e orçamentos, como através das campanhas de sensibilização para o tema, as múltiplas notícias que reportam más práticas de cibersegurança no setor, bem como o questionário realizado no âmbito deste relatório revelam que o impacto destas medidas tem ficado aquém do desejado. De acordo com o questionário realizado, em quase 60% dos operadores do setor, apenas 0%-25% dos profissionais de saúde têm formação básica em cibersegurança. Já no âmbito geral, cerca de 62% dos operadores têm 0%-25% dos profissionais com formação básica em cibersegurança, o que demonstra que este setor, comparado com os outros setores, tem mais profissionais com formação em cibersegurança (**Gráfico 33**).

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



Este é, no entanto, um cenário que pode vir a mudar. É importante relembrar que no seguimento dos impactos negativos causados pela pandemia surgiram também planos para os mitigar. Um dos mais importantes desses planos será o Plano de Recuperação e Resiliência (PRR), que gerou uma oportunidade sem precedentes para o investimento em cibersegurança, que será explorada em 1.4. Investimento em cibersegurança.

1.4. Investimento em cibersegurança

Tal como referido em

1.3. Capacitação, o PRR veio gerar uma oportunidade sem precedentes para o investimento em cibersegurança no setor da saúde. Ao todo, serão investidos, até ao final de 2024, cerca 300 milhões de euros para a transição digital da saúde, que se repartem por quatro pilares de investimento[146]. Os quatro pilares são:

- **Pilar I**: Reforma e Modernização da Rede de Dados da Saúde;
- **Pilar II**: Reforma dos Sistemas de Informação disponibilizados ao Cidadão;
- **Pilar III**: Reforma dos Sistemas de Informação disponibilizados aos Profissionais de Saúde;
- **Pilar IV**: Reforma do Sistema de Informação dos Registos Nacionais, Interoperabilidade e Circuito Digital do Medicamento, DM e MCDT[147].

O pilar no qual se insere o investimento em cibersegurança é o Pilar I, da reforma e modernização da rede de dados da saúde. O principal objetivo deste pilar é a renovação da infraestrutura digital do SNS e essa renovação compreende:

- A substituição do parque informático ao serviço dos profissionais do SNS, por equipamentos e dispositivos mais recentes e atualizados;
- O desenvolvimento de dois polos de infraestrutura central, os dois com redundância em tempo real e com reforço das condições locais de redes e dados;
- Reforço do nível da segurança de informação e cibersegurança;
- Alavancar o desenvolvimento de um *Data Lake* (repositório massivo de dados nativos[148]) universal e transversal ao SNS[149].
- Espera-se, através da prossecução desses projetos, atingir os seguintes resultados:
- Assegurar a efetiva resiliência e redundância de serviços digitais no SNS;
- Melhoria do desempenho e segurança dos serviços e aplicações, comunicações e dados de saúde;
- Reforço muito substancial de robustez e fiabilidade ao nível da SI e cibersegurança;
- Neutralização da exposição a riscos, falhas e incidentes;
- Redução dos custos indiretos resultantes de falhas e incidentes[150].

Dos 300 milhões de euros do PRR destinados à saúde, 116 milhões ficam alocados a este primeiro pilar[151].

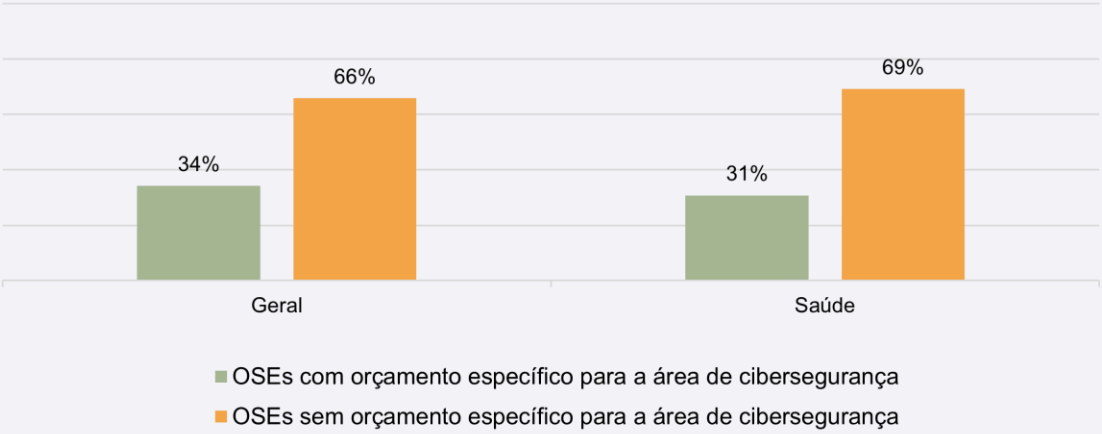
[146] Recuperar Portugal, "Investimento RE-C01-i06: Transição Digital da Saúde (300 M€)", 8 de junho de 2021, https://recuperarportugal.gov.pt/2021/06/08/investimento-re-c01-i06/.
[147] SPMS, "Plano de Atividades e Orçamento 2022", 76, setembro de 2021, https://www.spms.min-saude.pt/wp-content/uploads/2022/09/Plano-de-Atividades-e-Orcamento-2022_Assinado_09092022.pdf.
[148] Dados próprios da aplicação ou aplicações do SNS e não de terceiros.
[149] SPMS, "Plano de Atividades e Orçamento 2022", 107.
[150] SPMS, "Plano de Atividades e Orçamento 2022", 107.
[151] SPMS, "Plano de Atividades e Orçamento 2022", 111.

A execução orçamental dos fundos do PRR está, no entanto, atrasada. Na calendarização inicial, previa-se que o investimento no primeiro pilar ficaria completo até ao final de 2022. Contudo, em fevereiro de 2024, ainda só cerca 17% dos 300 milhões de euros (52,4 milhões) tinham sido pagos[152].

Além disso, a larga maioria do investimento parece estar alocada à aquisição de equipamento[153], sendo raras as referências à formação dos profissionais de saúde em matéria de cibersegurança. Embora a atualização de equipamento e de sistemas seja uma parte fundamental da cibersegurança, é também importante que não seja esquecida a formação dos recursos humanos que vão utilizar esses equipamentos e sistemas. Como se sabe, a maioria dos incidentes de cibersegurança devem-se a erro humano e, tal como já foi evidenciado, a falta de formação dos profissionais de saúde em cibersegurança é uma fragilidade prevalente no setor.

Deste setor, cerca de 31% 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



[152] Recuperar Portugal, "Monitorização", https://recuperarportugal.gov.pt/monitorizacao/.
[153] SPMS, "Plano de Atividades e Orçamento 2022", 76.

Relativamente às áreas de aplicação do orçamento de cibersegurança, 92% aplica na segurança das redes, 75% na capacitação em tecnologia e aquisição de *hardware* e 67% em gestão de vulnerabilidades, análise de segurança e aquisição de *software*. Em relação à média geral, a maior diferença está na aquisição de *software* e formação, estando este setor abaixo da mesma (**Gráficos 110 e 110.4**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

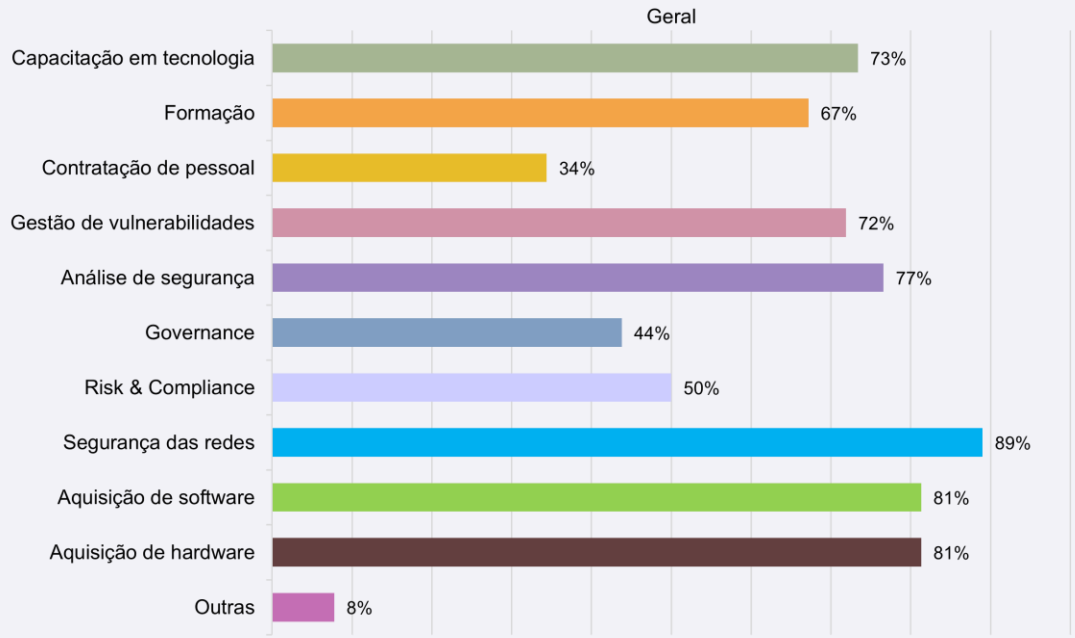
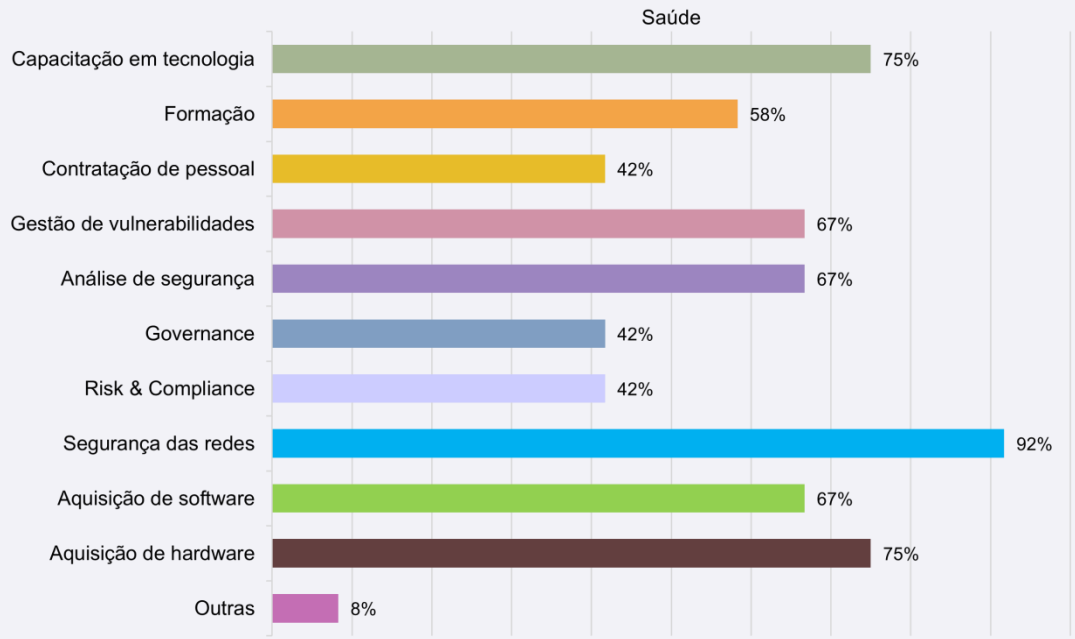
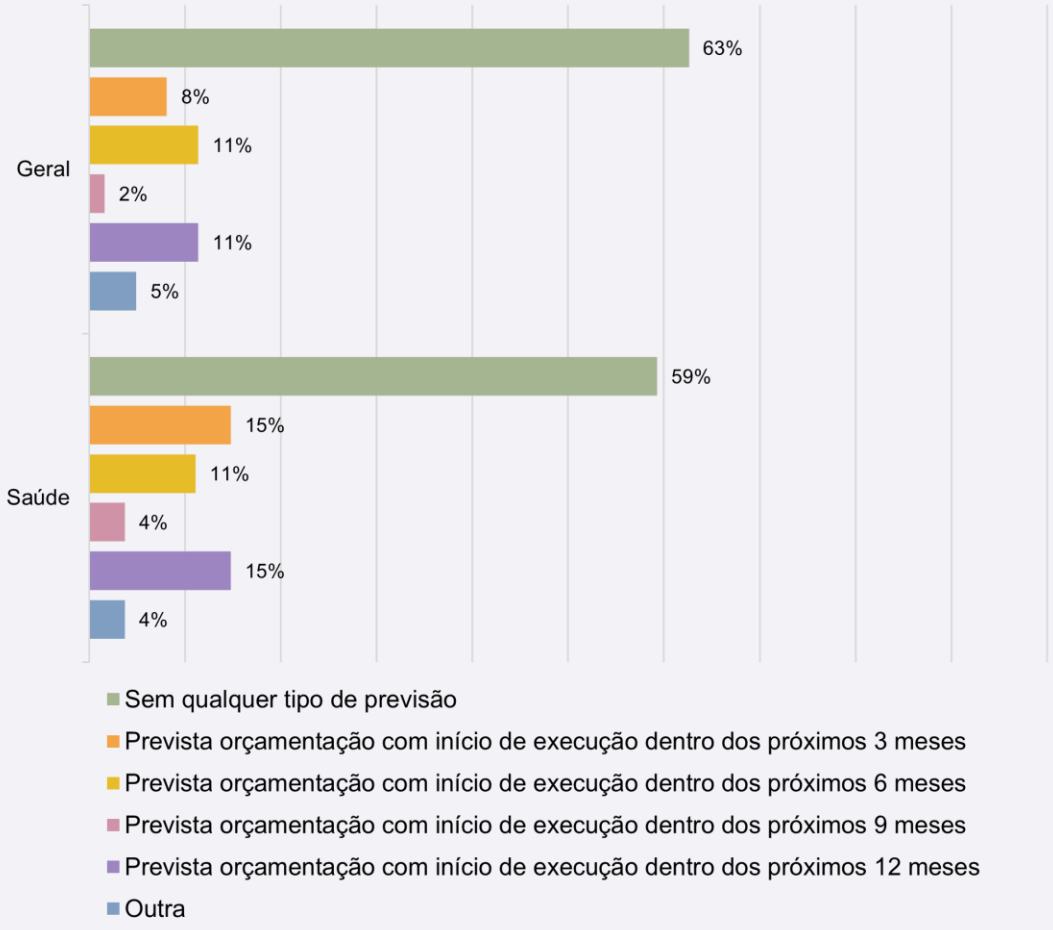


Gráfico 110.4 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 59% não tem qualquer previsão para a orçamentação, 15% tem previsto a orçamentação dentro dos próximos 3 meses ou 12 meses e 11% tem previsto a orçamentação para os próximos 6 meses. A maior diferença para o setor geral está na orçamentação a 3 e 12 meses com uma diferença de 7 pp e 4 pp, respetivamente (**Gráfico 111**).

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



1.5. RJSC e legislação setorial

O setor da saúde não é, quer a nível nacional, quer a nível europeu, um setor amplamente legislado ao nível da cibersegurança. No entanto, legislação como o Despacho n.º 8877/2017 estabelece importantes bases sobre estas matérias, tais como o modelo de governação a seguir pela SPMS, em articulação com o Gabinete Nacional de Segurança e Centro Nacional de Cibersegurança (GNS/CNCS), as medidas e procedimentos de segurança a adotar pelas entidades prestadoras de cuidados de saúde, ao nível da gestão do risco, da nomeação de CISO e CSO, e elaboração de relatórios sobre o nível de implementação de políticas e controlos de segurança na entidade, de forma a permitir avaliar e comparar níveis de maturidade, orientações sobre a aquisição e gestão de tecnologias com vista à cibersegurança, a necessidade de realizar auditorias e avaliações de cibersegurança, versando ainda sobre a capacitação e recursos humanos e o investimento em cibersegurança[154]. O mesmo despacho exige que todas as entidades do SNS adotem uma política de cibersegurança, que tenham um plano de contingência em caso de incidentes de cibersegurança e impele à cooperação e partilha de informação entre as várias entidades do SNS[155].

Há também legislação mais abrangente, destinada a múltiplas entidades, para além dos OSE, tal como a Lei da Proteção de Dados (Lei n.º 58/2019, de 8 de agosto), decorrente do Regulamento Geral sobre a Proteção de Dados, que impõe múltiplas obrigações ao nível do tratamento e proteção dos dados pessoais recolhidos, desde medidas de proteção, à obrigação de notificação aos titulares dos dados em caso de violação dos mesmos.

Aliás, na legislação existente sobre proteção de dados pessoais, os dados relativos à saúde constituem uma categoria especial de dados, tais como os dados pessoais que "revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas ou a filiação sindical, bem como os dados genéticos, os dados biométricos destinados a identificar uma pessoa singular de forma inequívoca (...) ou dados relativos à vida sexual ou à orientação sexual"[156] dos seus titulares. Tais dados podem ser apenas tratados com o consentimento explícito dos seus titulares, ou se o seu tratamento "for necessário para efeitos do cumprimento de obrigações e do exercício de direitos específicos (...) em matéria de legislação laboral, de segurança social e de proteção social (...), necessário para proteger os interesses vitais do titular ou de outra pessoa (...) se o tratamento for necessário para efeitos de medicina preventiva ou do trabalho, para a avaliação da capacidade de trabalho do empregado, o diagnóstico médico, a prestação de cuidados ou tratamentos de saúde ou de ação social" ou se este for necessário "por motivos de interesse público no domínio da saúde pública"[157].

[154] Despacho n.º 8877/2017, de 9 de outubro, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/despacho/8877-2017-108269312.
[155] Despacho n.º 8877/2017.
[156] Regulamento Geral sobre a Proteção de Dados, de 27 de abril de 2016 (artigo 9.º, n.º 1), https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis.
[157] Regulamento Geral sobre a Proteção de Dados, de 27 de abril de 2016 (artigo 9.º, n.º 2, alíneas a) a i).

Surge, depois, legislação multissetorial, tal como o Regime Jurídico da Segurança do Ciberespaço (RJSC), que transpõe a Diretiva 2016/1148 (Diretiva NIS), acompanhado do decreto-lei n.º 65/2021, de 30 de julho, que regulamenta o RJSC, em diversas obrigações para os OSE a nível de cibersegurança, tais como a nomeação de um contacto permanente para articulação com o CNCS, a nomeação de um responsável de segurança, a elaboração de um inventário de ativos, de um plano de segurança, de um relatório anual, de análise, gestão e tratamento do risco, e de notificação de incidentes. As diferentes obrigações legais que vão surgindo em matéria de cibersegurança tendem a conduzir as entidades a elas sujeitas a níveis mais elevados de maturidade, adotando práticas, processos e procedimentos cada vez mais seguros e robustos. Contudo, apesar da obrigatoriedade do cumprimento do RJSC, é notório que há um baixo cumprimento do exigido ao nível da análise do risco no setor da saúde, com apenas cerca de 50% das entidades a realizarem-na, segundo os dados do questionário.

O setor está ainda sujeito à Diretiva (UE) 2022/2555[158], ou Diretiva NIS 2, que veio atualizar a Diretiva anterior passados seis anos sobre a sua publicação. A NIS 2 classifica dois tipos de setores: "setores de importância crítica"[159] e "outros setores críticos"[160]. 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. O setor da saúde é um dos setores que passa abranger mais entidades. Enquanto a Diretiva NIS 1 incluía apenas instalações de prestação de cuidados de saúde (hospitais e clínicas privadas), a NIS 2 passa a incluir também no setor os laboratórios de referência da UE, entidades que fabricam produtos farmacêuticos de base e entidades que que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde pública[161].

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[162]. 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[163]. A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança, tais como "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[164].

---

[158] 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

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

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

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

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

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

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

1.6. Standards e boas práticas aplicáveis

O setor da saúde dispõe de um conjunto alargado de *standards* internacionais que, diretamente ou indiretamente, se relacionam com o *procurement* de produtos e serviços no setor.

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

Tabela 3 - Standards e Boas Práticas

Standards	Boas práticas
• ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002 • Health Insurance Portability and Accountability Act (HIPPA) • ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purpOSE • ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices • ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth; • Digital Imaging and Communications in Medicine (DICOM) • EC Medical Devices Regulation (text agreed by EP and Council - in adoption process) • NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide • Manufacturer Disclosure Statement for Medical Device Security (MDS2)	• Royal Australian College of General Practitioners (RACGP) Computer Information Security Standards (CISS)

Na tabela anterior estão os *standards* referentes à área da saúde. De seguida, apresenta-se um breve sumário de cada um:

- **ISO 27799:2008 Health informatics - Information security management in health using ISO/IEC 27002:** Este *standard* estabelece diretrizes específicas para a gestão de segurança da informação em ambientes de saúde, baseando-se nos princípios e boas práticas da norma ISO/IEC 27002[165];
- **Health Insurance Portability and Accountability Act (HIPPA):** A *HIPPA* é uma legislação dos Estados Unidos que foi promulgada em 1996 e tem como objetivo proteger a privacidade e a segurança das informações de saúde das pessoas[166];

[165] ISO, "Health informatics — Information security management in health using ISO/IEC 27002", julho de 2008, https://www.iso.org/standard/41298.html.

[166] Centers for Medicare & Medicaid Services, "HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules", fevereiro de 2023, https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf.

- **ISO 13485:2003 Medical devices -- Quality management systems – Requirements for regulatory purpOSE:** Esta norma especifica os requisitos para um sistema de gestão da qualidade para a indústria de dispositivos médicos. Foi projetada para ser utilizada por organizações envolvidas no *design*, produção, instalação e manutenção de dispositivos médicos[167];
- **ISO 80001-1:2010 Application of risk management for IT networks incorporating medical devices:** Esta norma especifica os requisitos para a aplicação de gestão de riscos em redes de *IT* que incorporam dispositivos médicos[168];
- **ETSI eHealth Standard TR 102 764 eHEALTH; Architecture; Analysis of user service models, technologies and applications supporting eHealth:** É um relatório técnico que foi publicado pela *ETSI* onde é abordada a arquitetura, modelos de serviços de utilizadores, tecnologias e aplicações de suporte ao *eHealth*[169];
- **Digital Imaging and Communications in Medicine (DICOM):** Conjunto de normas desenvolvidas para a gestão, armazenamento, impressão e transmissão de informações em imagens médicas. Este conjunto de normas assegura a interoperabilidade entre diferentes sistemas e dispositivos utilizados em radiologia, cardiologia, entre outras áreas[170];
- **EC Medical Devices Regulation (text agreed by EP and Council - in adoption process):** Este regulamento, cujo texto foi acordado pelo Parlamento Europeu e pelo Conselho Europeu, está num processo de adoção e tem como objetivo substituir as diretivas anteriores sobre os dispositivos médicos (93/42/EEC e 90/385/EEC)[171];
- **NIST SP 800-66 An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Guide:** É um guia elaborado pelo *NIST* e tem como objetivo fornecer orientações introdutórias para a implementação dos requisitos de segurança da *HIPAA*[172];
- **Manufacturer Disclosure Statement for Medical Device Security (MDS2)**: É um documento utilizado pelos fabricantes de dispositivos médicos onde é fornecido informações detalhadas sobre a segurança e a capacidade de gestão de riscos dos dispositivos[173].

Um *standard* do setor muito relevante para a temática da cibersegurança e *procurement* é o *Manufacturer Disclosure Statement for Medical Device Security (MDS2).* O formulário MDS2 dota os fornecedores de equipamentos médicos com os meios necessários para a divulgação das funcionalidades relacionadas com segurança dos seus equipamentos.

[167] ISO, “Medical devices — Quality management systems — Requirements for regulatory purposes”, julho de 2003, https://www.iso.org/standard/36786.html.
[168] ISO, “Application of risk management for IT-networks incorporating medical devices”, outubro de 2010, https://www.iso.org/standard/44863.html.
[169] ETSI, “Analysis of user service models, technologies and applications supporting eHealth”, fevereiro de 2009, https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf.
[170] DICOM, “Digital Imaging and Communications in Medicine (DICOM)”, maio de 2017, https://www.researchgate.net/publication/355550688_Digital_Imaging_and_Communications_in_Medicine_DICOM.
[171] Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.° 178/2002 e o Regulamento (CE) n.° 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho, https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32017R0745.
[172] NIST, “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide”, fevereiro de 2024, https://csrc.nist.gov/pubs/sp/800/66/r2/final.
[173] Asimily, “What are MDS2s and Why Should You Care”, https://asimily.com/blog/what-are-mds2s-and-why-should-you-care.

O formulário contém um conjunto de questões relativas aos equipamentos médicos e permite a comparabilidade de funcionalidades de segurança entre diferentes equipamentos de diferentes fabricantes.

Adicionalmente, a *ISO* está a desenvolver mais de 25 novos *standards* focados em informática médica, dos quais se destacam:

- **ISO/DTR 21332 *Health informatics***: Considerações sobre segurança e privacidade de informação em sistemas de computação em *cloud*[174]*;*
- **ISO/WD 13131 *Health informatics:*** Linhas orientadoras para planeamento de qualidade em prestação de serviços de saúde à distância (*telehealth*)[175];
- **ISO/AWI 22697 *Health informatics:*** Aplicação de boas práticas de gestão de privacidade de dados a informação de saúde pessoal[176].

[174] ISO, "Health informatics — Cloud computing considerations for the security and privacy of health information systems", 2021, https://www.iso.org/standard/70568.html.
[175] ISO, "Health informatics — Telehealth services — Quality planning guidelines", 2021, https://www.iso.org/standard/75962.html.
[176] ISO, "Health informatics — Application of privacy management to personal health information", https://www.iso.org/standard/73697.html.

1.7. Desafios

O setor da saúde continuará a ser um alvo muito apetecível por parte dos cibercriminosos devido à riqueza dos dados que armazena. A par dessa atratividade para os atacantes devida ao tipo de dados armazenados, a utilização de equipamentos e sistemas menos seguros, como nos dispositivos médicos implantáveis, ou nos equipamentos e sistemas *legacy*, continua a ser uma vulnerabilidade do setor. Mesmo com a atualização prevista dos equipamentos através dos fundos do PRR, não há sistemas 100% seguros.

Um outro desafio enfrentado pelo setor são as práticas pouco seguras no âmbito da cibersegurança. Este é um desafio que possivelmente poderia ser solucionado com formação adequada, mas num setor em que muitos dos turnos de médicos e enfermeiros estão a ser assegurados pela realização de horas extraordinárias, o tempo para mais do que a prestação de cuidados de saúde, como formações em cibersegurança, é escasso.

A criação de um *data lake*[177] neste setor, no qual podem existir práticas pouco seguras e há uma falta generalizada de formação no âmbito da cibersegurança, poderá constituir um elevado risco de segurança. Se dados pouco agregados já são um alvo apetecível, um repositório massivo de dados interoperáveis sê-lo-á ainda mais. Será necessária uma arquitetura de segurança robusta, bem como uma seleção criteriosa de quem poderá aceder ao *data lake* e formação adequada para a proteção do mesmo. Um facto importante é de que o ser humano tem um papel principal na maioria dos incidentes de cibersegurança (95%), tendo as falhas tecnológicas um papel menos importante[178].

De acordo com um relatório da Check Point, os ataques por via tecnológica tiveram um aumento de 40% a nível global (entre 2021 e 2022), sendo a saúde um dos setores mais afetados[179]. Acresce a este facto que o número de dispositivos médicos interligados em rede aumentou nos últimos anos, sendo que a maior parte dos sistemas utilizados por hospitais não tiveram um desenvolvimento focado na segurança informática, pelo que estão mais vulneráveis. Um exemplo desta falta de desenvolvimento focado na segurança informático é o facto de ainda serem utilizados em hospitais computadores cujo sistema operativo é o *Windows* 95 que já não é suportado pela *Microsoft* desde 2006[180].

Atualmente, a maior parte dos dispositivos médicos estão ligados à rede, alguns destes dispositivos são deveras importantes para o paciente, tais como: bombas de infusão, ventiladores, máquinas de hemodiálise, entre outros. É referido ainda que houve um ciberataque na Alemanha que levou à morte de uma paciente, tendo este ficado identificado como o primeiro homicídio causado por um ataque desta natureza[181]. De forma a ser possível prevenir este tipo de ataques é importante que todo o pessoal do setor da saúde coloque em prática os *standards* e as boas práticas de cibersegurança. Estas estarão descritas no próximo subcapítulo.

---

[177] Repositório central com o propósito de guardar, processar e proteger grandes quantidades de dados (fonte: "What is a Data Lake?", Google Cloud, Google, https://cloud.google.com/learn/what-is-a-data-lake).

[178] Paul Mee e Rico Brandenburg, "After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk", *World Economic Forum*, 17 de dezembro de 2020, https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/.

[179] Check Point Research, 2023 Cyber Security Report, Check Point, 2023, 48.

[180] "Cyberattacks on the Healthcare Sector", *Checkpoint*, 2023, https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/ .

[181] "Cyberattacks on the Healthcare Sector", *Checkpoint*.

1.8. Recomendações

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

Tabela 4 - Cenários de risco

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Campanha de *PHISHING* dirigida a colaboradores ou utentes da entidade com o fim de furtar dados sensíveis, como credenciais de *login* ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Intrusão em base de dados de utentes, fazendo uso de vulnerabilidades técnicas em formulários ou noutras funcionalidades de entrada de **APLICAÇÃO *WEB*** (*SQL Injection* ou *Cross-site Scripting*).
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 utentes, 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 23 de setembro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.pdf)

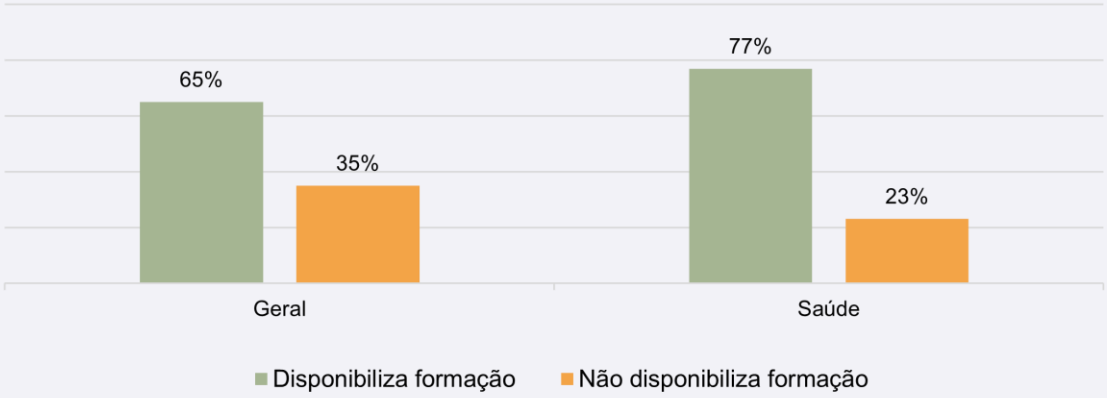
Com base nos resultados obtidos no questionário dirigido aos OSE, bem como as especificidades tecnológicas do mesmo e as principais ameaças identificadas no setor da saúde, sugerem-se diversas recomendações que se consideram pertinentes para as entidades do setor.

Formação

Como referido, as ameaças mais prevalentes no setor são o *ransomware* e ameaças relativas a dados, ameaças que geralmente só se concretizam quando tentativas de engenharia social são bem-sucedidas. A sensibilização para este tipo de riscos e a formação para identificar tais tentativas são essenciais para impedir que estas se concretizem, pois a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida, ou que se utilizem, por exemplo, *pendrives* de origem desconhecida[182], entre outras ações de risco.

Os resultados do questionário evidenciam que apesar de a maioria dos OSE do setor disponibilizarem formação em cibersegurança aos seus colaboradores (**Gráfico 38**), a maioria das formações (cerca de dois terços) são de caráter facultativo, e não obrigatório (**Gráfico 39**). Além disso, na maioria das entidades os momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor da saúde 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 38 - Disponibilização de formação em cibersegurança aos colaboradores



[182] "O maior banco do mundo sofreu ataque de ransomware e salvou-se graças a uma… pen USB", *PplWare*, 12 de novembro de 2023, https://pplware.sapo.pt/internet/o-maior-banco-do-mundo-sofreu-ataque-de-ransomware-e-salvou-se-gracas-a-uma-pen-usb/.

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

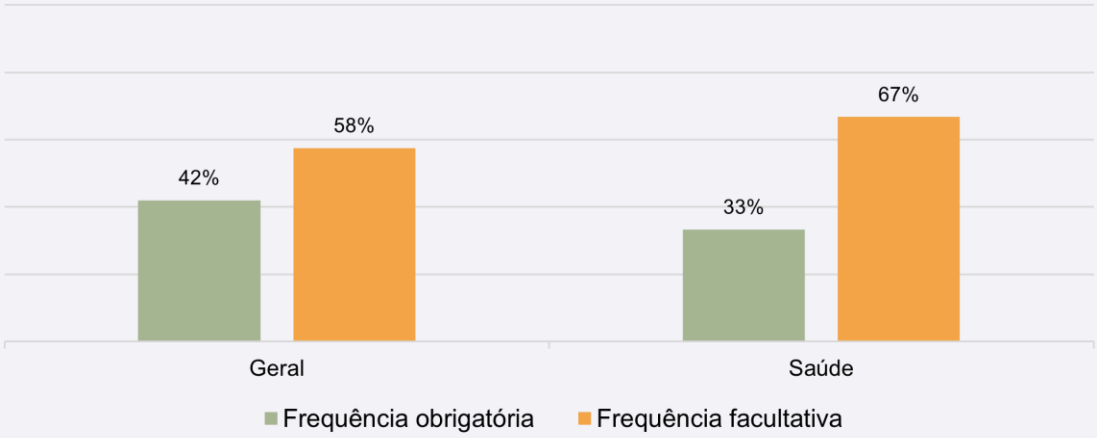
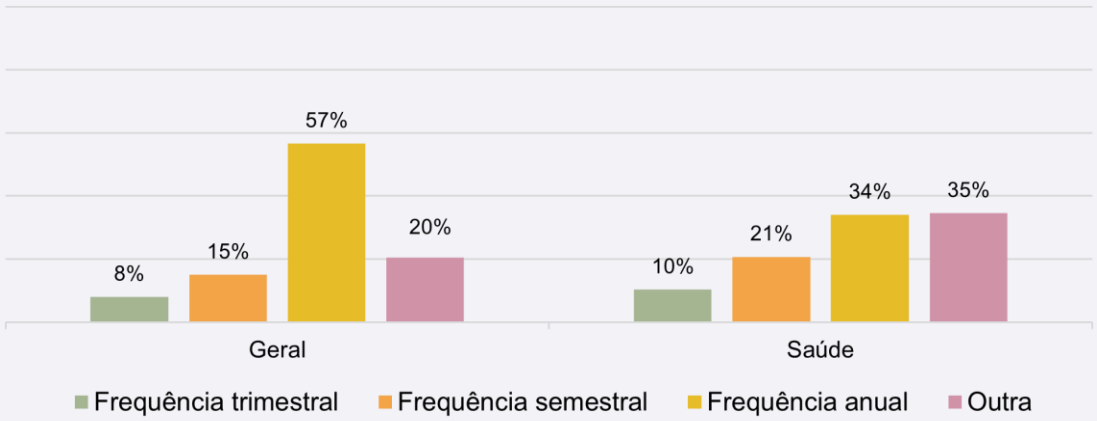


Gráfico 41 - Frequência média dos momentos de formação



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 saúde, comparativamente com os restantes, é um dos setores onde menos se observa a realização de avaliações de segurança, de utilização de autenticação multifator, de cifragem, de sistemas de gestão de palavras-passe e de análises de risco periódicas.

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

- Realizem avaliações de segurança pelo menos anualmente;
- Realizem análises de risco com periodicidade mínima anual;
- Implementem, onde possível, métodos de autenticação multifator;
- Utilizem, nos ficheiros relevantes e dados sensíveis, cifragem;
- Utilizem sistemas de gestão de palavras-passe, de modo a viabilizar a utilização de diversas palavras-passe complexas e seguras para cada sistema.

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. Por exemplo, a autenticação multifator pode impedir a progressão caso uma palavra-passe seja descoberta e a cifragem pode evitar que os dados sejam utilizados mesmo tendo sido obtidos.

Políticas, procedimentos e planos de cibersegurança

De acordo com os dados obtidos no questionário, apenas 59% dos OSE do setor tinham documentado e implementado políticas e procedimentos de cibersegurança. Adicionalmente, apenas 46% dos inquiridos no setor contemplavam a cibersegurança nos seus planos de segurança.

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

- Os diversos papéis e responsabilidades dos colaboradores em matéria de cibersegurança;
- A identificação, avaliação, tratamento e mitigação dos riscos de cibersegurança;
- Os controlos de segurança, tais como os controlos de acesso (lógico e físico);
- A gestão de incidentes, devendo ser elaborados um plano de resposta a incidentes, com procedimentos para a deteção, identificação, resposta e recuperação dos mesmos, bem como um plano de comunicação de incidentes;
- A conformidade legal, de modo a garantir que a organização cumpre todas as leis e regulamentos aplicáveis;
- A revisão e atualização da política, de forma periódica (no mínimo, anual), de modo a manter atualizada face à evolução das ameaças de cibersegurança e da própria organização.

Face à baixa percentagem de OSE do setor que indicaram possuir uma política de continuidade de negócio (39%), recomenda-se também a elaboração de uma tal política alinhada com a política de cibersegurança.

A elaboração de políticas, procedimentos e planos de cibersegurança e a comunicação destes aos profissionais, quer de saúde, quer das áreas tecnológicas, é também uma forma de dar a conhecer a estes o que lhes é permitido ou não fazer em contexto de cibersegurança, como devem tratar ativos de informação, desde dados sensíveis a dispositivos, e como devem atuar perante uma situação suspeita ou de concretização de uma ameaça.

Modernização dos sistemas *legacy*

A existência de sistemas *legacy* acaba por constituir um risco ou ameaça no setor da saúde. Embora seja uma tarefa difícil, devem ser procuradas formas de evitar o aparecimento deste tipo de sistemas. Para tal, é necessário haver avaliações regulares por parte do departamento de TI e desenvolver planos de ação claros para a modernização de toda a infraestrutura, adotar arquiteturas baseada em microsserviços, de forma a ser possível atualizar cada componente de maneira individual, investir em tecnologias baseadas em nuvem, de modo a reduzir a dependência de infraestruturas físicas e haver um desenvolvimento contínuo para garantir que os sistemas estão sempre atualizados.

Realização de testes de intrusão (*pentesting*)

Embora não exista obrigação legal no setor da saúde de realizar testes de intrusão, importa voltar a frisar que este setor é um dos que mais sofre ciberataques no contexto dos OSE e que esses ciberataques são sobretudo ataques de *ransomware* e ataques relativos a dados. Tendo em conta estes factos, bem como a baixa realização de *pentesting* no setor (35%), considera-se pertinente a realização deste tipo de testes de forma a permitir a identificação de vulnerabilidades, a correção destas e a melhoria da resiliência em cibersegurança das organizações do setor a diversos ciberataques.

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

- **Controlos básicos**: controlos utilizados para a gestão de privilégios de administrador, gestores de vulnerabilidades ou de *hardware/software*;
- **Controlos fundacionais**: controlos de configurações de segurança de rede como *firewalls*, *routers* e *switches*, proteção contra *malware* e *browsers*;
- **Controlos organizacionais**: controlos de implementação de treinos de segurança, gestão e respostas a incidentes, testes de penetração e exercícios de *Red Team*[183].

No setor da saúde, os controlos fundacionais relacionados com a segurança de rede são particularmente críticos. Infraestruturas de saúde, como sistemas de gestão hospitalar, plataformas de telemedicina e redes que suportam a troca de dados de pacientes, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, a disponibilidade e a continuidade dos seus serviços. Falhas ou configurações incorretas nesses sistemas podem ser exploradas para interromper o acesso a dados vitais dos pacientes, comprometer a privacidade de informações sensíveis, ou até mesmo afetar a operação de dispositivos médicos conectados, colocando em risco a segurança dos pacientes e a eficácia do atendimento.

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

A tabela seguinte inclui a listagem completa dos controlos identificados pelo *CIS*, assim como a respetiva categoria dos mesmos[184]:

Tabela 5 - Controlos de Segurança da CIS

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

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

184 "The 18 CIS Critical Security Controls".

Notas metodológicas

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

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

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

Bibliografia

- Abreu, Laurinda. “Pensar historicamente os cuidados de saúde em Portugal”. *O Referencial: Revista da Associação 25 de Abril*. https://dspace.uevora.pt/rdpc/bitstream/10174/24717/1/REFERENCIAL%20130_bx_12_17.pdf .
- Agência para a Modernização Administrativa (AMA). “Cibersegurança na Administração Pública: O Imperativo da Conformidade Global no SNS”, *Encontros SAMA 2020* (Lisboa), 26 de abril de 2020. https://bo.tic.gov.pt/api/assets/etic/2e7a0cf7-68f5-4008-a95f-29594569d584/.
- Alder, Steve “Editorial: Why Do Criminals Target Medical Records”. *The HIPAA Journal*, 2 de novembro de 2023. https://www.hipaajournal.com/why-do-criminals-target-medical-records/
- 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.
- Asimily. “What are MDS2s and Why Should You Care”. https://asimily.com/blog/what-are-mds2s-and-why-should-you-care.
- BBVA. “História da Segurança Social (parte I)”, 20 de novembro de 2013. https://www.aminhapensao.pt/blog/historia-da-seguranca-social-parte-i/.
- Biscaia, André, António Pereira, Ana Alves, Rui Cardeira, Leonor Xavier da Rocha e Gonçalo Melo. “Síntese dos resultados do estudo ‘O Momento Atual da Reforma dos Cuidados de Saúde Primários em Portugal 2022/2023: Questionário aos coordenadores de USF’”. *Associação Nacional das Unidades de Saúde Familiar*. https://usf-an.pt/sintese-dos-resultados-do-estudo-o-momento-atual-da-reforma-dos-cuidados-de-saude-primarios-em-portugal-2022-2023-questionario-aos-coordenadores-de-usf/.
- Björnberg, Arne e Ann Phang. “Euro Health Consumer Index 2018”. *Health Consumer Powerhouse*, 2019. https://healthpowerhouse.com/media/EHCI-2018/EHCI-2018-report.pdf
- Borys, Christian. “The day a mysterious cyber-attack crippled Ukraine”, *BBC*, 4 de julho de 2017. https://www.bbc.com/future/article/20170704-the-day-a-mysterious-cyber-attack-crippled-ukraine.
- Caires, Marta. “Serviço de Saúde da Madeira: ataque informático deixa utentes sem consultas e sem exames”. *Expresso*, 7 de agosto de 2023. https://expresso.pt/sociedade/2023-08-07-Servico-de-Saude-da-Madeira-ataque-informatico-deixa-utentes-sem-consultas-e-sem-exames-e0cee143
- Centers for Medicare & Medicaid Services. “HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules”, fevereiro de 2023. https://www.cms.gov/outreach-and-education/medicare-learning-network-mln/mlnproducts/downloads/hipaaprivacyandsecurity.pdf.

- Checkpoint. "Cyberattacks on the Healthcare Sector", 2023. https://www.checkpoint.com/pt/cyber-hub/cyber-security/what-is-healthcare-cyber-security/cyberattacks-on-the-healthcare-sector/.
- Checkpoint."Cyber Attack Trends: 2020 Mid-Year Report", 22 de julho de 2020. https://research.checkpoint.com/2020/cyber-attack-trends-2020-mid-year-report/ .
- CIP. "Empresas privadas do setor da saúde com valor acrescentado acima de 6,7 mil milhões", 20 de outubro de 2023. https://cip.org.pt/empresas-privadas-do-setor-da-saude-com-valor-acrescentado-acima-de-67-mil-milhoes/.
- CNCS, "Compromisso C-Academy". https://www.cncs.gov.pt/pt/c-academy-compromisso/.
- CNCS, "Estratégia Nacional de Segurança do Ciberespaço 2019-2023". https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.
- CNCS, "Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança", dezembro de 2022. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.
- CNCS, ISAC. https://www.cncs.gov.pt/pt/isac/.
- CNCS. "Boletim do Observatório de cibersegurança n.º 4/2021", setembro de 2021. https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf .
- CNCS. "Incidentes e Setores: 2019-2023". Conhecimento Situacional: Estatísticas, última atualização a 21 de agosto de 2024. https://www.cncs.gov.pt/pt/estatistica/.
- CNCS. "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021". https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancacncs.pdf.
- CNCS. "Relatório Cibersegurança em Portugal: Riscos & Conflitos 2023". https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf.
- CNCS. "Relatório Cibersegurança em Portugal: Riscos e Conflitos 2024". https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs.pdf.
- CNCS. "Relatórios", Conhecimento Situacional: Observatório de Cibersegurança. https://www.cncs.gov.pt/pt/observatorio/#relatorios.
- Comissão Europeia. "€1.3 billion from the Digital Europe Programme for Europe's digital transition and cybersecurity". https://digital-strategy.ec.europa.eu/en/news/eu13-billion-digital-europe-programme-europes-digital-transition-and-cybersecurity.
- Conselho das Finanças Públicas, "Evolução do Desempenho do Serviço Nacional de Saúde em 2022 (Relatório n.º 7/2023)", junho de 2023. https://www.cfp.pt/uploads/publicacoes_ficheiros/cfp-rel-07-2023.pdf.
- Conselho Europeu, "Horizonte Europa". https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Constituição da República Portuguesa. https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx
- Decreto-Lei n.º 145/2009, de 17 de junho. *Diário da República*. https://diariodarepublica.pt/dr/detalhe/decreto-lei/145-2009-494558.
- 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
- Despacho n.º 8877/2017, de 9 de outubro. *Diário da República*. https://diariodarepublica.pt/dr/detalhe/despacho/8877-2017-108269312 .
- DICOM. "Digital Imaging and Communications in Medicine (DICOM)", maio de 2017. https://www.researchgate.net/publication/355550688_Digital_Imaging_and_Communications_in_Medicine_DICOM.
- 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
- DSI. "RNU - Registo Nacional de Utentes: Especificação Técnica", SPMS, 12 de novembro de 2015. SC_InfoSite_2015 (min-saude.pt).
- Empowering EU ISACs, "European ISACs". https://www.isacs.eu/european-isacs.
- ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU". https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.
- ENISA, "NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist", 11 de dezembro de 2020, https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
- ENISA. "ENISA Threat Landscape: Health Sector", 5 de julho de 2023. https://www.enisa.europa.eu/publications/health-threat-landscape.
- 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.
- ETSI. "Analysis of user service models, technologies and applications supporting eHealth", fevereiro de 2009. https://www.etsi.org/deliver/etsi_tr/102700_102799/102764/01.01.01_60/tr_102764v010101p.pdf.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), "Impact". https://www.ee-isac.eu/impact/#.
- *Eurostat*. "Physicians and physiotherapists in the EU: how many?", 18 de agosto de 2023. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20230818-1.
- Ferreira, Ana, William Melo, Rita Costa, Sabrina Pereira e Nuno Duarte. "Os Profissionais do SNS: Retrato e Evolução". *PLANAAP*: *Coleção Profissionais da Saúde* - n.º 2, março de 2024. https://www.planapp.gov.pt/wp-content/uploads/2024/03/PlanAPP_ProfissionaisSNS-2.pdf.
- ForeNova, "Cyber Threat Analysis Done the Right Way". https://www.forenova.com/threat-detection/how-to-conduct-a-cyber-threat-analysis.
- Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", janeiro de 2024.
- Google. "What is a Data Lake?", Google Cloud. https://cloud.google.com/learn/what-is-a-data-lake.
- Health Cluster Portugal. "Saúde fecha o ano de 2023 a ultrapassar a meta dos 3 mil milhões", 27 de fevereiro de 2024. https://www.healthclusterportugal.pt/pt/noticias/exportacoes-em-saude-2023/.
- IEFP, Cheque-Formação + Digital. https://www.iefp.pt/cheque-formacao-digital.
- INE, "Inquérito à Utilização das TIC nas Empresas", 2022. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y.
- INE. "Em 2022, a despesa corrente em saúde aumentou a um ritmo inferior ao do PIB". Informação à Comunicação Social, 4 de julho de 2023. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_destaques&DESTAQUESdest_boui=594883237&DESTAQUESmodo=2.

- INE. "Estatísticas da Saúde - 2022", edição de 2024. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=660521049&att_display=n&att_download=y.
- INE. "Estatísticas da saúde 2021", edição de 2023. https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_publicacoes&PUBLICACOESpub_boui=11677508&PUBLICACOESmodo=2
- INE. "Estatísticas Demográficas 2022", 16 de novembro de 2023. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=637367953&att_display=n&att_download=y#.
- INFARMED. "Dispositivos Médicos", Perguntas Frequentes. https://www.infarmed.pt/web/infarmed/perguntas-frequentes-area-transversal/novo-sistema-de-informacao-para-dispositivos-medicos-sidm.
- INFARMED. "Pesquisa de Dispositivos Médicos". https://www.infarmed.pt/web/infarmed/pesquisa-dispositivos#.
- INFARMED. "Sistema de Informação para Dispositivos Médicos (SIDM)". https://www.infarmed.pt/web/infarmed/infarmed?p_p_id=101&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&_101_struts_action=%2Fasset_publisher%2Fview_content&_101_assetEntryId=4088116&_101_type=content&_101_urlTitle=sistema-de-informacao-para-dispositivos-medicos-sidm-&inheritRedirect=false.
- Institute of Medicine Committee on Health Research and the Privacy of Health Information. "The Value and Importance of Health Information Privacy", em *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, editado por Sharyl Nass, Laura Levit e Lawrence Gostin. Washington DC: National Academies Press, 2009. https://www.ncbi.nlm.nih.gov/books/NBK9579/.
- International Citizens Insurance. "The Best Healthcare in the World: Country Rankings", 2024. https://www.internationalinsurance.com/health/systems/.
- ISO, "ISO/IEC 27001:2022". https://www.iso.org/standard/27001.
- ISO. "Application of risk management for IT-networks incorporating medical devices", outubro de 2010. https://www.iso.org/standard/44863.html.
- ISO. "Health informatics — Application of privacy management to personal health information". https://www.iso.org/standard/73697.html.
- ISO. "Health informatics — Cloud computing considerations for the security and privacy of health information systems", 2021. https://www.iso.org/standard/70568.html.
- ISO. "Health informatics — Guidance on the identification and authentication of connectable Personal Healthcare Devices (PHDs)", 2020. https://www.iso.org/standard/73696.html.
- ISO. "Health informatics — Information security management in health using ISO/IEC 27002", julho de 2008. https://www.iso.org/standard/41298.html.
- ISO. "Health informatics — Telehealth services — Quality planning guidelines", 2021. https://www.iso.org/standard/75962.html.
- ISO. "Medical devices — Quality management systems — Requirements for regulatory purpOSE", julho de 2003. https://www.iso.org/standard/36786.html.
- Lei n.º 35/2018, de 20 de julho, *Procuradoria-Geral Distrital de Lisboa*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2920&tabela=leis&so_miolo=.
- Lei n.º 46/2018, de 13 de agosto, *Diário da República*. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- McGoogan, Cara. "London HIV clinic accidentally leaks data of 780 patients". *Wired*, 2 de setembro de 2015. https://www.wired.com/story/56-dean-street-hiv-leak/.
- MedTech Dive. "'Hospitals' IoMT Device Security Risk Quantified in New Report", 23 de agosto de 2023. https://www.medtechdive.com/press-release/20230823-hospitals-iomt-device-security-risk-quantified-in-new-report/.

- Mee, Paul e Rico Brandenburg. “After reading, writing and arithmetic, the 4th 'r' of literacy is cyber-risk”. *World Economic Forum*, 17 de dezembro de 2020. https://www.weforum.org/agenda/2020/12/cyber-risk-cyber-security-education/.
- Mendonça, Cátia e Rita Costa, “40 anos do SNS. O que mudou?”, *Público*, 14 de setembro de 2019. https://www.publico.pt/2019/09/14/infografia/40-anos-sns-mudou-340.
- Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- Ministério das Finanças. “Orçamento do Estado 2024: Relatório - versão consolidada de 16 de outubro de 2023”. https://www.dgo.gov.pt/politicaorcamental/OrcamentodeEstado/2024/Proposta%20do%20Or%C3%A7amento/Documentos%20do%20OE/OE2024_doc16_Relatorio.pdf.
- MITRE. “Next Steps Toward Managing Legacy Medical Device Cybersecurity Risks”, 15 de novembro de 2023. https://www.mitre.org/news-insights/publication/next-steps-toward-managing-legacy-medical-device-cybersecurity-risks.
- Nicolau, Teresa. “Da democracia nasceu o Serviço Nacional de Saúde”. *RTP Ensina*, 2014. https://ensina.rtp.pt/artigo/da-democracia-nasceu-o-servico-nacional-de-saude/.
- NIST. “Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule: A Cybersecurity Resource Guide”, fevereiro de 2024. https://csrc.nist.gov/pubs/sp/800/66/r2/final.
- Oliveira, Daniela. “Desenvolvimento de um Sistema Eletrónico de Vigilância Epidemiológica (eVDmed): recolha, análise e publicação de informação”. Dissertação de mestrado, Universidade do Minho, 2017. https://repositorium.sdum.uminho.pt/bitstream/1822/49627/1/Daniela%20Pimentel%20de%20Oliveira.pdf.
- Pallardy, Richard. “The Unique Cyber Vulnerabilities of Medical Devices”. *Information Week*, 14 de novembro de 2023. https://www.informationweek.com/cyber-resilience/the-unique-cyber-vulnerabilities-of-medical-devices#close-modal
- PORDATA, “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- PORDATA. “Produto Interno Bruto (PIB): Quanta riqueza é criada em Portugal”, Estatísticas. https://www.pordata.pt/pt/estatisticas/economia/crescimento-e-produtividade/produto-interno-bruto-pib.
- PplWare. “O maior banco do mundo sofreu ataque de ransomware e salvou-se graças a uma… pen USB”, 12 de novembro de 2023. https://pplware.sapo.pt/internet/o-maior-banco-do-mundo-sofreu-ataque-de-ransomware-e-salvou-se-gracas-a-uma-pen-usb/.
- 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/.
- Recuperar Portugal. “Monitorização”. https://recuperarportugal.gov.pt/monitorizacao/.
- Regulamento (UE) 2017/745 do Parlamento Europeu e do Conselho, de 5 de abril de 2017, relativo aos dispositivos médicos, que altera a Diretiva 2001/83/CE, o Regulamento (CE) n.° 178/2002 e o Regulamento (CE) n.° 1223/2009 e que revoga as Diretivas 90/385/CEE e 93/42/CEE do Conselho. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32017R0745.
- Seacord, Robert, Daniel Plakosh e Grace Lewis. *Modernizing Legacy Systems: Software Technologies, Engineering Processes, and Business Practices.* Boston: Addison-Wesley, 2003.
- Séneca, Hugo. “Hackers publicam passwords de milhares de médicos e enfermeiros do SNS na internet”. *Expresso*, 20 de julho de 2020. https://expresso.pt/sociedade/2020-07-20-Hackers-publicam-passwords-de-milhares-de-medicos-e-enfermeiros-do-SNS-na-internet.
- Simão, Mafalda. “A Prestação de Cuidados de Saúde em Função do Território”. Publicado no Repositório Científico da Universidade de Coimbra, 2022. https://estudogeral.uc.pt/handle/10316/102463.

- SNS. “História do SNS”. https://www.sns.gov.pt/sns/servico-nacional-de-saude/historia-do-sns/.
- SPMS. “Alertas e Segurança”. https://www.spms.min-saude.pt/alertaseseguranca/.
- SPMS. “BI CSP – Bilhete de Identidade dos Cuidados de Saúde Primários”. https://www.spms.min-saude.pt/2020/07/bi-csp-bilhete-de-identidade-dos-cuidados-de-saude-primarios/.
- SPMS. “Cibersegurança”, abril de 2019. https://www.spms.min-saude.pt/2019/04/ciberseguranca-2/.
- SPMS. “Circular Normativa n.º 03/2017: medidas excecionais de segurança”, 19 de maio de 2017. https://spms.min-saude.pt/wp-content/uploads/2017/05/Circular-Normativa-n%C2%BA3-Medidas-Excecionais-de-Ciberseguran%C3%A7a.pdf.
- SPMS. “Conteúdos de Sensibilização de Cibersegurança”, Academia SPMS. https://academia.spms.min-saude.pt/atis-de-sensibilizacao-de-ciberseguranca/.
- SPMS. “Exames Sem Papel”, julho de 2020. https://www.spms.min-saude.pt/2020/07/exames-sem-papel/.
- SPMS. “FAQs PEM - Receita sem papel”, novembro de 2015. https://spms.min-saude.pt/wp-content/uploads/2015/11/FAQs1.pdf.
- SPMS. “PEM | Prescrição Eletrónica Médica”, julho de 2020. https://www.spms.min-saude.pt/2020/07/pem/.
- SPMS. “Plano de Atividades e Orçamento 2022”, 76, setembro de 2021. https://www.spms.min-saude.pt/wp-content/uploads/2022/09/Plano-de-Atividades-e-Orcamento-2022_Assinado_09092022.pdf.
- SPMS. “Prescrição Eletrónica Médica: Especificação dos Serviços para integração com o Sistema Central de Prescrições”, janeiro de 2018. SPMS (min-saude.pt).
- SPMS. “Receita Sem Papel”, abril de 2019. https://www.spms.min-saude.pt/2019/04/receita-sem-papel-2/.
- SPMS. “RNU: Registo Nacional de Utentes”, outubro de 2015. https://www.spms.min-saude.pt/2015/10/rnu/.
- SPMS. “SClínico | Cuidados de Saúde Hospitalares (CSH)”, julho de 2020. https://www.spms.min-saude.pt/2020/07/sclinico-hospitalar/.
- SPMS. “SClínico | Cuidados de Saúde Primários (CSP)”, julho de 2020. https://www.spms.min-saude.pt/2020/07/sclinico-cuidados-de-saude-primarios-csp/.
- SPMS. “SINAVE | Sistema Nacional de Vigilância Epidemiológica”. https://www.spms.min-saude.pt/2020/07/sinave-2/.
- SPMS. “Sistema Central de Prescrições”, janeiro de 2018. https://spms.min-saude.pt/wp-content/uploads/2018/10/PEM_ServicosPrescri%C3%A7%C3%A3o_ET-2.5.pdf.
- Sulaiman Asif, “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, *Knowledge Hut*, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- Turhune, Chad. “UCLA Health System data breach affects 4.5 million patients”, *Los Angeles Times*, 17 de julho de 2015. https://www.latimes.com/business/la-fi-ucla-medical-data-20150717-story.html.
- United States Government Accountability Office. “Medical Device Cybersecurity: Agencies Need to Update Agreement to Ensure Effective Coordination”. Report to Congressional Committees, dezembro de 2023. https://www.gao.gov/assets/d24106683.pdf.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.
- *World Population Review* .“Euro Health Consumer Index by Country 2024”. https://worldpopulationreview.com/country-rankings/euro-health-consumer-index-by-country.

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