CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de **Cibersegurança**

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

Bancário

Caracterização, Regulamentação e Recomendações no Âmbito do Observatório de Cibersegurança

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

Índice

Introdução 11
Contexto do relatório 13
Objetivos do relatório 14
Contexto Geral 15
Análise do questionário dirigido aos Reguladores de Serviços Essenciais 18
Resultados do questionário dirigido aos Operadores de Serviços Essenciais 40
Análise Setorial 106
1. Bancário 106
1.1. Contextualização setorial 106
1.2. Ameaças 116
1.3. Capacitação 121
1.4. Investimento em cibersegurança 123
1.5. RJSC e legislação setorial 127
1.6. Standards e boas práticas aplicáveis 131
1.7. Desafios 135
1.8. Recomendações 137
Notas metodológicas 147
Bibliografia 148

Índice de Gráficos

Gráfico 1 - Reguladores que já comunicaram com os OSE sobre questões de cibersegurança.19

Gráfico 2 - Origem da comunicação sobre questões de cibersegurança.....19

Gráfico 3 - Formalidade da comunicação realizada.....20

Gráfico 4 - Frequência da comunicação.....21

Gráfico 5 - Impacto sentido na sua organização e nos OSE regulados.....21

Gráfico 6 - Dificuldades sentidas relativamente à conformidade com a Diretiva NIS / Lei n.º 46/2018 22

Gráfico 7 - Perceção sobre a capacidade para fazer a supervisão dos OSE em matéria de cibersegurança, em caso de atribuição da competência 23

Gráfico 8 - Recursos em falta para a capacidade de supervisão em matéria de cibersegurança23

Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores 24

Gráfico 10 - Medidas adotadas pelas entidades reguladoras para promover a maturidade em cibersegurança.....25

Gráfico 11 - Perceção sobre o número de profissionais capacitados em matéria de cibersegurança na entidade reguladora 25

Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados 26

Gráfico 13 - Perceção dos reguladores sobre o nível de cibersegurança estabelecido pela Diretiva NIS 1 / lei n.º 46/2018, de 13 de agosto, face aos desafios, perigos e ameaças existentes 26

Gráfico 14 - Reguladores que se encontram a fazer categorização de ameaças de cibersegurança 27

Gráfico 15 - Reguladores que partilham a informação relativa à categorização de ameaças de cibersegurança com os OSE, de entre os que realizam essa categorização.....28

Gráfico 16 - Reguladores que orientam os OSE na digitalização de processos e na promoção de uma cultura digital.....28

Gráfico 17 - Perceção sobre a necessidade de apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança nos setores regulados 29

Gráfico 18 - Tipos de apoio pretendidos pelos reguladores que consideram necessário apoio adicional por parte do CNCS.....30

Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS.....31

Gráfico 20: Áreas através das quais o CNCS poderia prestar mais auxílio 32

Gráfico 21 - Standards e boas práticas recomendados aos OSE pelos reguladores.....33

Gráfico 22 - Percentagem aproximada de OSE nos setores certificados em normas internacionais (como ISO/IEC 27001 ou ISO 22301) do conhecimento do regulador....34

Gráfico 23 - Reguladores com equipa de resposta a incidentes definida....35

Gráfico 24 - Reguladores que estão ou já estiveram em programas de formação e sensibilização para os riscos no ciberespaço promovidos pelo CNCS ou por outra entidade 35

Gráfico 25 - Reguladores recipientes de formação que partilharam os conhecimentos adquiridos com os OSE do setor....36

Gráfico 26 - Reguladores que frequentaram programas, e consideram que ter frequentado o programa robusteceu comportamentos relativos à cibersegurança dentro da organização....36

Gráfico 27 - Reguladores que, no âmbito dos programas, sentiram que a entidade formadora os sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto 37

Gráfico 28 - Reguladores pertencentes a estruturas de cooperação nacional/internacional de proteção do ciberespaço (ISACs - Centros de Análise e Partilha de Informação) 38

Gráfico 29: Reguladores que recomendam a participação dos OSE em centros de partilha de informação como os ISACs....38

Gráfico 30 - Número de colaboradores na organização 40

Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores....41

Gráfico 32 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança....42

Gráfico 33 - Percentagem aproximada de trabalhadores do operador com formação básica em cibersegurança....42

Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança....43

Gráfico 35 - Percentagem aproximada de trabalhadores do operador com certificações em cibersegurança....44

Gráfico 36 - Existência de equipa de profissionais dedicada a dar apoio aos colaboradores do operador (*helpdesk*), em matéria de cibersegurança e/ou tecnologias da informação....45

Gráfico 37 - Composição das equipas de helpdesk....46

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores 46

Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa 47

Gráfico 40 - Caráter das formações disponibilizadas - formação interna ou externa 48

Gráfico 41 - Frequência média dos momentos de formação 48

Gráfico 42 - Motivos para a não disponibilização de formação entre os OSE que não disponibilizam 49

Gráfico 43 - Existência de cursos de atualização (“refresher courses”) para os colaboradores ..49

Gráfico 44 - Perceção sobre a falta de profissionais em cibersegurança e áreas relacionadas..50

Gráfico 45 - Vagas abertas para a área de cibersegurança 51

Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança.....51

Gráfico 47 - Motivos para a não abertura de vagas entre os OSE sem vagas abertas para a área de cibersegurança.....52

Gráfico 48 - Percentagem aproximada de trabalhadores com acesso a equipamentos digitais na realização do seu trabalho 53

Gráfico 49 - Os OSE são responsáveis pelo funcionamento dos equipamentos necessários às funções dos colaboradores 54

Gráfico 50 - Percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções.....54

Gráfico 51 - Fornecimento de acesso remoto a sistemas (e-mail, aplicações ou documentos) dos OSE aos colaboradores 55

Gráfico 52 - Sistemas do OSE aos quais é dado acesso remoto aos colaboradores 56

Gráfico 53 - Boas práticas de segurança para acesso remoto aplicadas pelos OSE.....57

Gráfico 54 - OSE que utilizam *Customer Relationship Management Software* (CRM).....58

Gráfico 55 - OSE que utilizam CRM para captar, armazenar e disponibilizar informação de clientes a outras funções do negócio 59

Gráfico 56 - OSE que adquiriram serviços de Computação Cloud (CC).....59

Gráfico 57 - Finalidades dos serviços de Computação Cloud adquiridos 60

Gráfico 58 - Utilização de serviços de CC em conjunto com Internet of Things (IoT).....61

Gráfico 59 - Percentagem de sistemas core em *cloud* 62

Gráfico 60 - Percentagem de sistemas *core on-perm*.....62

Gráfico 61- Utilização de IoT pelos OSE 63

Gráfico 62 - Contextos de utilização de IoT.....64

Gráfico 63 - Motivos pelos quais não utilizam IoT 65

Gráfico 64 - OSE que utilizam processos que recorrem a IA.....66

Gráfico 65 - Funções para as quais utilizam IA 67

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança 69

Gráfico 67 - Divisão entre rede dos colaboradores e rede para *guests* 71

Gráfico 68 - OSE que já sofreram incidentes de segurança em contexto TIC 72

Gráfico 69 - Tipos de incidentes ocorridos 73

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS.....74

Gráfico 71 - Dificuldades no processo de notificação ao CNCS 75

Gráfico 72 - Dificuldades encontradas pelos OSE durante a notificação de incidentes ao CNCS75

Gráfico 73 - Importância da intervenção do CNCS na resolução do incidente 76
Gráfico 74 - Avaliação da resposta dada pelo CNCS 76
Gráfico 75 - Motivos para a não notificação de incidentes de cibersegurança ao CNCS 77
Gráfico 76 - Seguro contra incidentes de cibersegurança 77
Gráfico 77 - Documentação/implementação de políticas e procedimentos de cibersegurança ... 78
Gráfico 78 - Existência de Plano de Segurança que contemple a cibersegurança 79
Gráfico 79 - Políticas incluídas no Plano de Segurança 80
Gráfico 80 - Revisão do Plano de Segurança 81
Gráfico 81 - OSE que realizam procedimentos de deteção e gestão de vulnerabilidades 81
Gráfico 82 - OSE que dentro dos procedimentos de deteção e gestão de vulnerabilidades realizam análise de vulnerabilidades 82
Gráfico 83 - Frequência da análise de vulnerabilidades 82
Gráfico 84 - Realização de testes de intrusão 83
Gráfico 85 - Frequência de testes de intrusão 83
Gráfico 86 - Observação de requisitos mínimos e segurança por parte dos fornecedores em contexto de cadeia de abastecimento 84
Gráfico 87 - Outras entidades previstas para a notificação em caso de ciberataque/incidente, para além do CNCS 84
Gráfico 88 - Nomeação do contacto permanente que assegura os fluxos de informação de nível operacional e técnico com o CNCS 85
Gráfico 89 - Designação do contacto permanente 86
Gráfico 90 - Designação do responsável de segurança 86
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança 87
Gráfico 92 - Formação específica de cibersegurança do responsável de segurança 88
Gráfico 93 - Tipo de formação específica em cibersegurança 88
Gráfico 94 - Motivos pelos quais o responsável de segurança não tem formação específica em cibersegurança 89
Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado 90
Gráfico 96 - Submissão do inventário de ativos ao CNCS 90
Gráfico 97 - Elaboração do relatório anual previsto pelo decreto-lei n. º65/2021, de 30 de julho 91
Gráfico 98 - Submissão do relatório anual ao CNCS 91
Gráfico 99 - Realização de análise de riscos anual no âmbito de cibersegurança 92
Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança 92

Gráfico 101 - Definição de calendário para cumprimento das obrigações decorrentes do decreto-lei n.º 65/2021, de 30 de julho....93

Gráfico 102: Equipa de resposta a incidentes de cibersegurança....93

Gráfico 103 - Composição da equipa de resposta a incidentes de cibersegurança....94

Gráfico 104 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança....94

Gráfico 105 - Disponibilização aos colaboradores de canais rápidos para reporte de incidentes95

Gráfico 106 - Acessibilidade e distribuição por todos os colaboradores dos contactos a utilizar em caso de incidente de cibersegurança....95

Gráfico 107 - Realização de exercícios de resposta a ciberataques....96

Gráfico 108 - Hábitos de recolha de informações sobre boas práticas respeitantes a riscos e incidentes de cibersegurança....97

Gráfico 109 - Orçamento específico para a área de cibersegurança....99

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança....100

Gráfico 111 - Previsão de orçamentação entre OSE que não possuem orçamento específico para a área de cibersegurança....101

Gráfico 112 - Conhecimento de incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança....102

Gráfico 113 - Plano de Comunicação de Crises....103

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises....103

Gráfico 115 - Motivos para a não definição de Plano de Comunicação de Crises....105

Índice de Figuras

Figura 1 - Número de incidentes no setor Bancário anualmente 120

Figura 2 - Perda de controlo de informação no setor Bancário 136

Índice de Tabelas

Tabela 1 - Setores, Subsetores e Tipos de Entidades 16

Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança 34

Tabela 3 - Estimativa do total de entidades reguladas pelos reguladores por setor 39

Tabela 4 - Número estimado das entidades reguladas que são OSE 39

Tabela 5 - Agentes de ameaça mais prováveis (Bancário) 120

Tabela 6 - Capacitação no setor Bancário 121

Tabela 7 - Standards e Boas Práticas (Bancário) 131

Tabela 8 - Cenários de risco (Bancário) 141

Tabela 9 - Controlos de Segurança da CIS (Bancário) 146

Introdução

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

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

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

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

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

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

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

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

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

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

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

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

Contexto do relatório

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

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

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

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

Objetivos do relatório

Este relatório teve como principais objetivos:

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

O relatório elaborado atenderá aos seguintes pontos na análise setorial:

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

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

Contexto Geral

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

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

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

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

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

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

- A entidade presta um serviço essencial para a manutenção de atividades societais e/ou económicas cruciais;
- A prestação desse serviço depende de redes e sistemas de informação; e
- Um incidente pode ter efeitos perturbadores importantes na prestação desse serviço[6].
- Assim, segundo a Lei n.º 46/2018, foram explicitados os seguintes setores, subsetores e tipos de entidades:

Tabela 1 - Setores, Subsetores e Tipos de Entidades

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

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

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

Análise do questionário dirigido aos Reguladores de Serviços Essenciais

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

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

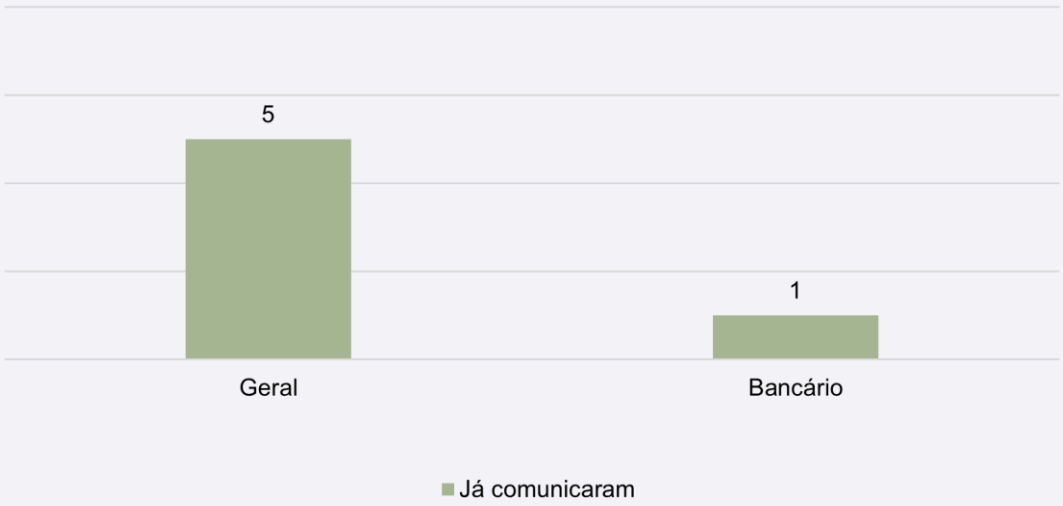
O questionário dirigido aos Reguladores é menos extenso e incide principalmente sobre as atividades de comunicação, regulação, regulamentação, supervisão e de acompanhamento feitas junto dos OSE em matéria de cibersegurança. O questionário dirigido aos Operadores de Serviços Essenciais, por sua vez,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

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

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

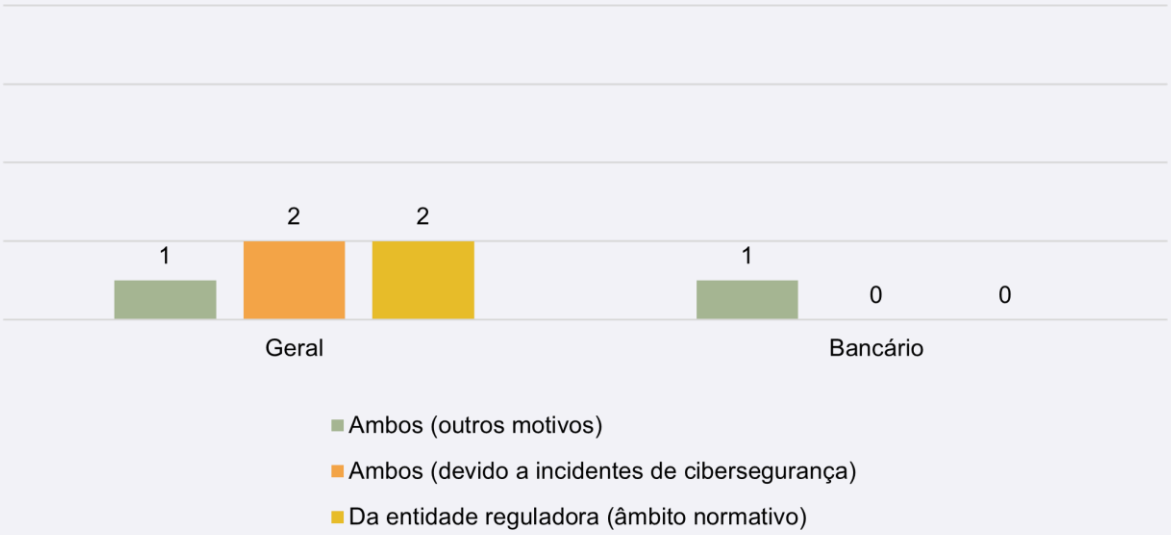
1. Comunicação entre OSE e respetivos Reguladores

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



Entre os oito reguladores que responderam, cinco indicaram já ter comunicado com os OSE sobre questões de cibersegurança. O regulador inquirido do setor bancário digitais indicou já ter realizado qualquer comunicação sobre estas matérias aos OSE por si regulados.

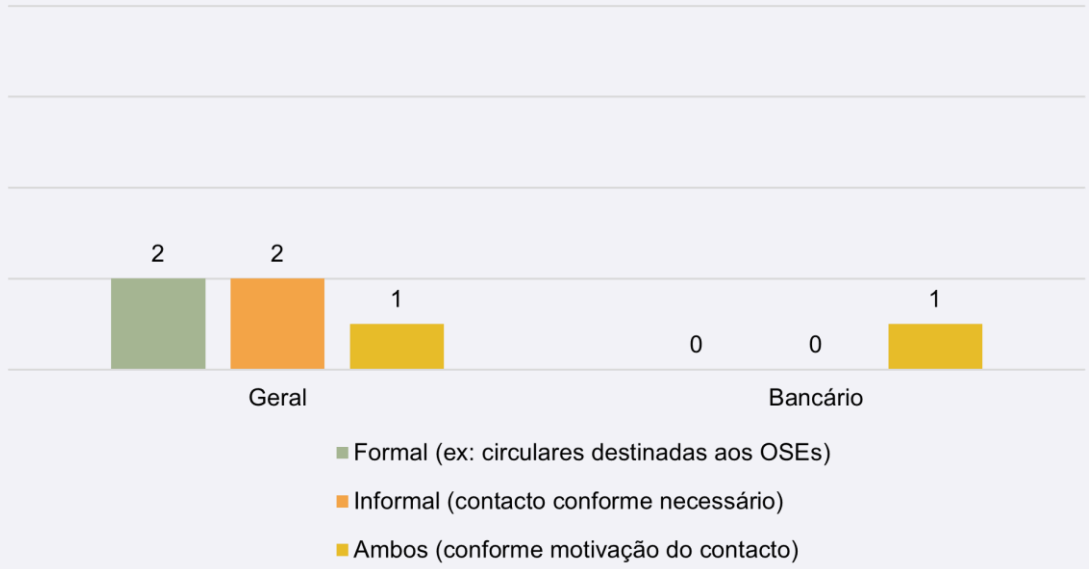
Gráfico 2 - Origem da comunicação sobre questões de cibersegurança



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

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

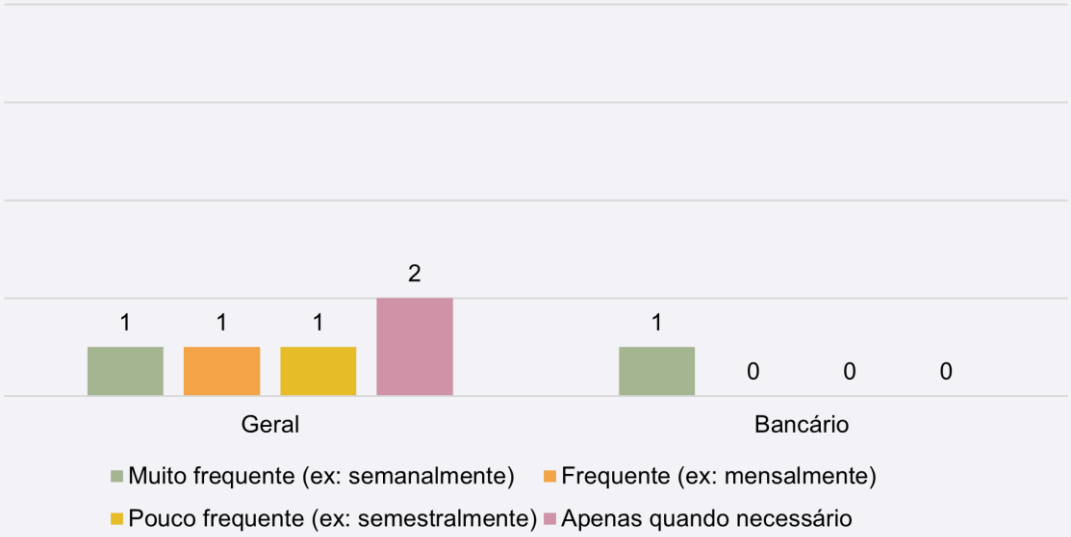
Gráfico 3 - Formalidade da comunicação realizada



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

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

Gráfico 4 - Frequência da comunicação



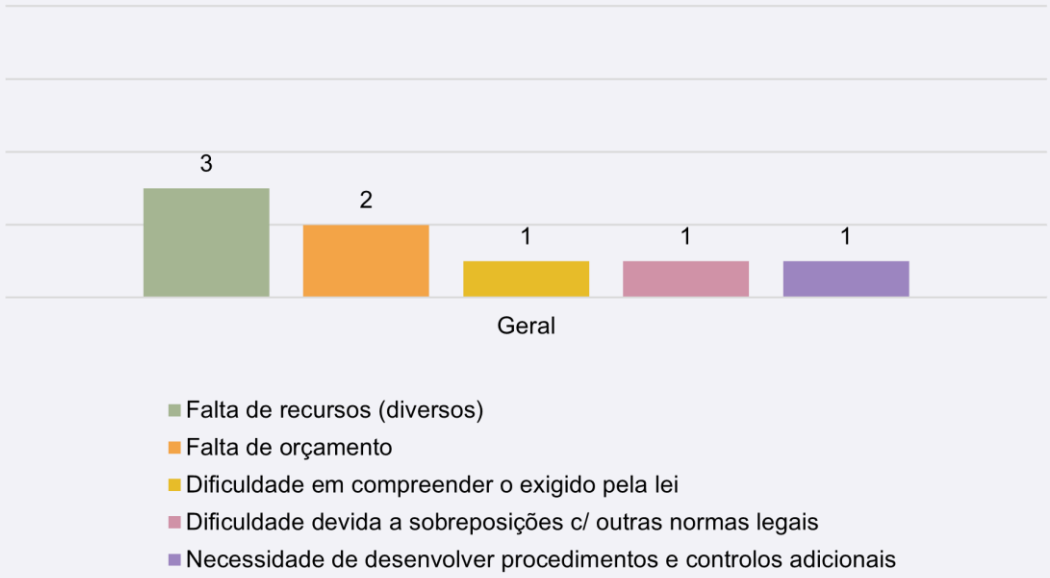
No que à frequência da comunicação sobre cibersegurança entre reguladores e operadores diz respeito, esta não é uniforme entre os vários setores. O regulador do setor bancário foi o único a indicar que a comunicação é realizada muito frequentemente, praticamente de forma semanal.

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

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

Questionou-se aos reguladores se sentiram impacto nas suas organizações e nos OSE por si regulados pela publicação da Diretiva NIS. Entre os oito reguladores que responderam, cinco indicaram ter sentido esse impacto. O setor bancário não mencionou ter sentido esse impacto.

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



Três dos cinco reguladores que indicaram ter sentido impacto na sua organização ou nos OSE por si regulados devido à publicação da Diretiva NIS afirmaram que uma das dificuldades encontradas foi a falta de recursos diversos para estar em conformidade com a mesma. Indicam também a falta de orçamento a conformidade com regime jurídico, como outra das dificuldades sentidas. Soma-se ainda a dificuldade em compreender o que era exigido pela nova legislação, tendo este sido o único setor a apontar esta dificuldade. Dificuldades relativas à sobreposição com outras normas legais foram indicadas apenas por um dos reguladores, já a necessidade de desenvolver procedimentos e controlos adicionais foi unicamente indicada por um regulador.

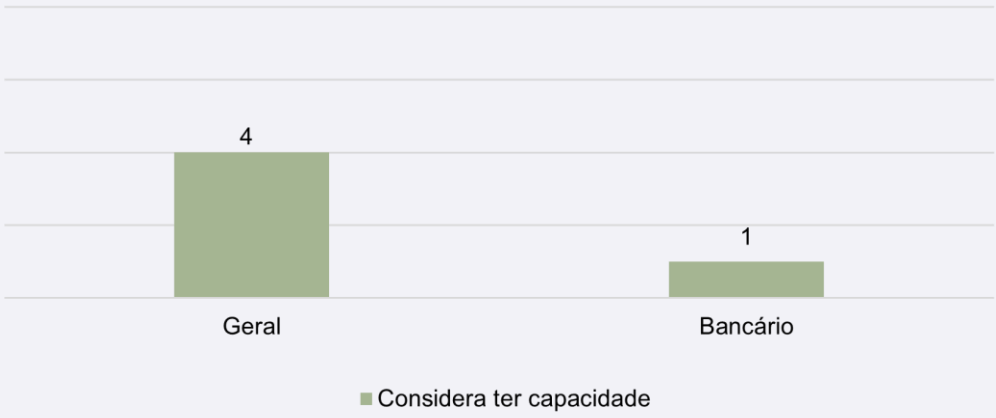
O setor bancário não é abordado pois nenhum inquirido mencionou dificuldades.

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

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

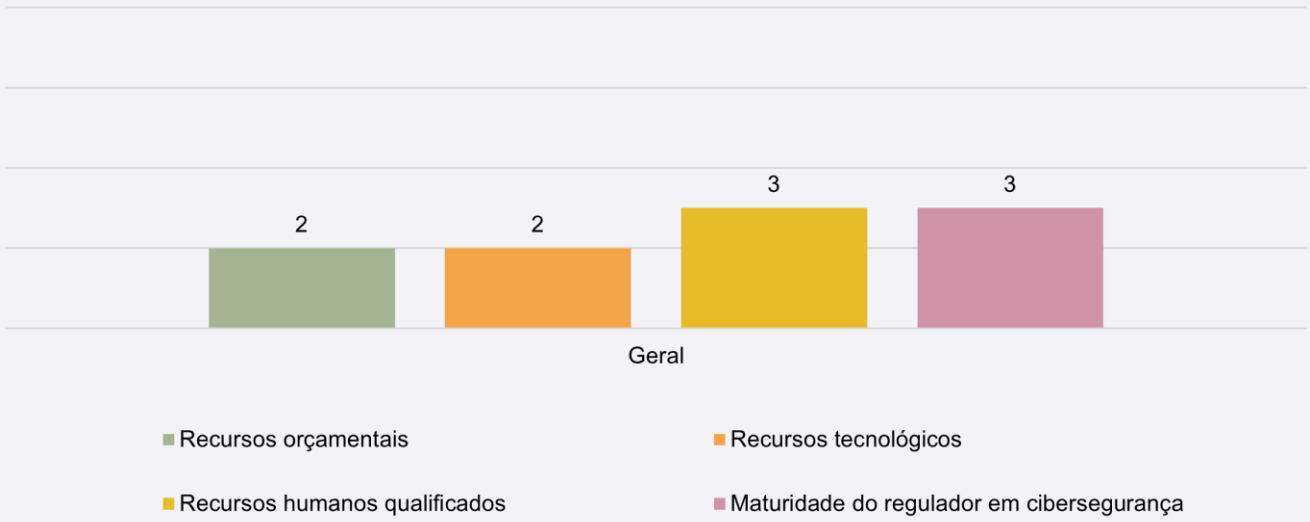
3. Supervisão dos OSE em matéria legislativa de cibersegurança por parte dos Reguladores

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



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

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

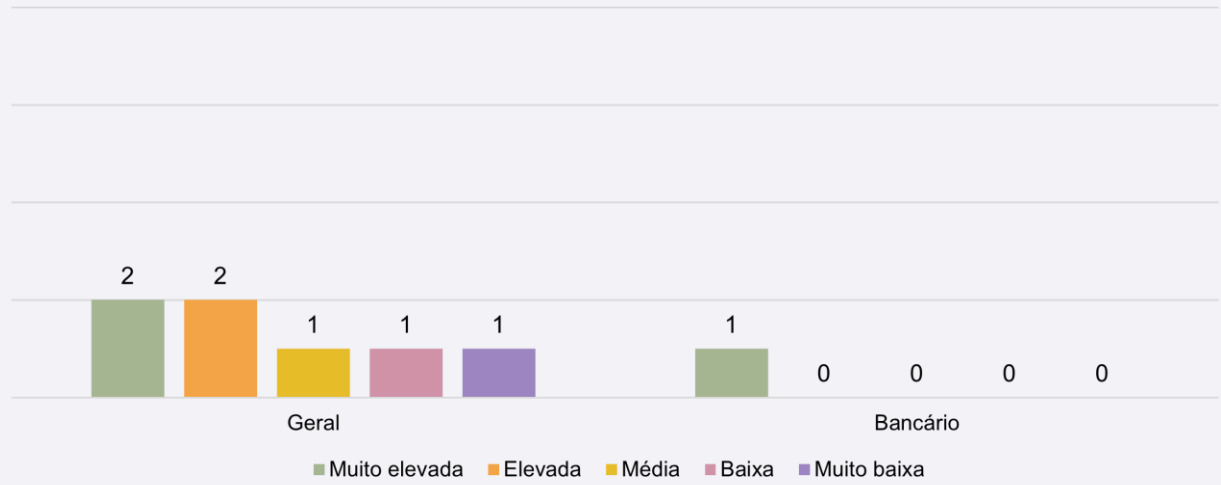


Entre os reguladores que consideram não ter essa capacidade, dois deles indicaram não ter suficientes recursos orçamentais, dois mencionaram suficientes recursos tecnológicos e três suficiente maturidade em cibersegurança. Além destes, três das entidades que consideram não ter a capacidade de realizar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

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

4. Maturidade em cibersegurança no setor

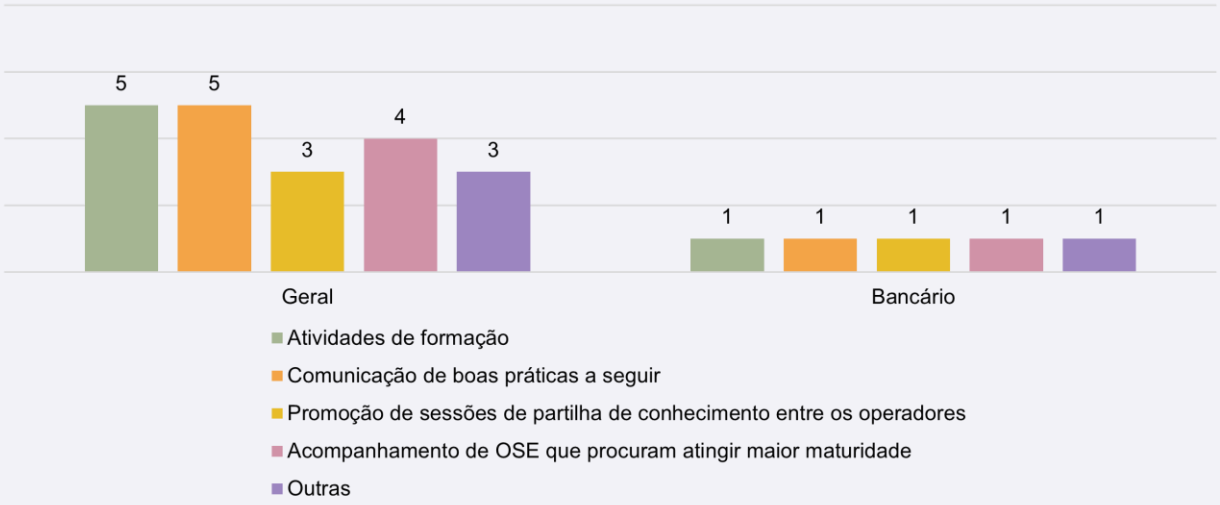
Gráfico 9 - Perceção dos reguladores sobre maturidade em cibersegurança nos setores



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

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

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



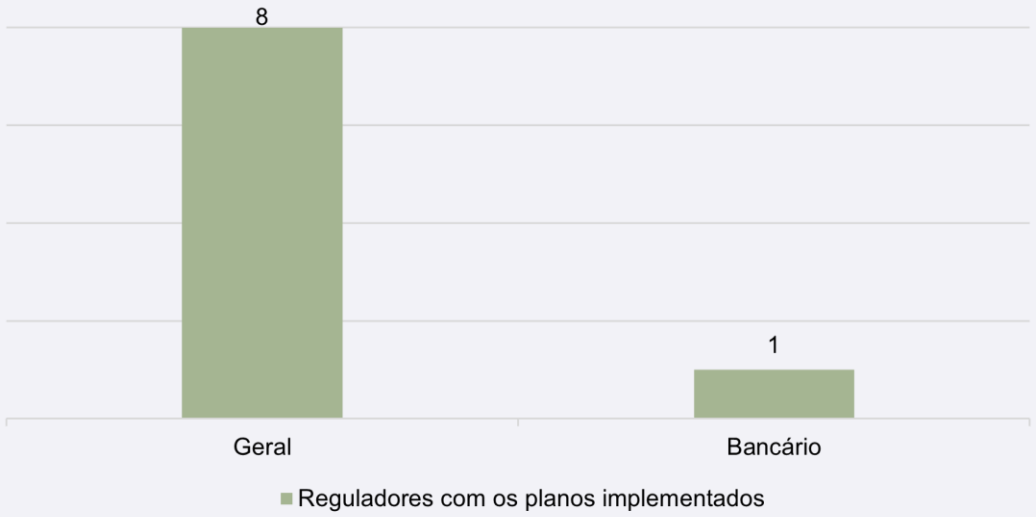
Os reguladores tentam promover a maturidade em cibersegurança nos seus respetivos setores através da adoção de diferentes medidas. Cinco dos reguladores inquiridos, promovem atividades de formação num esforço para aumentar a maturidade no setor. Verifica-se o mesmo número de reguladores a recomendar boas práticas a seguir. Relativamente à promoção de sessões de partilha de conhecimento, apenas três reguladores indicaram fazê-lo. Quanto ao acompanhamento de OSE que procurem atingir maior maturidade em cibersegurança, quatro entidades referiram fazer esse acompanhamento,

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

Apenas duas das entidades reguladoras inquiridas, sendo uma delas o regulador do setor bancário, consideram ter suficientes profissionais capacitados em matéria de cibersegurança, enquanto os restantes seis não consideram ter suficientes profissionais capacitados na área.

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

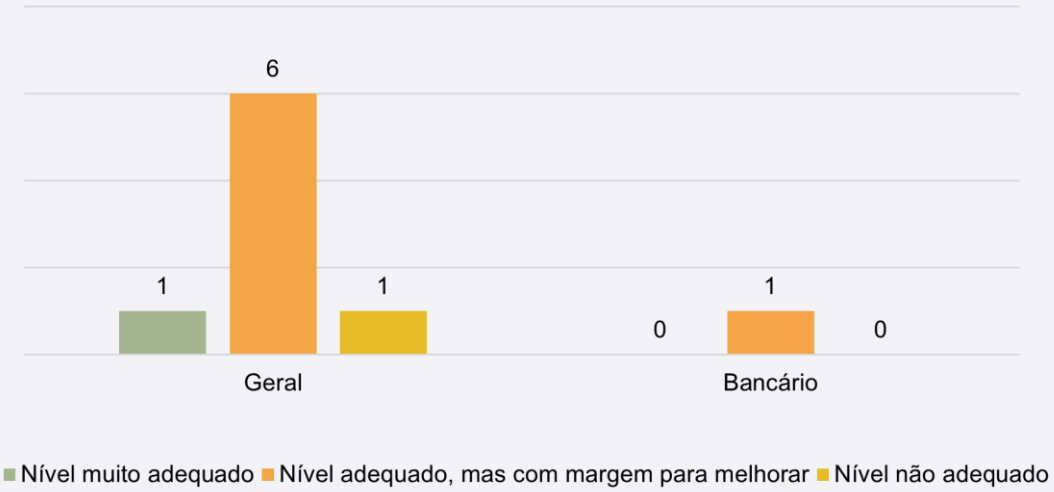
Gráfico 12 - Reguladores com os planos de segurança e de resposta a incidentes implementados



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

5. Nível de segurança estabelecido pela legislação em vigor

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



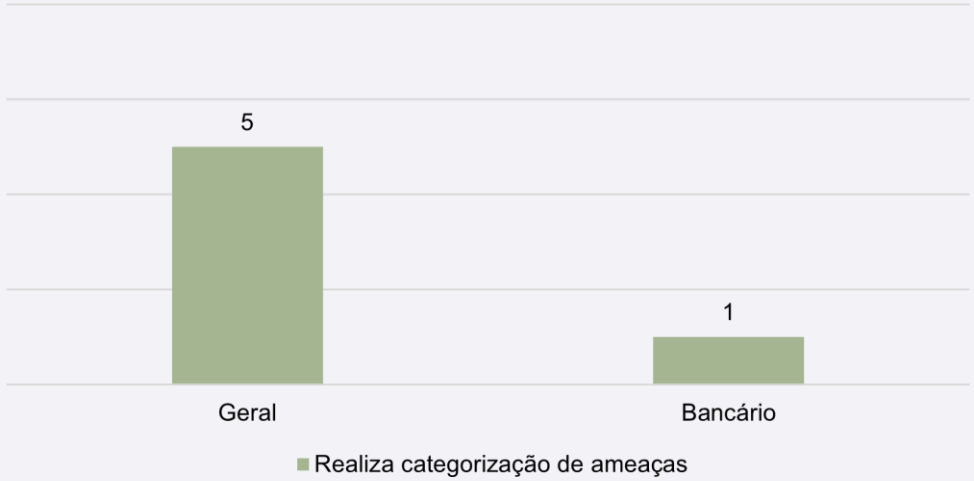
Na generalidade, a maioria dos reguladores dos OSE, nomeadamente seis, consideram que a Diretiva NIS procura estabelecer um nível adequado de cibersegurança entre os OSE, mas com margem para melhorar, face aos atuais desafios, perigos e ameaças nesta matéria. Apenas um regulador considera que o nível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

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

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

6. Categorização de ameaças

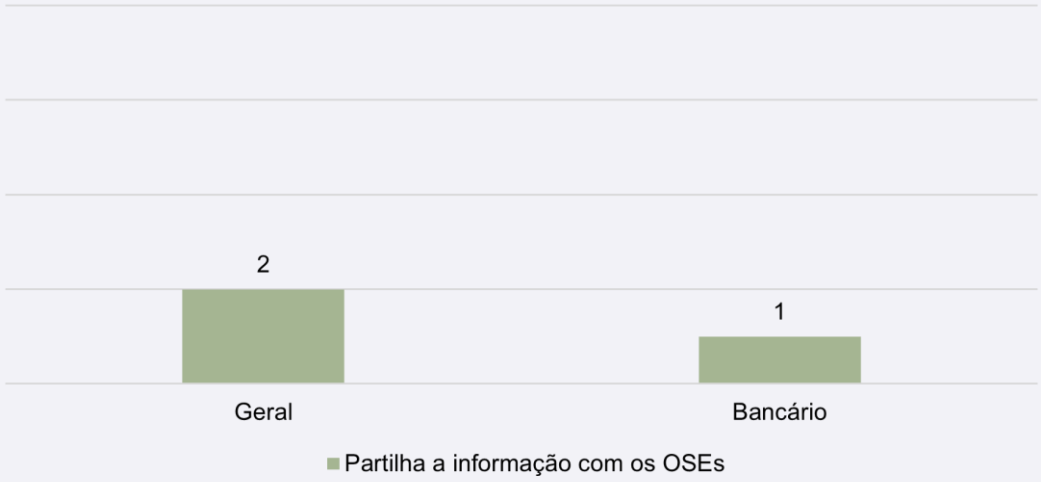
Gráfico 14 - Reguladores que se encontram a fazer categorização de ameaças de cibersegurança



Cinco dos oito reguladores, sendo novamente um deles o do setor bancário, realizam categorização de ameaças de cibersegurança, ficando de fora dois reguladores.

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

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



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

7. Orientação dos OSE por parte da entidade reguladora

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

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

8. Apoio por parte do CNCS

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

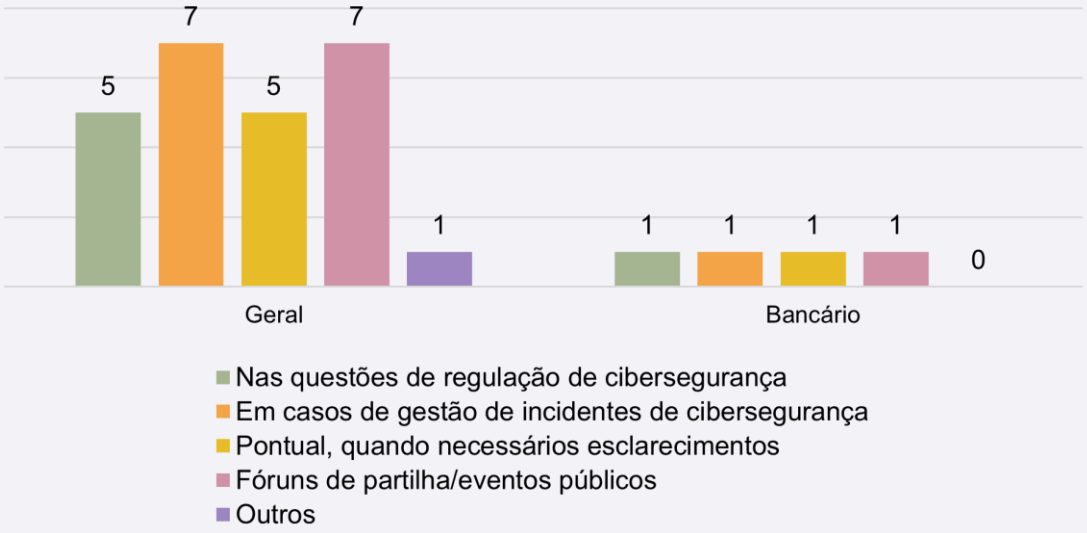
Entre os reguladores inquiridos, cinco têm a perceção de que é necessário apoio adicional por parte do CNCS para atingir maior maturidade em cibersegurança, enquanto os restantes três consideram que não é necessário apoio adicional, encontrando-se o regulador do setor bancário incluído nos restantes.

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

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

No setor bancário a questão não se aplica, pois, o setor mencionou não necessitar de apoio adicional.

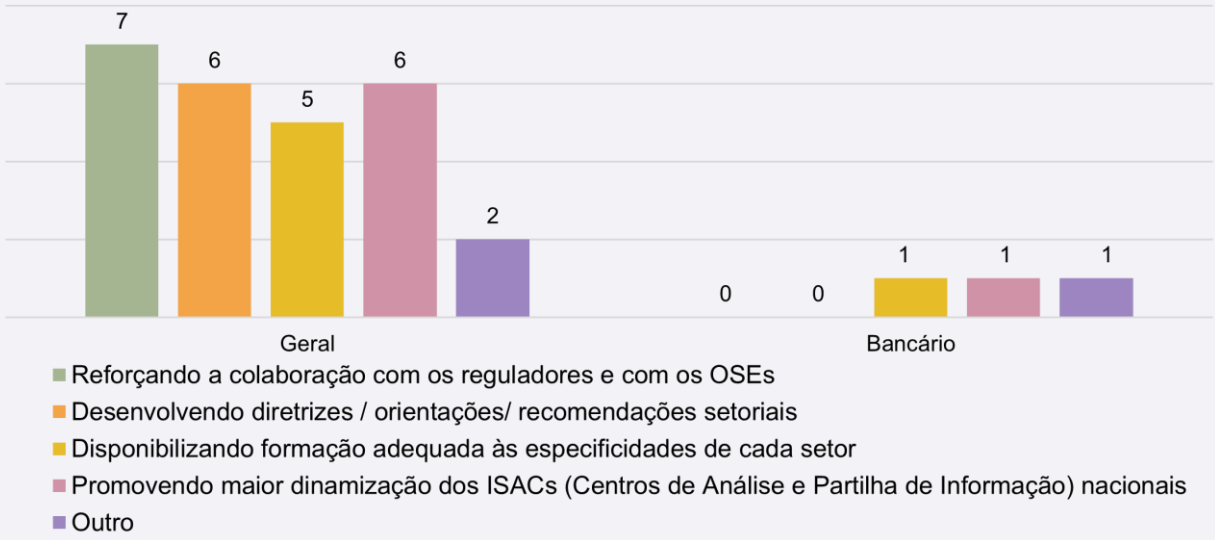
Gráfico 19 - Tipos de interação existentes entre reguladores e CNCS



Relativamente às interações entre os reguladores e o CNCS, sete dos reguladores interagem com o Centro no contexto de incidentes de cibersegurança ou em fóruns de partilha/eventos públicos. Já menos reguladores, cinco, interagem com o CNCS devido a questões relacionadas com regulação de cibersegurança ou de forma pontual quando necessita de esclarecimentos em matéria de cibersegurança. Apenas um refere interagir noutros contextos, como na definição de limiares de reporte incidentes.

No setor bancário interage com o CNCS em todas as situações referidas anteriormente.

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



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

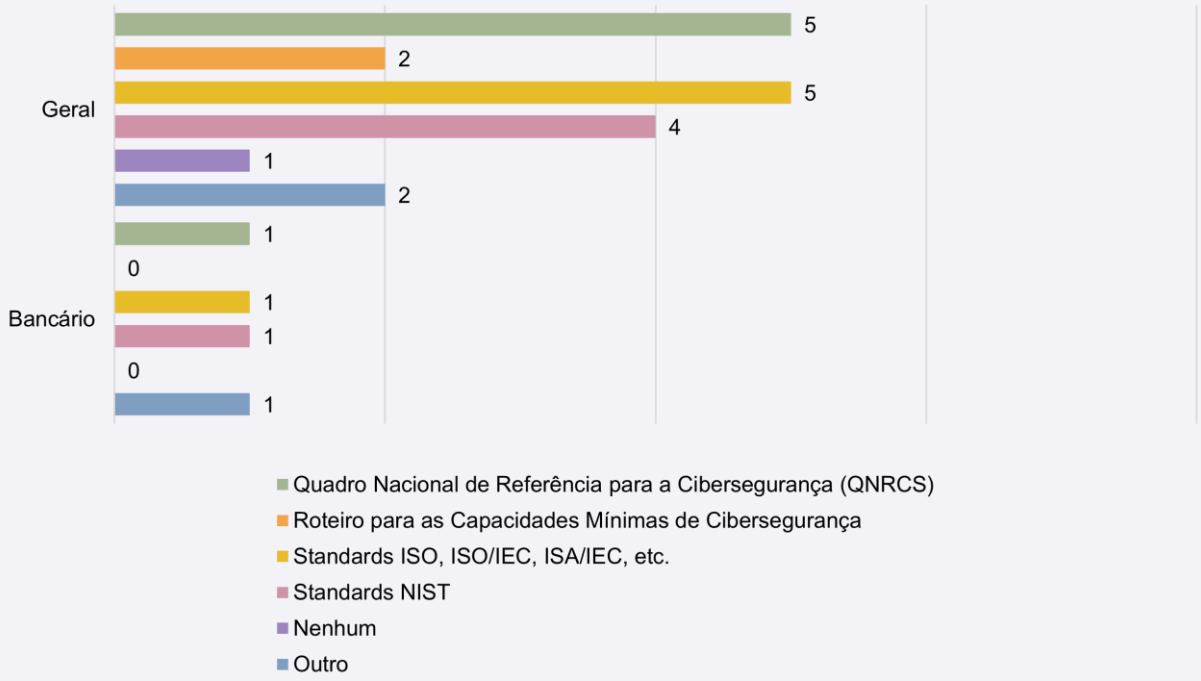
No setor bancário, o regulador inquirido considera que o CNCS poderia promover maior dinamização dos ISACs nacionais, prestar mais auxílio através da disponibilização de formação adequada às especificidades de cada setor, através da alimentação destes com informação.

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

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

9. *Standards* e boas práticas recomendadas

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



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

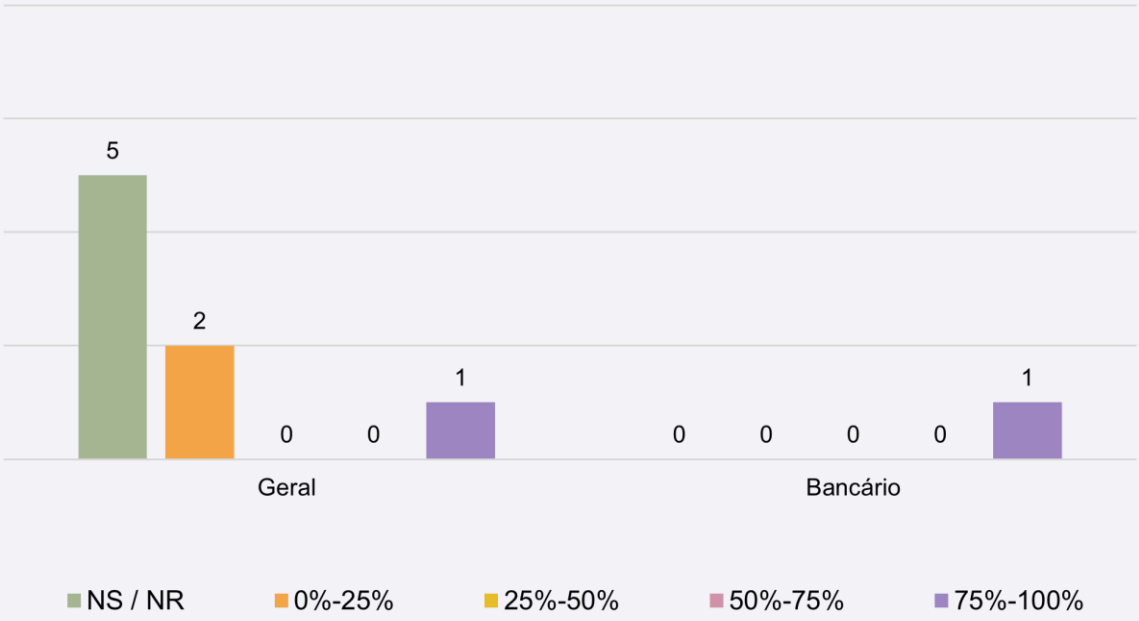
Na opção "outros", foram referidos *standards* da International Civil Aviation Organization (ICAO), legislação específica do setor bancário (EBA/GL/2019/04), legislação específica do setor bancário, e boas práticas como a utilização de DNSSEC (*Domain Name System Security Extensions*), DKIM (*Domain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

No setor bancário, o regulador refere recomendar o QNRCS, standards ISO, standards NIST e ainda outras recomendações setoriais, como a EBA/GL/2019/04, da Autoridade Bancária Europeia (EBA, no inglês).

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

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

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



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

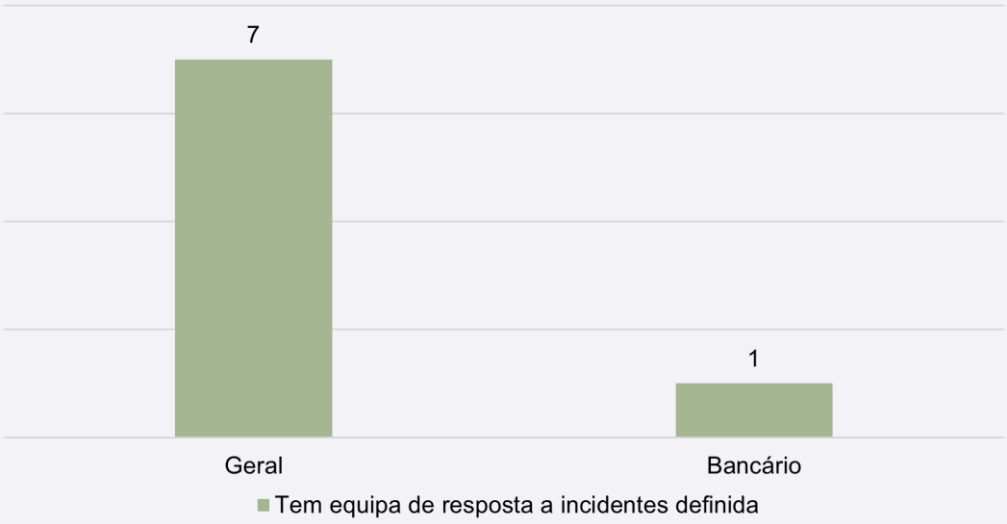
Tabela 2 - Setores com normativos específicos nacionais ou da UE em matéria de cibersegurança

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

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

10. Definição de equipa de resposta a incidentes de cibersegurança

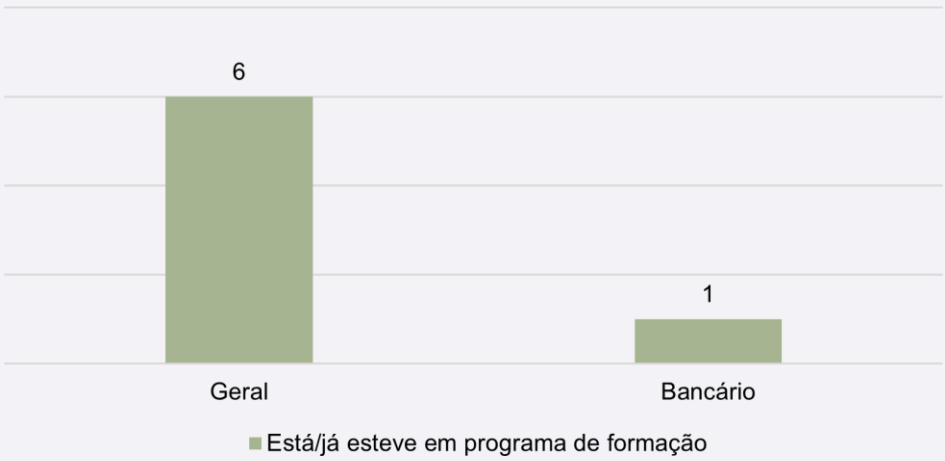
Gráfico 23 - Reguladores com equipa de resposta a incidentes definida



Relativamente à definição de equipas de resposta a incidentes, a grande maioria dos reguladores inquiridos (sete) tem uma equipa definida. O setor bancário indicou ter quipá definida.

11. Sensibilização e consciencialização

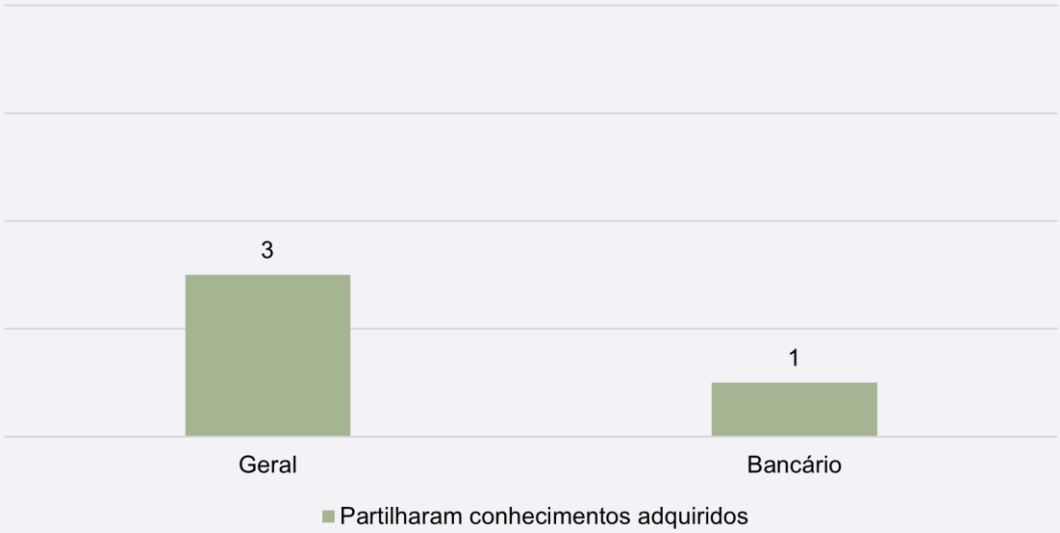
Gráfico 24 - Reguladores que estão ou já estiveram em programas de formação e sensibilização para os riscos no ciberespaço promovidos pelo CNCS ou por outra entidade



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

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

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

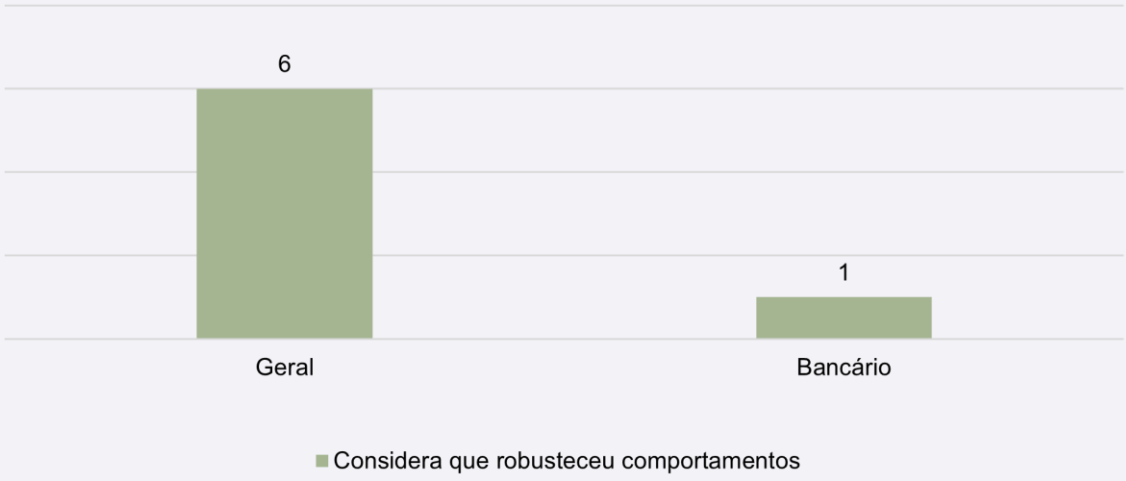


No seguimento da participação nos programas de formação e sensibilização para os riscos no ciberespaço, questionou-se se os conhecimentos adquiridos nesses programas foram partilhados com os OSE do setor. Os setores que fizeram essa partilha e os que não fizeram dividem-se igualmente.

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

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

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



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

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

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

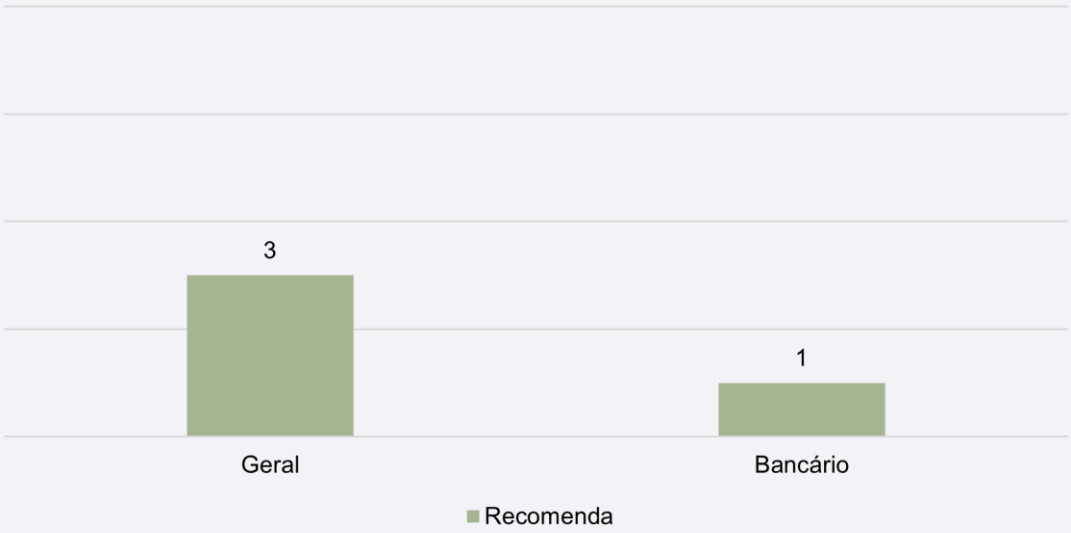
No setor bancário, o regulador inquirido considerou que a entidade formadora o sensibilizou para as principais vulnerabilidades a que o setor se encontra exposto.

12. Cooperação nacional/internacional de proteção do ciberespaço

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

Relativamente à pertença a estruturas de cooperação nacional ou internacional de proteção do ciberespaço, como os Centros de Análise e Partilha de Informação, apenas dois dos reguladores indicaram fazer parte de alguma dessas estruturas, enquanto os restantes seis indicaram não pertencer a qualquer estrutura do tipo. No caso do regulador inquirido do setor bancário, este indicou pertencer a estruturas do tipo referido.

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



Relativamente à pertença a estruturas de cooperação nacional ou internacional de proteção do ciberespaço, como os Centros de Análise e Partilha de Informação, apenas três dos reguladores indicaram fazer parte de alguma dessas estruturas, enquanto os restantes cincos indicaram não pertencer a qualquer estrutura do tipo. No setor bancário, o regulador inquirido recomenda a participação em centros de partilha e análise de informação aos OSE.

13. Regulação de entidades e OSE

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

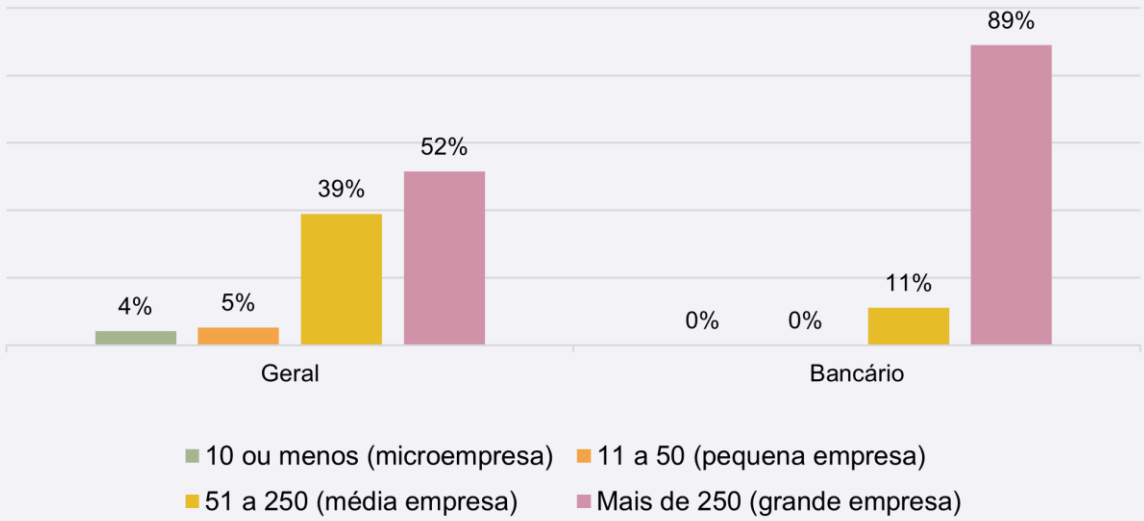
Tabela 3 - Estimativa do total de entidades reguladas pelos reguladores por setor

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

Tabela 4 - Número estimado das entidades reguladas que são OSE

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

Gráfico 30 - Número de colaboradores na organização



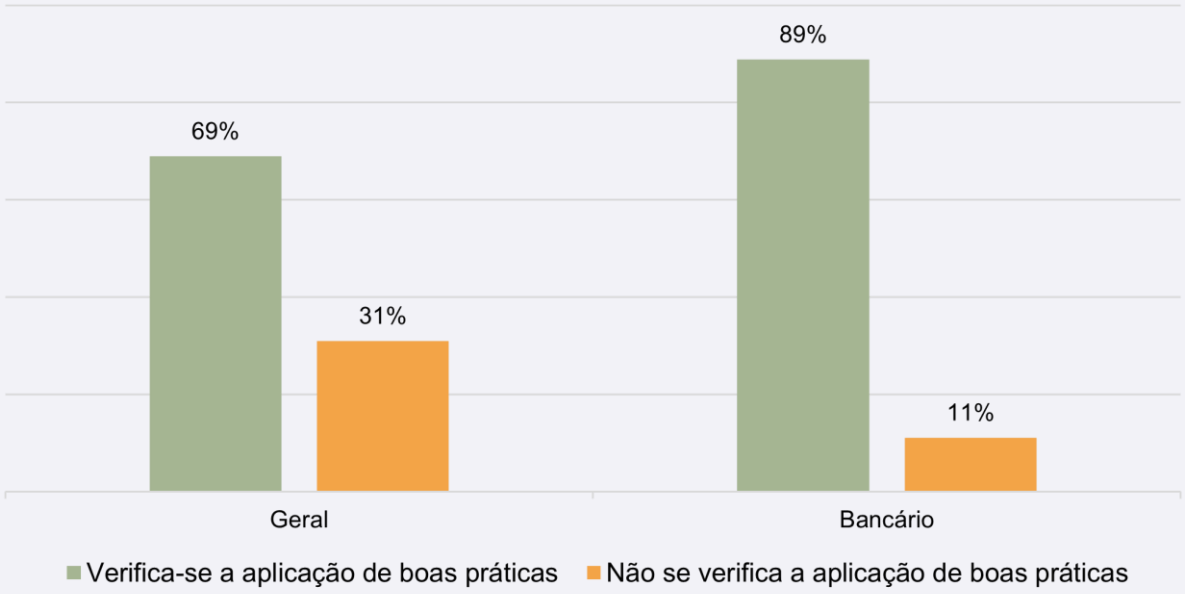
O tecido empresarial dos Operadores de Serviços Essenciais é constituído, na sua maioria, por grandes empresas (empresas com mais de 250 colaboradores), representando estas 52% entre os OSE. As médias empresas representam 39% dos OSE, distribuindo-se os remanescentes 9% pelas micro e pequenas empresas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

Destaca-se o setor bancário, em que as grandes empresas são mais comuns, nomeadamente 89% e médias empresas 11%. Não apresentando micro nem pequenas empresas.

A composição do tecido empresarial dos OSE difere grandemente daquele que é o tecido empresarial geral das empresas portuguesas. Enquanto entre os OSE mais de 50% destes são grandes empresas, 99,9% das demais empresas em Portugal são, segundo dados de 2022 da PORDATA, pequenas e médias empresas, com apenas 0,1% sendo grandes empresas[13].

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

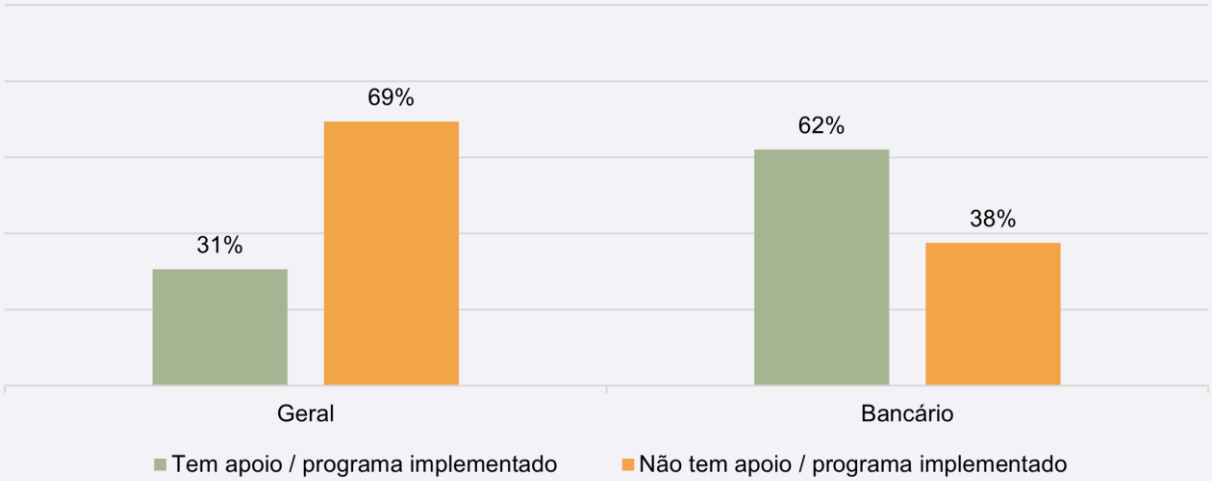
Gráfico 31 - Perceção sobre boas práticas de cibersegurança por parte dos colaboradores



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

O setor bancário destaca-se por ser um dos setores nos quais mais de 80% dos operadores consideram que boas práticas de cibersegurança são aplicadas pelos seus colaboradores, mais propriamente 89%.

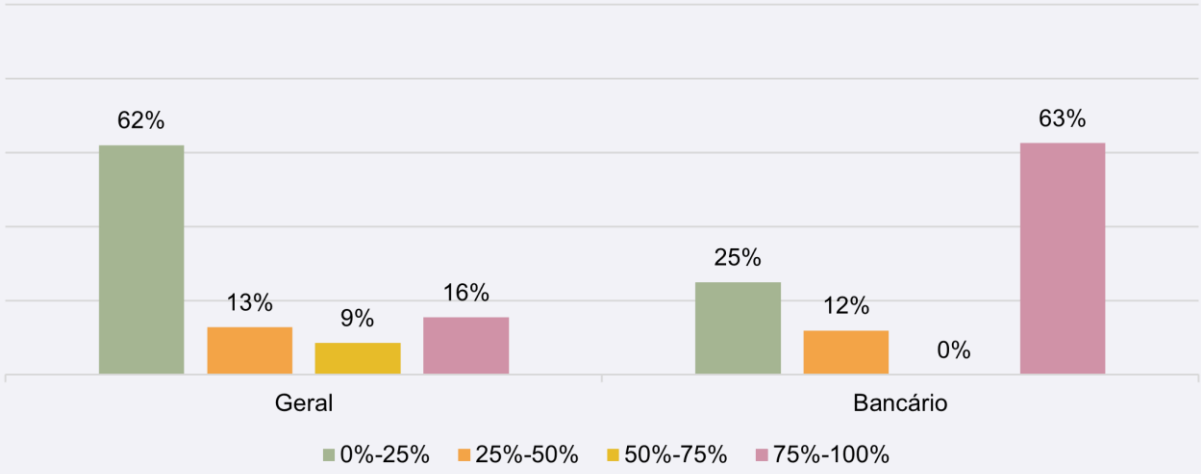
Gráfico 32 - Implementação de apoios ou programas, próprios ou do Estado, para colaboradores que desejem formação na área de cibersegurança



À data de realização do questionário, apenas um terço dos operadores tinham apoios ou programas próprios ou do Estado para colaboradores interessados em formação na área de cibersegurança. O setor bancário destaca-se dos restantes setores em estudo, uma vez que, no setor bancário, a maioria dos operadores (63%) tem maneira de fornecer esse apoio ou programa formativo aos colaboradores.

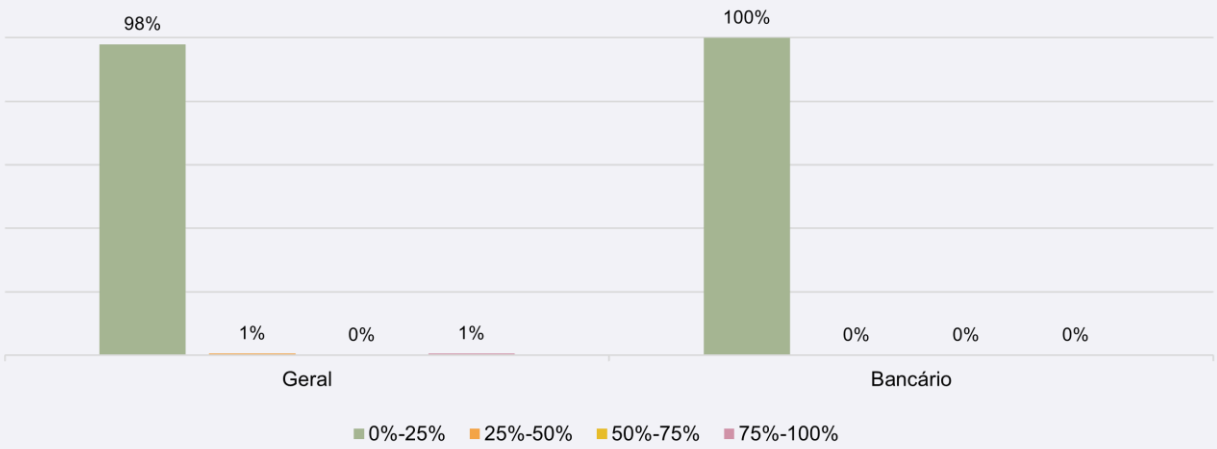
Importa sublinhar, que estas respostas não significam que não seja dada formação em cibersegurança aos colaboradores. O que acontece é que muita da formação disponibilizada pelos operadores aos colaboradores não está inserida num programa de formação específico, ou então não existem apoios para colaboradores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

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



Na maioria dos OSE (62%), a percentagem de colaboradores com formação básica em cibersegurança não ultrapassa os 25%. O setor bancário apresenta resultados positivos, dado que 63% dos operadores inquiridos indicam que a percentagem de colaboradores com formação básica na área se situa no intervalo 75%-100%.

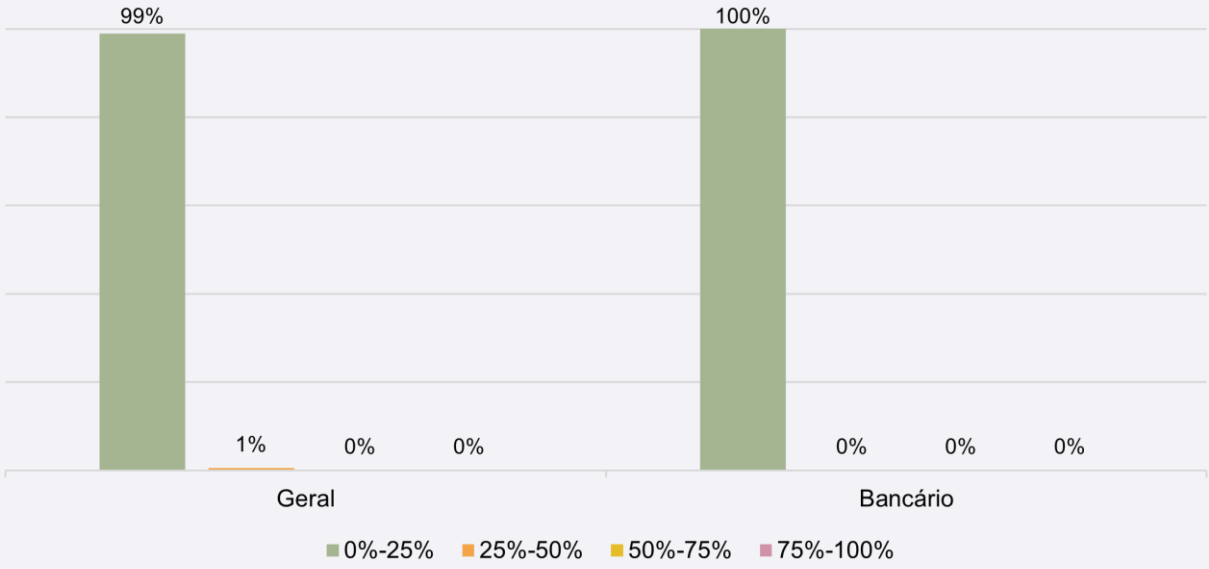
Gráfico 34 - Percentagem aproximada de trabalhadores do operador com formação superior em cibersegurança



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

Em termos gerais, a percentagem de trabalhadores dos operadores com formação superior em cibersegurança situa-se predominantemente na faixa entre 0%-25% em todos os operadores de todos os setores. No setor bancário a totalidade dos operadores encontra-se na faixa dos 0%-25% com formação superior em cibersegurança.

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

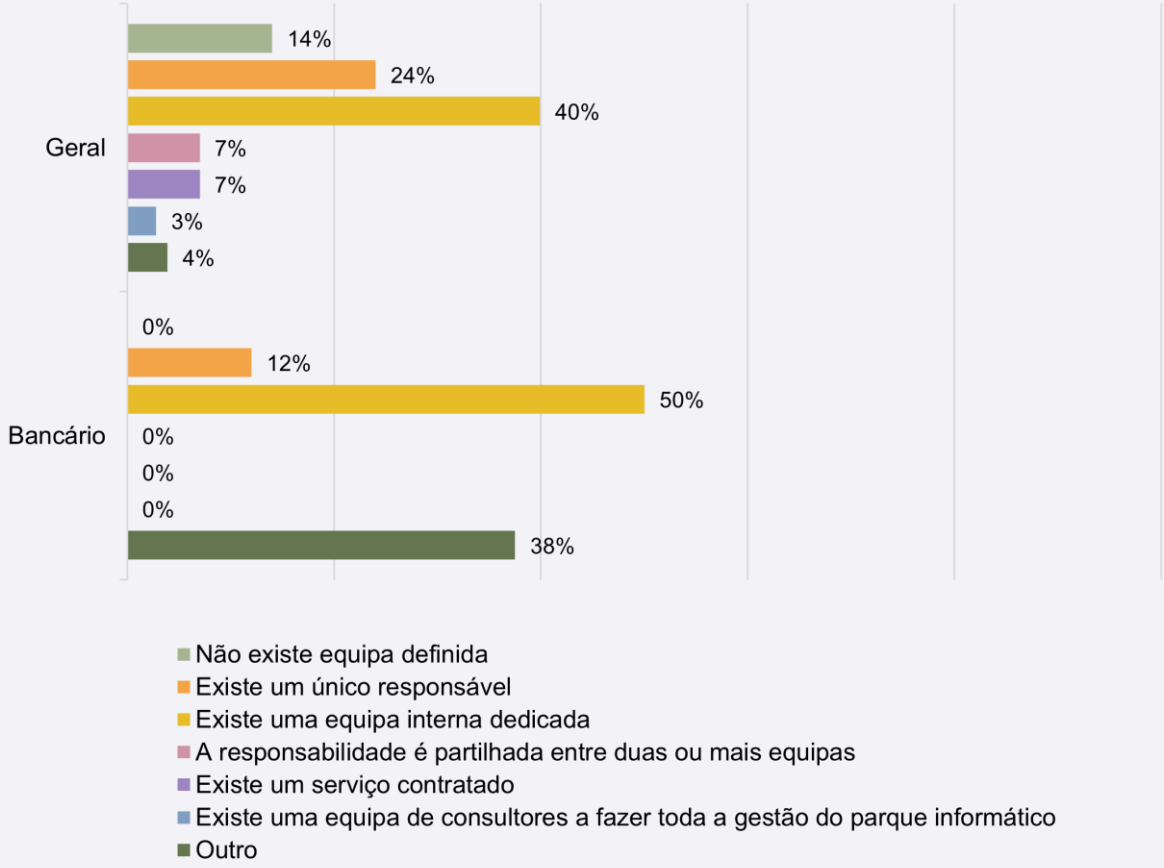


A proporção de trabalhadores com certificações em cibersegurança situa-se no intervalo 0%-25% em 99% dos casos. Contudo, há que destacar um setor, onde 3% dos operadores indicaram haver 25%-50% de colaboradores com certificações em cibersegurança.
No setor bancário a totalidade dos inquiridos situa-se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

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

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

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

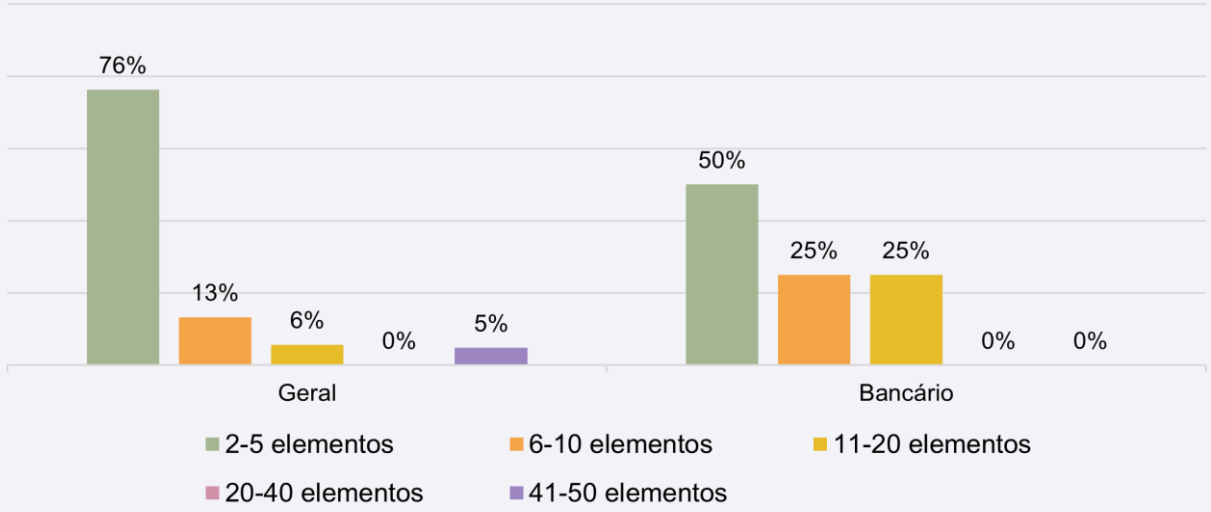


De maneira geral, no que diz respeito à existência de equipas de *helpdesk* em questões de cibersegurança e/ou tecnologias da informação, os setores apresentam duas abordagens principais: uma equipa interna responsável (40% dos casos) ou a existência de um único responsável (25% dos casos).

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

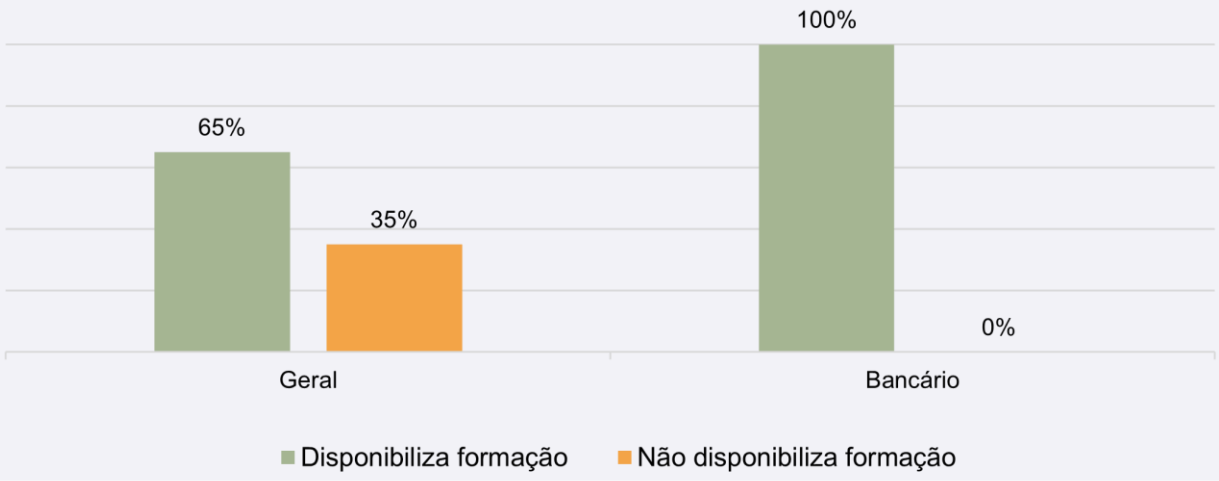
No setor bancário a responsabilidade é maioritariamente atribuída a uma equipa interna dedicada (50%), a existência de um único responsável (12%) e outras situações (38%).

Gráfico 37 - Composição das equipas de helpdesk



Na sua larga maioria, as equipas de *helpdesk* são compostas por 2-5 elementos. Entre os OSE com equipas de *helpdesk*, 76% apresentam equipas com esta composição. Esta composição foi a mais indicada em todos os setores, correspondendo em qualquer um destes à realidade de pelo menos 50% dos OSE com equipas de *helpdesk*. Verificam-se também outras composições, com equipas mais vastas, nas organizações de maior dimensão. No entanto, enquanto é evidente que apenas grandes empresas têm equipas de *helpdesk* com mais de 41 elementos, nem todas as grandes empresas têm equipas tão vastas. Resulta assim que há grandes empresas em que as funções de *helpdesk* são asseguradas por equipas mais reduzidas, até um máximo de 20 elementos. Concomitantemente, nenhum dos inquiridos indicou ter uma equipa de 20-40 elementos. No setor bancário predominam as equipas de 2-5 elementos (50%), as equipas de 6-10 elementos (25%) e as equipas de 11-20 elementos com igual percentagem.

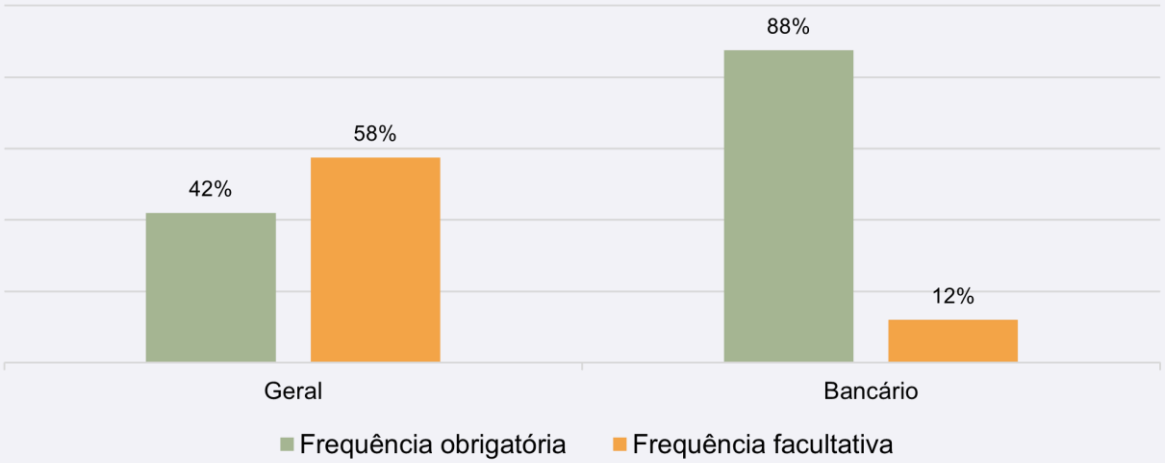
Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores



Em termos gerais, a formação em cibersegurança é disponibilizada a colaboradores em 65% dos OSE nos diversos setores. No setor da banca todos os OSE indicaram disponibilizar formação em cibersegurança aos seus colaboradores.

Comparando com dados do Inquérito à Utilização das TIC nas Empresas (IUTICE) de 2022, realizado pelo Instituto Nacional de Estatística (INE), 63,3% das empresas em Portugal procuraram consciencializar os seus colaboradores sobre cibersegurança durante o ano de 2021[15]. Já um outro estudo, realizado pela Microsoft Portugal em setembro de 2023, intitulado "Estado da Cibersegurança em Portugal", indica que 84% das empresas portuguesas ministram formação de sensibilização para a cibersegurança. A discrepância nestes resultados poder-se-á dever à composição das amostras de cada estudo. Embora seja expectável que cada vez mais empresas disponibilizem formação em cibersegurança aos seus colaboradores, um crescimento de 20% em dois anos das entidades que disponibilizam formação em cibersegurança aos seus colaboradores é improvável.

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



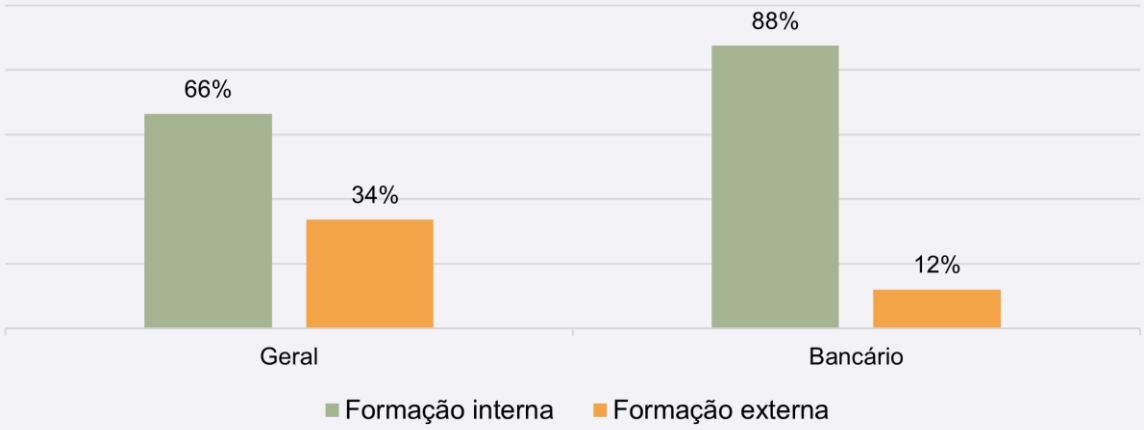
De uma forma geral, o caráter das formações disponibilizadas tende a ser mais facultativo (58%) do que obrigatório (42%). Surgem, no entanto, setores nos quais esta tendência não se verifica. Por exemplo, no setor da banca, são mais os OSE nos quais a formação tem caráter obrigatório em vez de facultativo. Destacam-se as elevadas percentagens de OSE nos quais a frequência das formações é obrigatória nos setores da banca (88%).

Voltando a comparar com dados do IUTICE de 2022, verificam-se percentagens discrepantes ao nível das formações obrigatórias ou facultativas entre OSE e demais empresas em Portugal. Enquanto em 42% dos OSE que disponibilizam formação, esta é de caráter obrigatório, apenas em 19,2% das empresas portuguesas há formações obrigatórias. Já ao nível das de caráter facultativo (ou voluntário, nos termos do IUTICE), os resultados são mais similares aos do questionário realizado pelo CNCS, uma vez que estas se verificam em 58% dos OSE que disponibilizam formação e em 56,2% das empresas participantes no inquérito[16].

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

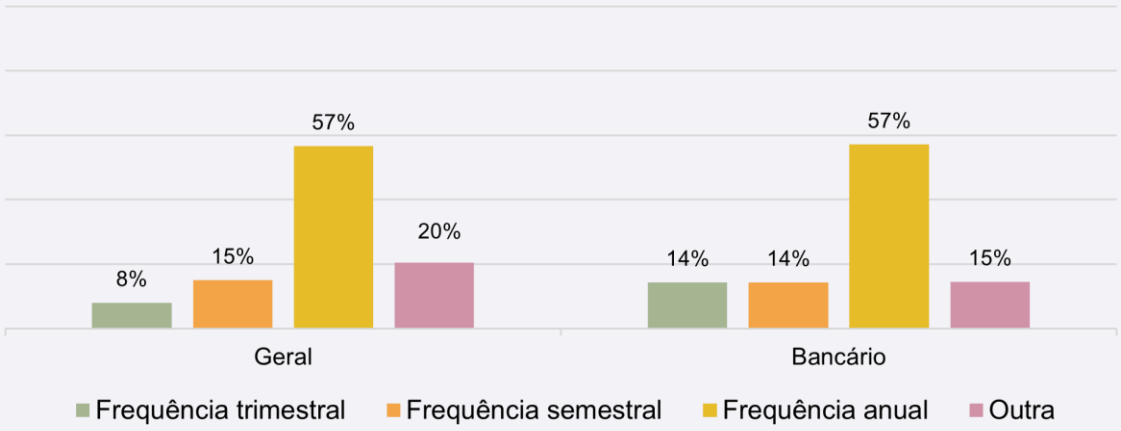
[16] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19.

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



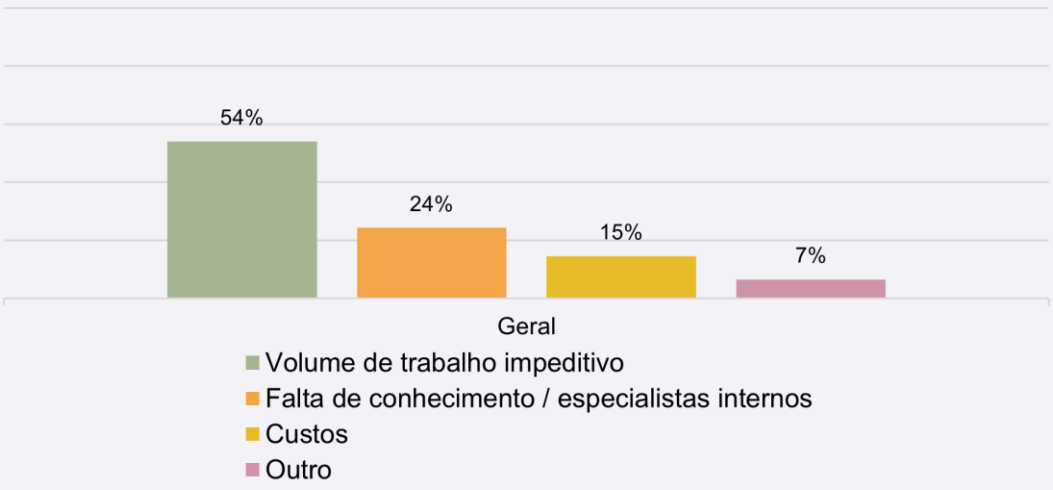
Neste gráfico, fica evidenciado o maior recurso à formação interna do que externa entre os OSE. A maioria dos inquiridos (66%) recorre aos meios internos para fins de formação aos colaboradores. Surge em destaque o setor bancário, com as maiores percentagens de OSE a darem formação interna (88% respetivamente).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

Gráfico 41 - Frequência média dos momentos de formação



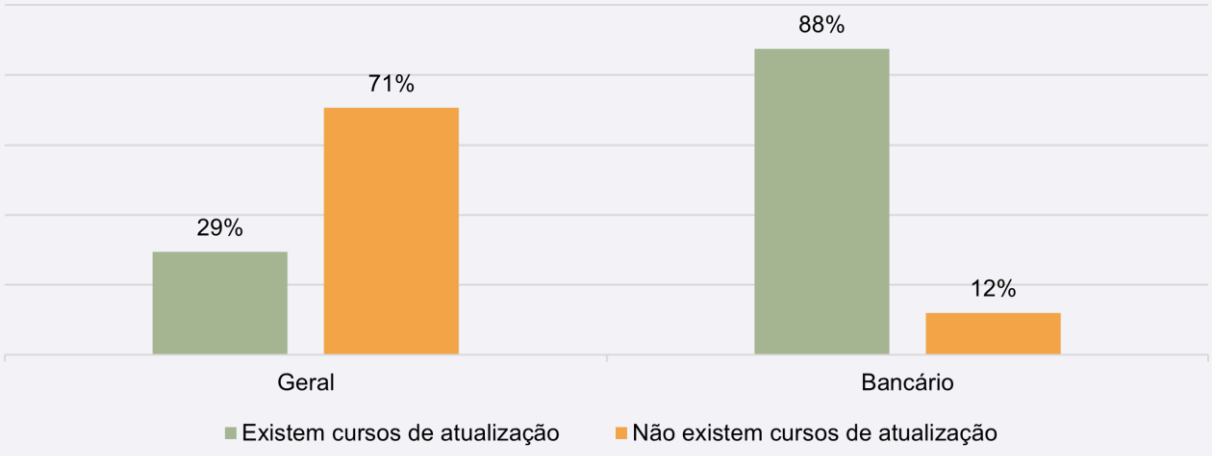
Em termos gerais, a maioria dos OSE que disponibiliza formação (57%) indica que a frequência média dos momentos de formação é anual.
Entre os OSE que indicaram "Outra" frequência, tanto se registam frequências superiores à trimestral, chegando os momentos de formação a ser mensais ou mesmo semanais, como frequências inferiores à anual, onde não existe uma periodicidade definida e os momentos de formação sucedem de modo *ad hoc*. O setor bancário segue a tendência geral na frequência das formações.

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



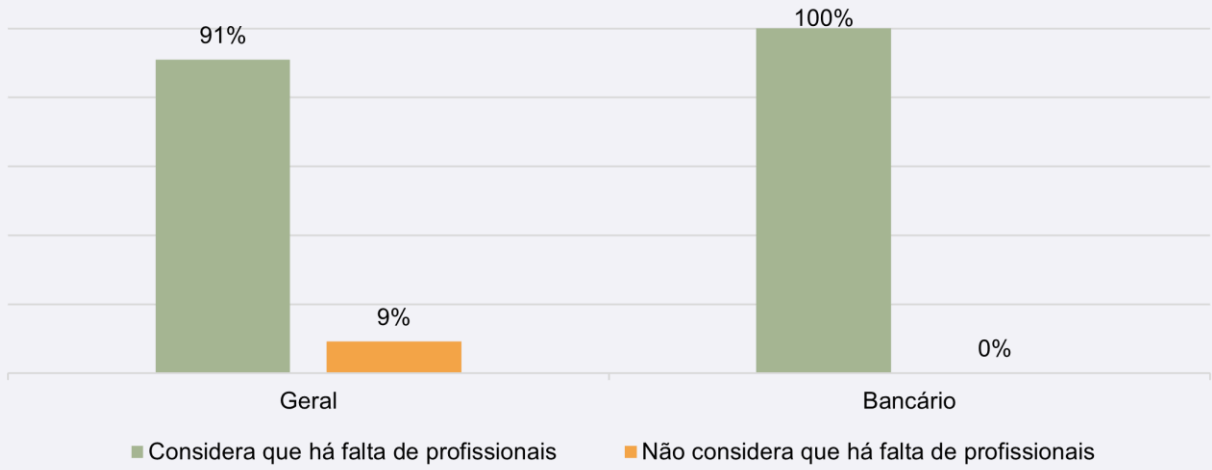
Os motivos para a não disponibilização de formação são na sua maioria atribuídos ao volume de trabalho impeditivo, tendo este motivo sido indicado por 54% dos OSE que afirmaram não disponibilizar formação em cibersegurança aos seus colaboradores. A falta de conhecimento ou de especialistas internos por 24% já os custos por 15%. Foram ainda mencionados outros motivos por 7% dos OSE. Esses outros motivos passam, segundo os OSE, pela falta de planos de formação dentro das organizações e pela alocação de recursos financeiros a formação noutras áreas que não a cibersegurança. Como a totalidade do setor bancário disponibiliza formação esta questão não se aplica.

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



A oferta de cursos ou formações de atualização em cibersegurança para os colaboradores é escassa na generalidade, com apenas 29% dos OSE inquiridos a indicarem a existência destes cursos. Contudo, o setor bancário contraria essa tendência geral, com 88% dos inquiridos no setor bancário a indicarem que disponibilizam cursos de atualização.

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



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

A escassez de profissionais em cibersegurança é um problema que persiste há largos anos, devido à discrepância entre a velocidade a que a tecnologia evolui e o tempo que leva a formar os profissionais. Segundo o Fórum Económico Mundial, a atual escassez global de profissionais em cibersegurança é de cerca de 4 milhões de profissionais[17] e, segundo dados da ENISA, essa escassez será de cerca de 300 mil profissionais na União Europeia[18]. Esta falta de profissionais coloca aos empregadores na área desafios como conseguir pessoal qualificado, conseguir desenvolver equipas que possuam as capacidades técnicas desejadas e conseguir manter os bons profissionais encontrados[19]. De modo a combater esta escassez, organizações como o Fórum Económico Mundial e a ENISA têm feito diversas recomendações, que passam pela contratação de profissionais vindos de outras áreas de formação que não apenas as das TIC, engenharia e matemática, pela admissão de colaboradores menos experientes, ou mesmo sem experiência (sendo esta adquirida ao longo do desempenho das funções pretendidas), a admissão de colaboradores em trabalho totalmente remoto, e pela valorização dos profissionais, não só a nível salarial, mas também a nível das perspetivas de progressão de carreira e até mesmo do respeito pelos profissionais no local de trabalho[20] [21].

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

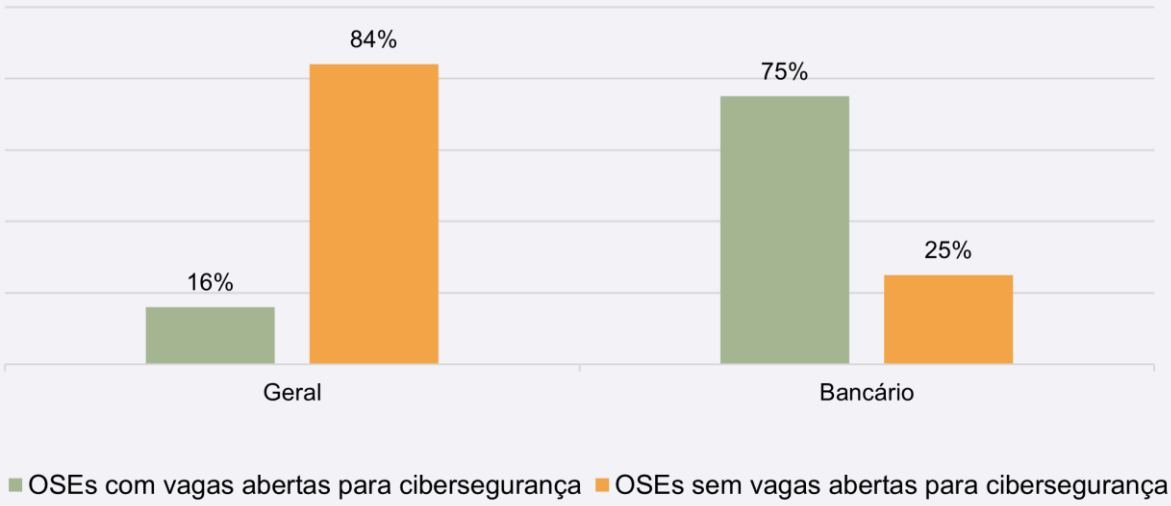
[18] ENISA, “Cybersecurity Skills Conference: Strengthening human capital in the EU”, https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.

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

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

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

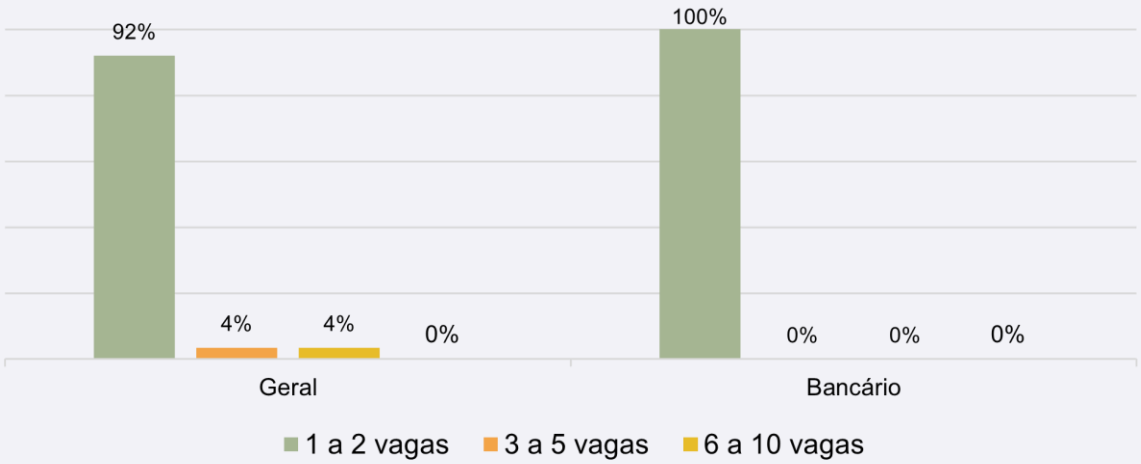
Gráfico 45 - Vagas abertas para a área de cibersegurança



À data da realização do questionário, apenas 16% dos OSE inquiridos tinham vagas abertas para cibersegurança. Sectorialmente, registaram-se duas exceções, sendo uma delas o setor bancário, com 75% dos OSE a indicarem ter vagas em aberto.

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

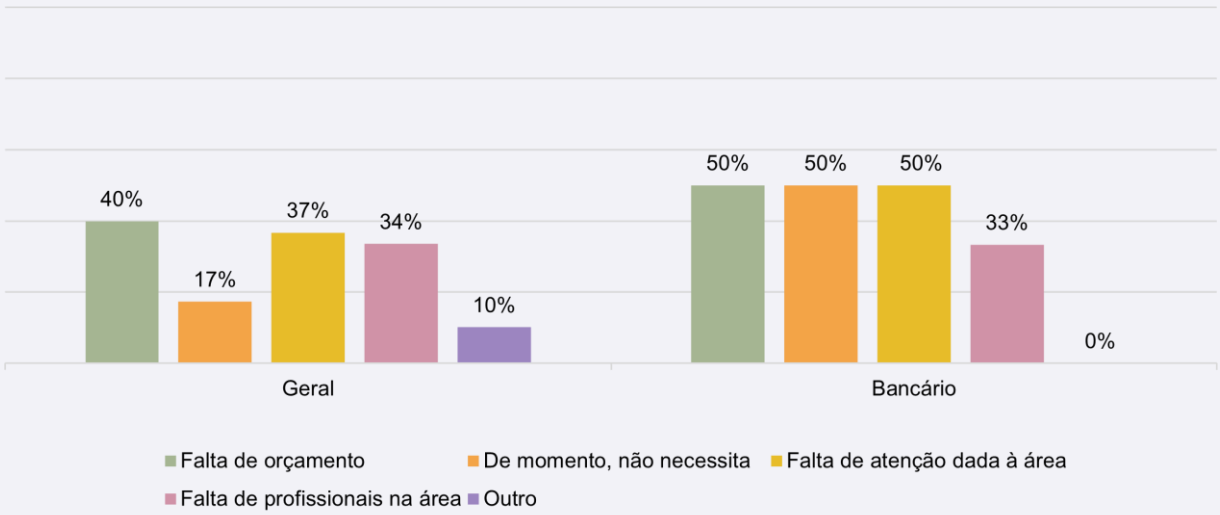
Gráfico 46 - Número de vagas nos OSE com vagas abertas para a área de cibersegurança



Entre os 16% de OSE que tinham vagas abertas na área de cibersegurança, a maioria destes (92%) tinha 1 a 2 vagas por preencher. Tal era o caso para todos os OSE com vagas em aberto no setor da banca.

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

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

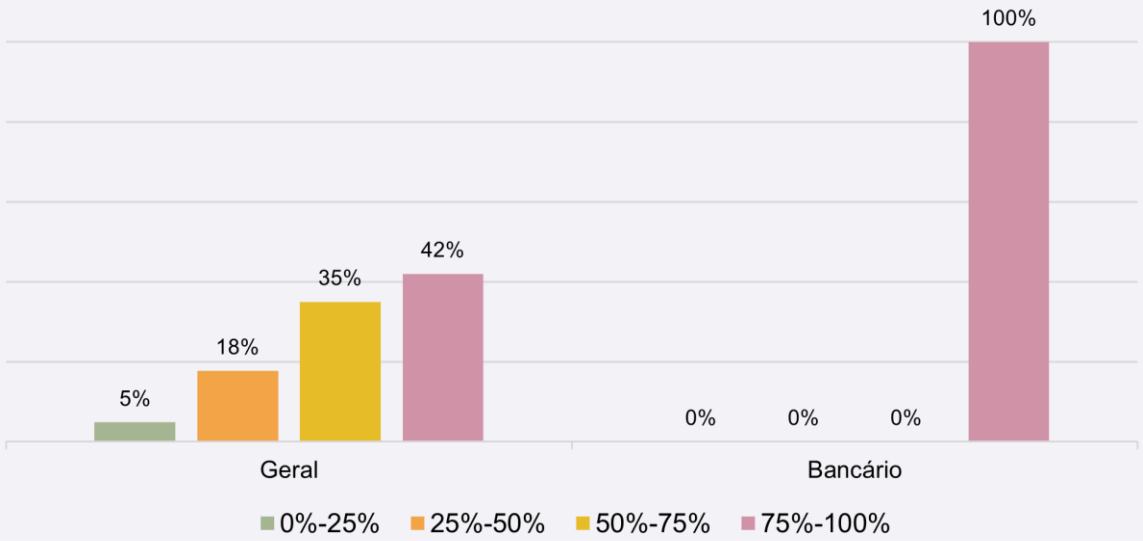


No seguimento das questões sobre vagas em aberto para a área de cibersegurança, questionou-se também os motivos pelos quais os OSE não teriam tais vagas disponíveis.
A resposta mais comum foi a falta de orçamento, indicada por 40% dos OSE sem vagas em aberto, seguida da falta de atenção dada à área (37%) e da falta de profissionais de cibersegurança (34%). Apenas em 17% dos casos foi indicado que não havia vagas em aberto por se considerar que de momento não eram necessários mais profissionais.Os 10% de OSE que indicaram "outros" motivos mencionaram motivos como o facto de existirem poucos conhecimentos/noção da gravidade de um ataque informático, haver questões legais que impedem a contratação de mais recursos.
No setor bancário todos os motivos foram apontados por 50% dos OSE com exceção da falta de profissionais na área que apenas foi mencionado por 33% dos OSE.

De acordo com os dados do IUTICE de 2022, 61,4% das empresas portuguesas sentiram dificuldades no recrutamento. Entre estas, 82,1% apontaram a falta de candidaturas como um problema, cerca de 57% mencionaram a falta de qualificações ou de experiência relevante dos candidatos como outra dificuldade e 91,9% indicaram que as expectativas de remuneração dos candidatos eram demasiado elevadas[23].
Voltando aos dados obtidos através do questionário realizado, a "falta de atenção dada à área" indicada por 37% dos OSE sem vagas em aberto é um dos aspetos mais preocupantes que surgem na análise. Um dos Objetivos Estratégicos (Objetivo 3) da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 passa por gerar e "garantir a alocação de recursos adequados para a edificação e sustentação da capacidade nacional para a segurança do ciberespaço"[24], objetivo esse que não pode ser cumprido quando há falta de atenção dada à área. Tratando-se de Operadores de Serviços Essenciais, esta lacuna torna-se ainda mais grave. Recorda-se, também, que é uma boa prática constante de normativos internacionais, como a ISO/IEC 27001, que a direção/administração das organizações demonstre o seu compromisso para com segurança da informação e que esta assegure a alocação dos recursos necessários para cumprir esse desígnio[25].

[23] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 15-17.
[24] CNCS, "Estratégia Nacional de Segurança do Ciberespaço 2019-2023", 11, https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.
[25] International Organization for Standardization, "International Standard ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements", 2.

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

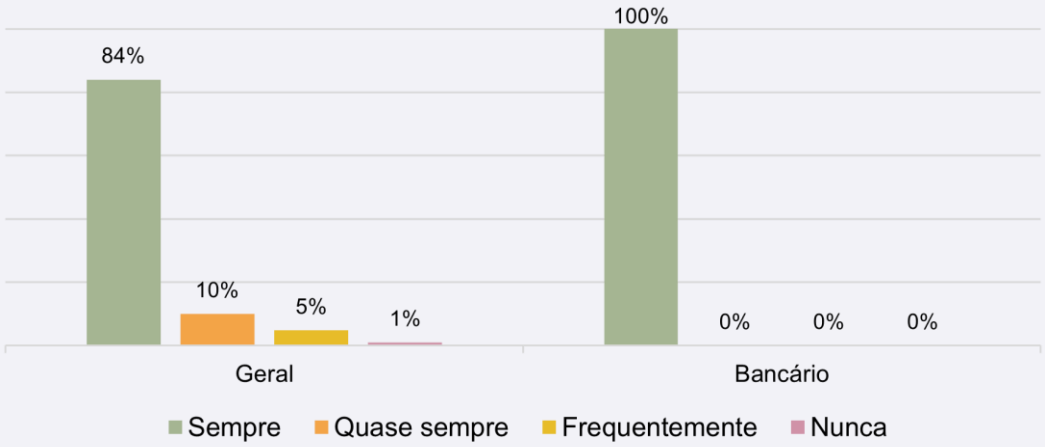


Apesar de predominar entre os OSE o intervalo 75%-100% de colaboradores com acesso a equipamentos digitais (indicado por 42% dos OSE), é visível que, com exceção de dois setores, sendo um deles o setor da banca onde 100% dos OSE encontra-se no intervalo de 75%-100%, há diversos setores que operam sem que a quase totalidade dos colaboradores tenham acesso a esse tipo de equipamentos.

Segundo dados do IUTICE de 2022, em 2021, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais (+17,2 p.p. face a 2021), abrangendo 28,1% do pessoal ao serviço (+4,2 p.p. que em 2021). Neste ano, 74,7% das empresas tinham pessoal ao serviço com acesso remoto ao sistema de correio eletrónico da empresa[26].

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

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

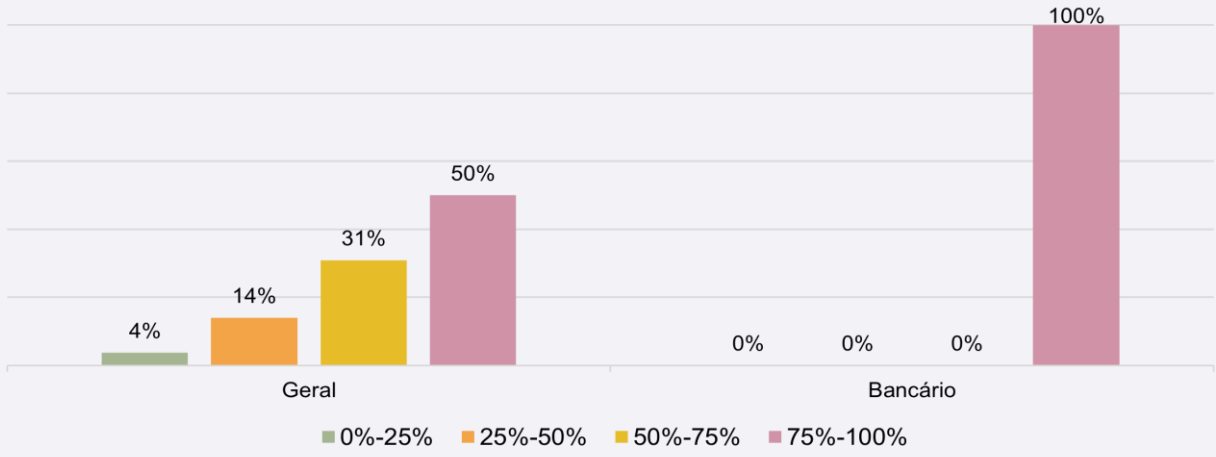


Os OSE dos setores em análise são, na sua maioria (84%), sempre responsáveis pelo fornecimento dos equipamentos necessários para as funções dos colaboradores. Todos os operadores inquiridos no setor da banca indicaram ser os próprios a fornecer sempre os equipamentos necessários aos colaboradores.

Ressalva-se ainda que não se registaram situações em que os operadores nunca fornecem os equipamentos, impondo esse encargo aos colaboradores.

Novamente, sublinha-se que segundo o IUTICE de 2022, 85,7% das empresas disponibilizavam dispositivos portáteis permitindo ligação móvel à Internet para fins profissionais, abrangendo 28,1% do pessoal ao serviço[27].

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

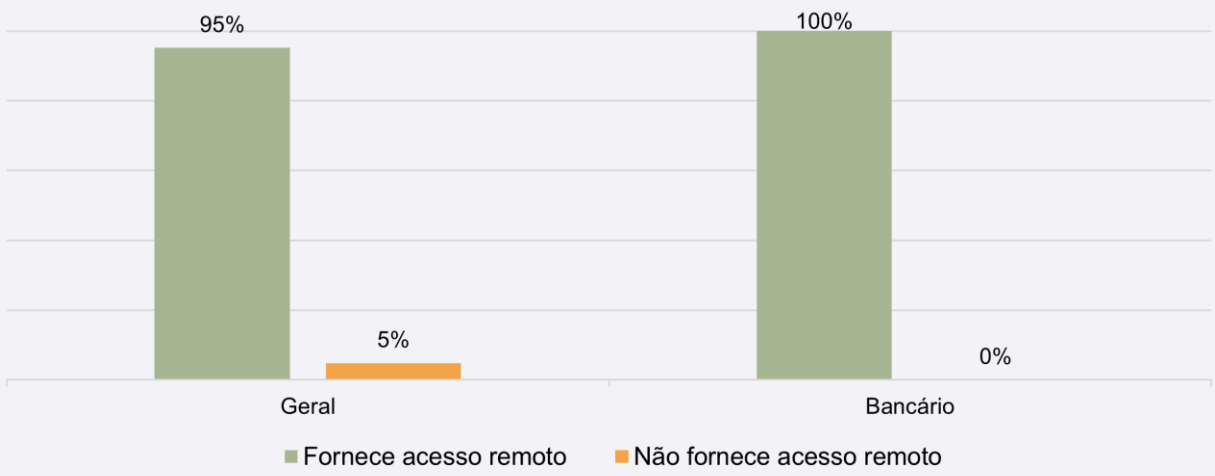


A percentagem aproximada de colaboradores com acesso à Internet no desempenho das suas funções é predominantemente acima de 50% em todos os setores.
No setor bancário, verifica-se que todos os operadores fornecem esse acesso a pelo menos 75% dos colaboradores.

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

Voltando a comparar com dados do IUTICE, mas agora com o de 2023, verifica-se que há mais colaboradores com acesso à Internet no contexto específico dos OSE do que das várias empresas portuguesas. Juntando os dois intervalos onde mais de 50% dos colaboradores têm acesso à Internet, obtém-se 81% de OSE onde 50% dos colaboradores acedem à Internet no desempenho das suas funções. No contexto empresarial português, apenas 48,9% dos colaboradores têm acesso à Internet para fins de trabalho. Mesmo comparando sectorialmente onde possível, como nos setores da energia e dos transportes, os OSE continuam a apresentar mais colaboradores com acesso à Internet: segundo o IUTICE, no setor da energia, há 39,8% de colaboradores com acesso à Internet, enquanto o questionário realizado demonstra que em 89% dos OSE desse setor, 50% dos colaboradores ou mais têm acesso à Internet; e no setor dos transportes, 56,6% dos colaboradores têm acesso à Internet no contexto empresarial português, enquanto no contexto dos OSE 88% indicam haver 50% ou mais colaboradores com acesso à Internet para fins de trabalho[28].

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



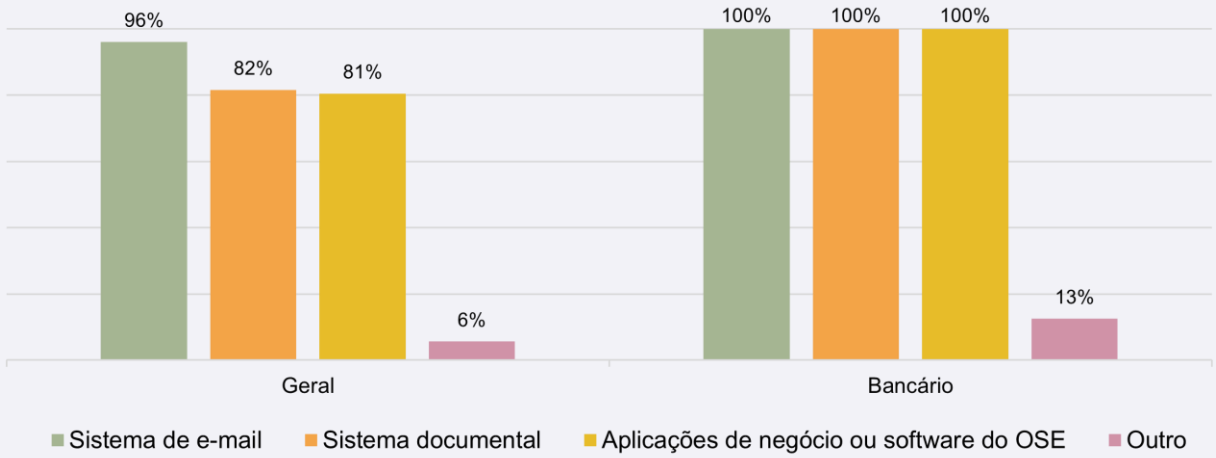
O fornecimento de acesso remoto aos sistemas (e-mail, aplicações ou documentos) pelos OSE aos colaboradores é uma realidade em praticamente todos os OSE inquiridos (95%). No setor da banca, todos os OSE indicaram permitir o acesso remoto a esses sistemas por parte dos seus colaboradores.

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

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

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

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

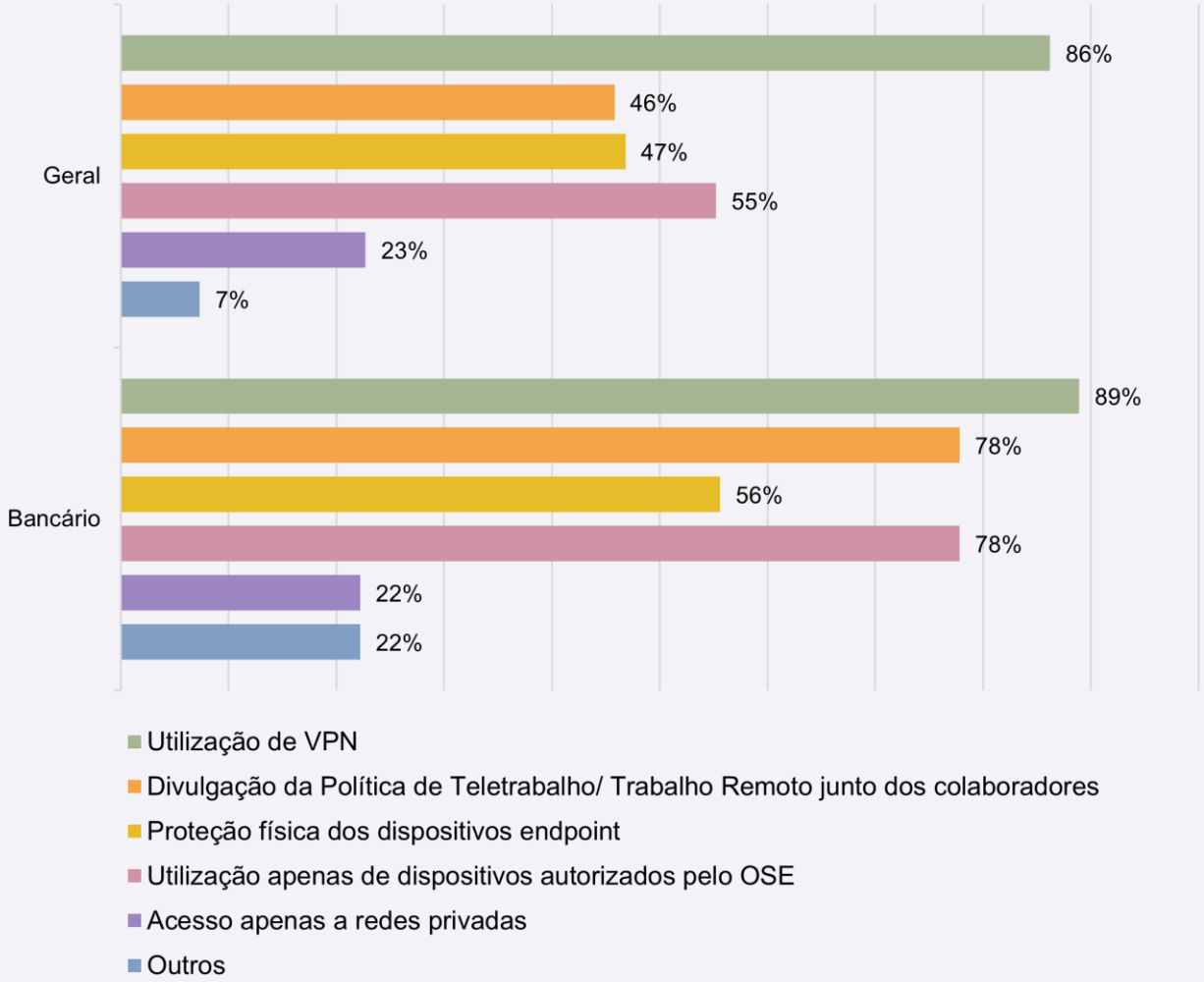


Para realizar uma análise mais granular no seguimento da questão anterior, foi questionado aos OSE a que sistemas em concreto é fornecido o acesso remoto. Entre os que concedem o acesso remoto os colaboradores, 96% concedem-no ao sistema de *e-mail*, 82% concedem-no ao sistema documental e 81% concedem-no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

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

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

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

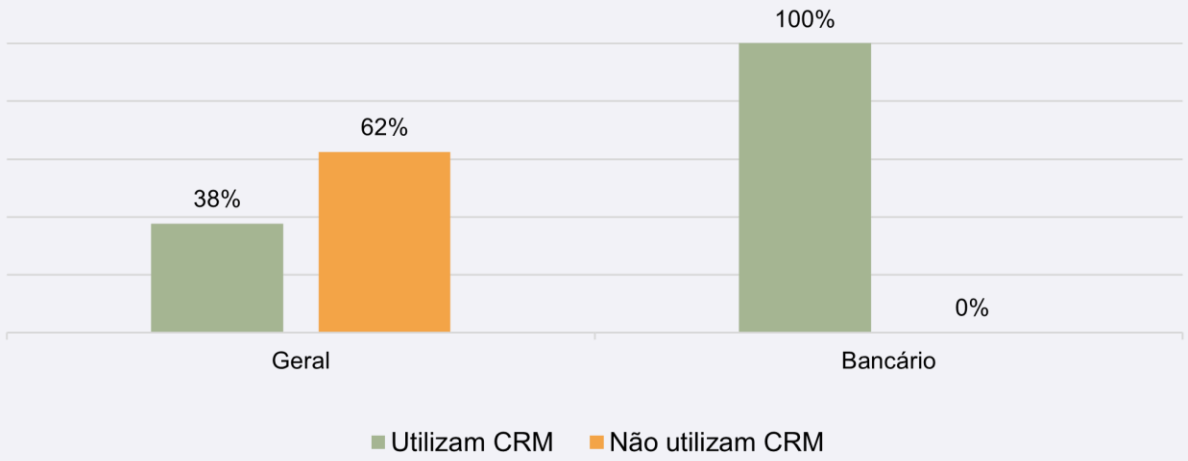


No que respeita às boas práticas de cibersegurança nos acessos remotos disponibilizados, a utilização de VPN é a que mais se verifica (86% dos casos em geral e 89% dos casos do setor bancário). Tal leva a que o acesso remoto realizado apenas através de redes privadas não seja uma exigência frequente dos operadores, tornando-a a medida de segurança para acesso remoto menos utilizada pelos OSE. No entanto, esta pode ser uma medida de segurança adicional, mesmo quando se utiliza VPN.

A segunda boa prática mais aplicada é a utilização de dispositivos autorizados pelos OSE, mas com uma prevalência bem mais reduzida (verificada apenas em 55% dos casos e 78% no setor da banca). Medidas como a divulgação da Política de Teletrabalho/Trabalho Remoto, proteção física dos dispositivos *endpoint* e acesso apenas através de redes privadas verificam-se em menos de 50% dos operadores inquiridos. Os operadores que indicaram outras boas práticas mencionaram a utilização de autenticação multifator, máquinas virtuais a operar nos servidores do operador (VDI's: *Virtual Desktop Infrastructure*) e gestão de acessos privilegiados (PAM: *Privileged Access Management*).

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

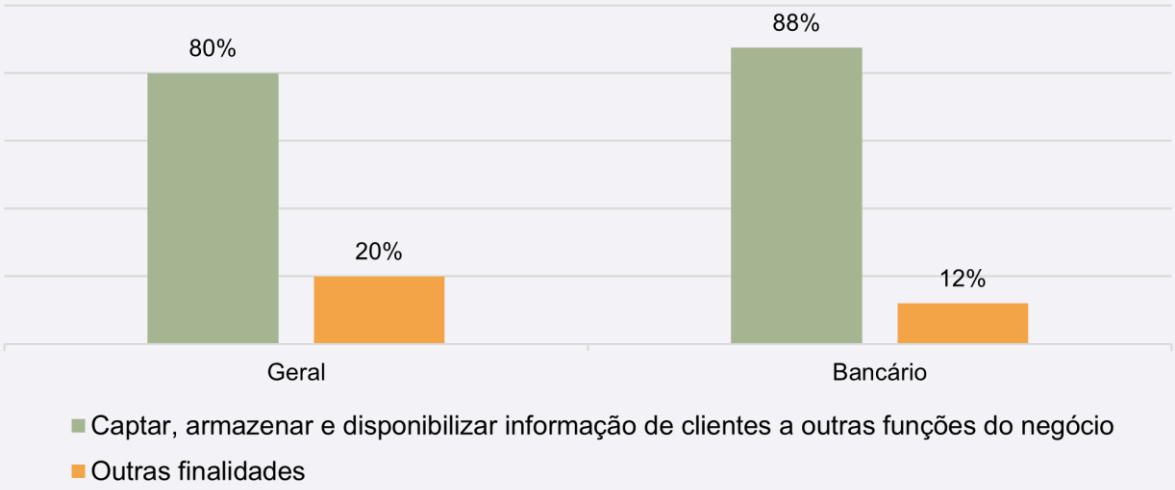
Gráfico 54 - OSE que utilizam *Customer Relationship Management Software* (CRM)



São mais os operadores que não utilizam *software* de *Customer Relationship Management* (CRM)[31] - 62% - do que aqueles que utilizam - 38%. Curiosamente, nos dois setores da área financeira (bancário e IMF) observa-se um grande contraste já que de todos os OSE do setor bancário utilizarem CRM e nenhum dos OSE das IMF utilizar este tipo de *software*.

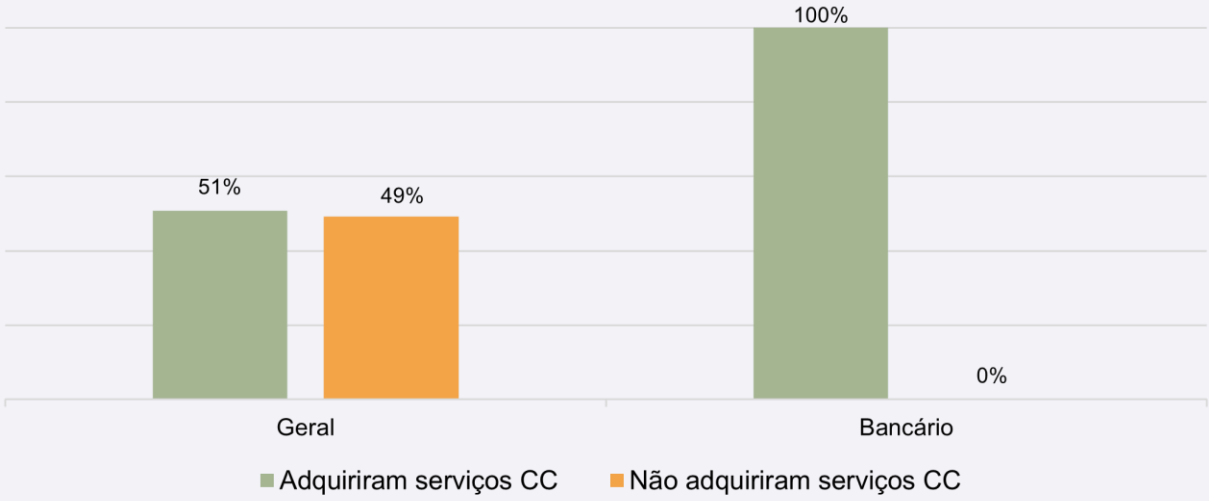
[31] *Software* de *Customer Relationship Management* (CRM) refere-se a *software* que permite às organizações gerir as suas interações e relações com atuais e potenciais clientes. As soluções de CRM podem auxiliar ainda na gestão de contactos, de vendas, da produtividade, na simplificação de processos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

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



Entre os operadores que utilizam CRM, a maioria utiliza-o para captar, armazenar e disponibilizar informações de clientes a outras funções do negócio (80%). Os restantes 20% utilizam CRM para outros fins não especificados. Um dos setores em que mais OSE utilizam CRM para as funções especificadas é o bancário, com 88% dos inquiridos a mencionar utilizar CRM.

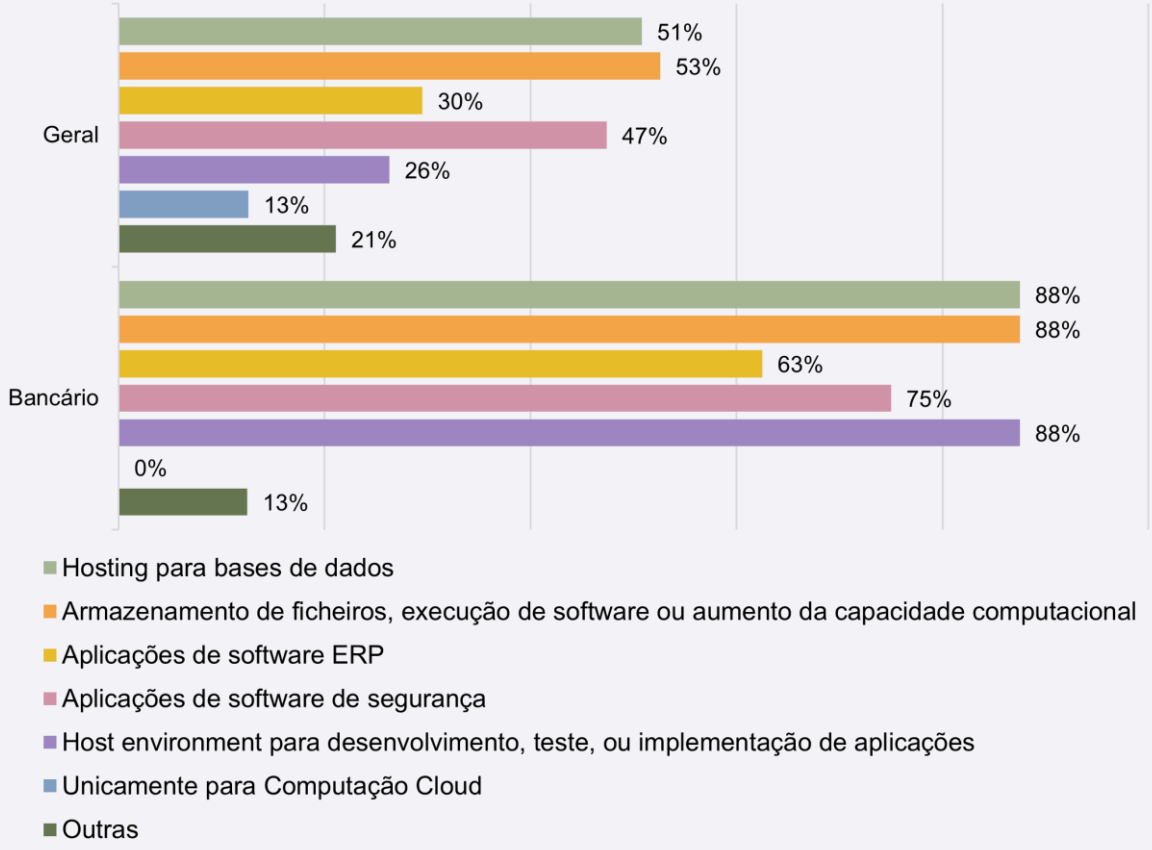
Gráfico 56 - OSE que adquiriram serviços de Computação Cloud (CC)



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

O relatório *NIS Investments* de 2022 demonstra que a procura por serviços *cloud* aumentou grandemente devido aos efeitos da pandemia, tendo sido uma prioridade de investimento nesse ano - cerca de 45% dos OSE colocaram o investimento em serviços *cloud* como um dos principais objetivos de 2021[32]. 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*)[33]. Contrastando com os dados do IUTICE de 2023, no panorama geral das empresas portuguesas, apenas 37,5% destas tinham adquirido serviços de *cloud computing*[34].

Gráfico 57 - Finalidades dos serviços de Computação Cloud adquiridos



As finalidades dos serviços de Computação Cloud são múltiplas, variando entre *hosting* para bases de dados; armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional; aplicações de *software* ERP[35] aplicações de *software* de segurança; *host environment* para desenvolvimento, teste ou implementação de aplicações; e, por fim, exclusivamente para Computação *Cloud*.

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

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

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

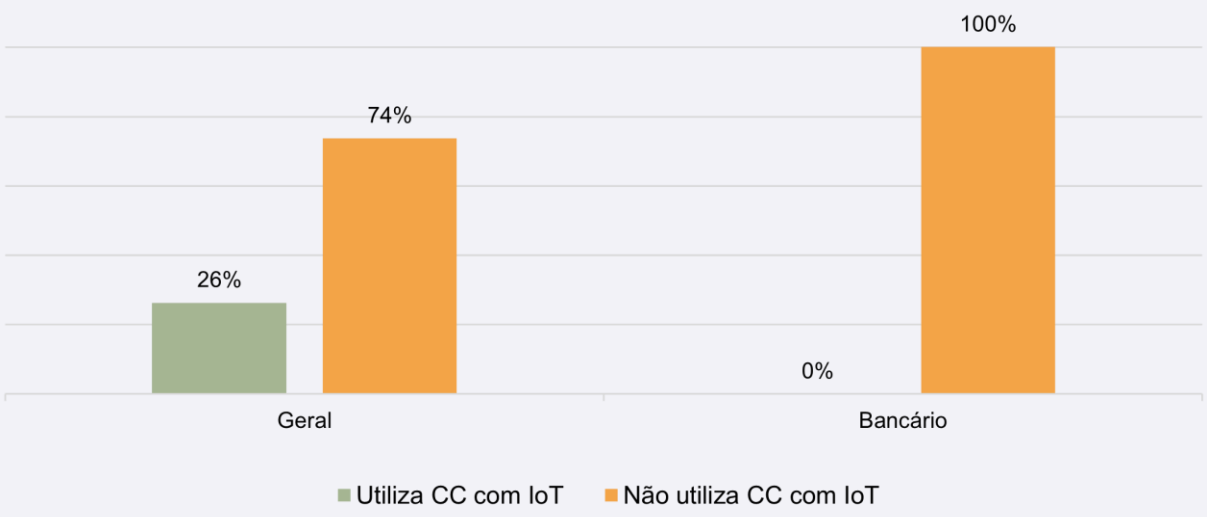
[35] *ERP (Enterprise Resource Planning)* refere-se a um tipo de *software* que as organizações utilizam para gerir os seus recursos e atividades do dia-a-dia, passando pela gestão de projetos, de recursos humanos e logística, entre outras áreas fundamentais para o funcionamento de uma organização. Uma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

De forma geral, é mais comum os operadores terem como finalidade *hosting* para bases de dados, armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional e aplicações de *software* de segurança.
No setor bancário, uma das aplicações com grande destaque é a utilização de Computação *Cloud* para *host environment* para desenvolvimento, para além do *hosting* para base de dados e do armazenamento de ficheiros.

A nível setorial, torna-se evidente que o armazenamento de ficheiros, execução de *software* ou aumento da capacidade computacional é uma das finalidades mais comuns no setor da banca, tendo sido indicada por pelo menos 88% dos OSE deste setor.

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

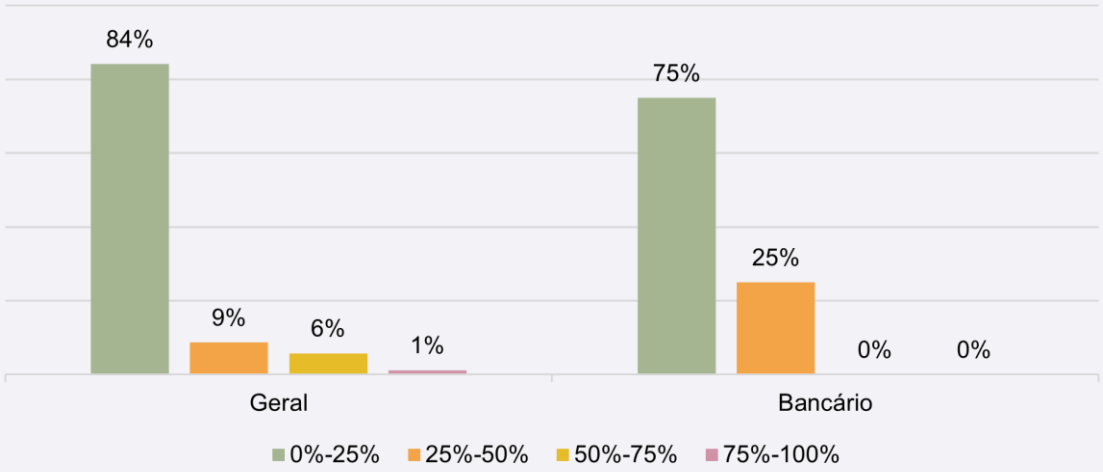
Gráfico 58 - Utilização de serviços de CC em conjunto com Internet of Things (IoT)



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

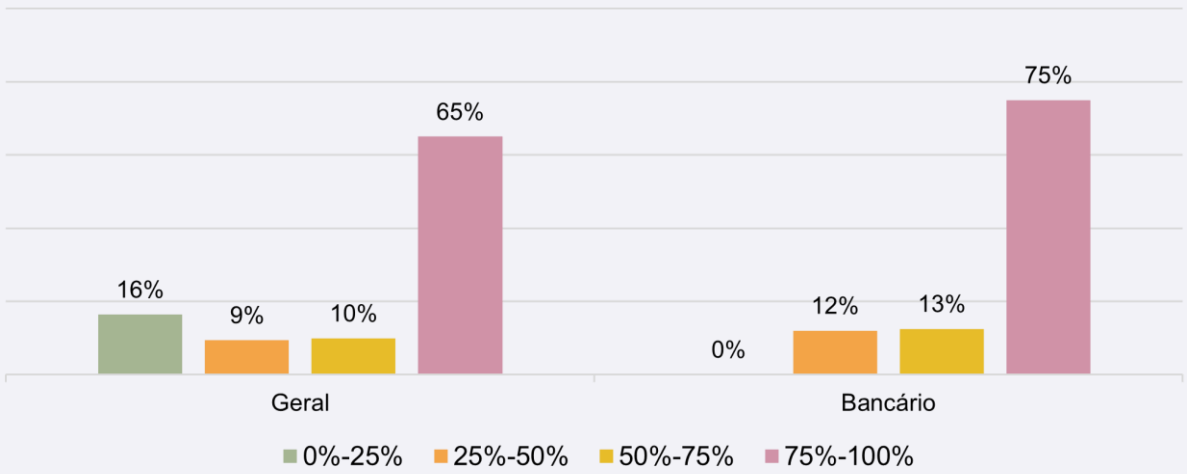
[36] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2023, 15-16.

Gráfico 59 - Percentagem de sistemas core em *cloud*



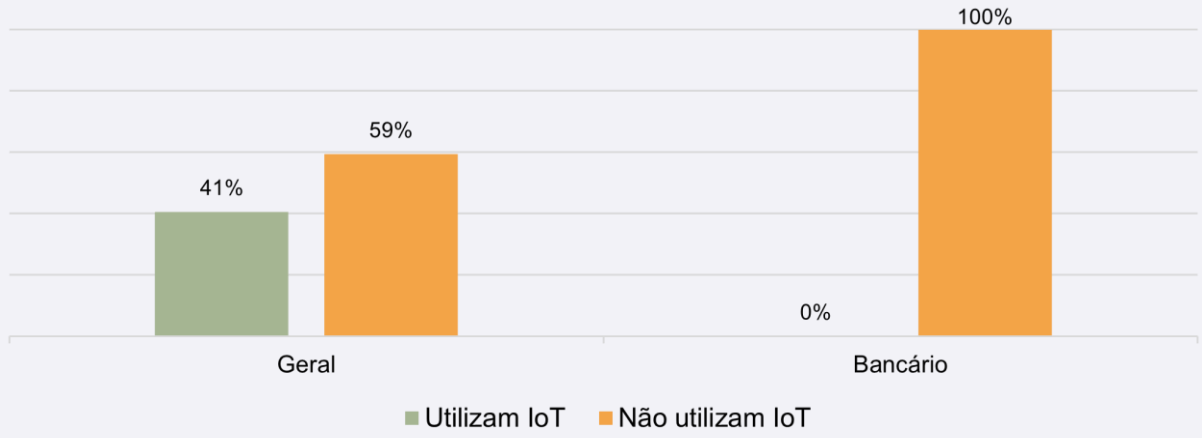
Genericamente, os operadores de serviços essenciais não procuram colocar os seus sistemas *core* na *cloud*. A percentagem de sistemas core em *cloud* não ultrapassa os 25% na maioria dos casos. No setor bancário registam-se ainda 25% de OSE no intervalo de 25%-50% a utilizar sistemas core em cloud.

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



Contrastando com o gráfico anterior, aqui se mostra a tendência dos operadores em manter os seus sistemas core no próprio ambiente da organização (*on-prem*) e não na *cloud*. De um modo geral, cerca de 60% dos operadores inquiridos referem que mantêm entre 75% a 100% de sistemas principais dentro do ambiente de TI da sua organização. No setor bancário prevalece a faixa de 75% a 100%, havendo ainda uma pequena percentagem no intervalo de 25%-50% e 50%-75% (12% e 13% respetivamente).

Gráfico 61- Utilização de IoT pelos OSE

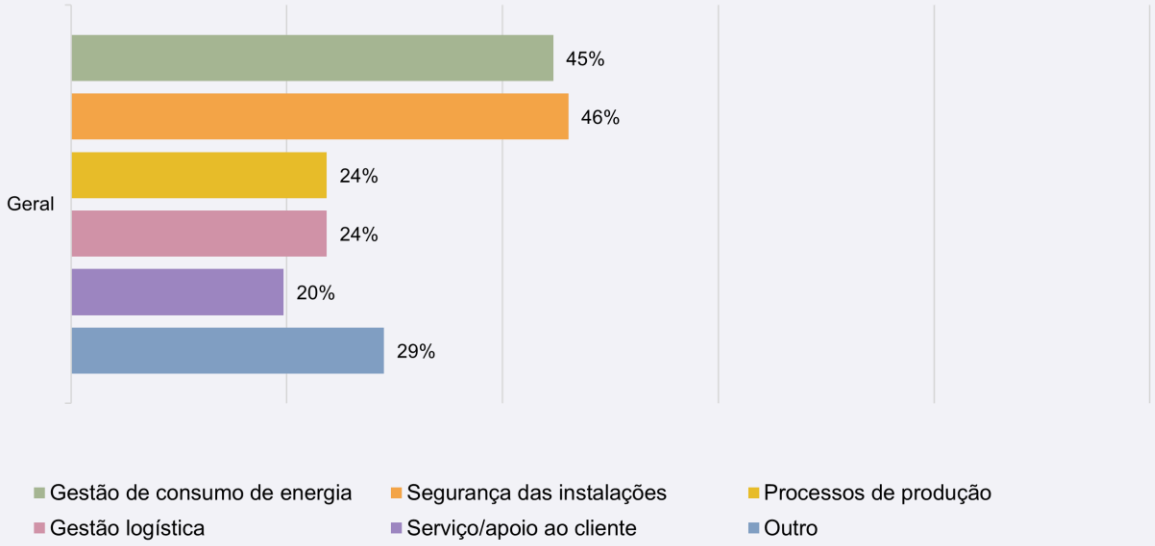


A maioria dos operadores (59%) não utiliza (ou ainda não utiliza) IoT. Destaca-se o setor bancário, onde a totalidade dos inquiridos respondeu não utilizar de todo IoT.

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

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

Gráfico 62 - Contextos de utilização de IoT



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

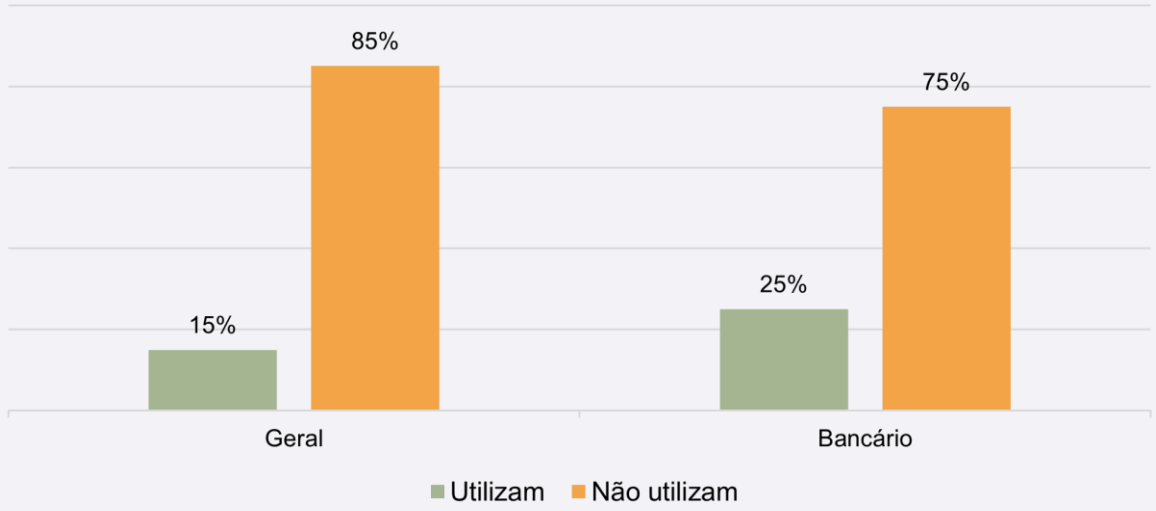
O mesmo estudo da ANACOM mencionado no gráfico anterior indica que "os equipamentos IoT foram sobretudo utilizados para segurança das instalações (86%), gestão do consumo de energia (32%), gestão logística (21%), processos de produção (19%), monitorização das necessidades de manutenção (18%) e serviço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

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

Gráfico 63 - Motivos pelos quais não utilizam IoT

São vários os motivos que fazem com que os operadores não utilizem IoT, desde os custos associados à incompatibilidade com sistemas em utilização, passando por vários outros. No entanto, o motivo mais evidente para a não utilização de IoT é não haver necessidade para tal no contexto de negócio ou organizacional (52%).
Na opção “Outros”, foi sobretudo indicado que se estava a preparar a implementação de IoT na organização para os anos de 2024 e 2025.
O setor bancário menciona ter dificuldades de perceção relativamente a consequências legais da sua utilização e não ter necessidade de IoT no contexto de negócio e organizacional.

Gráfico 64 - OSE que utilizam processos que recorrem a IA



A utilização ou o recurso à IA é ainda reduzido entre os OSE. Apenas 15% dos inquiridos referem já utilizar ou recorrer a IA dentro das suas organizações.
Por norma, há pouca utilização de processos com recurso a Inteligência Artificial (IA) por parte dos operadores. Tal é verificável em todos os setores. Contudo, é de salientar o setor da banca, no qual já se registam mais de 25% dos operadores a recorrer a Inteligência Artificial.

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

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

Gráfico 65 - Funções para as quais utilizam IA

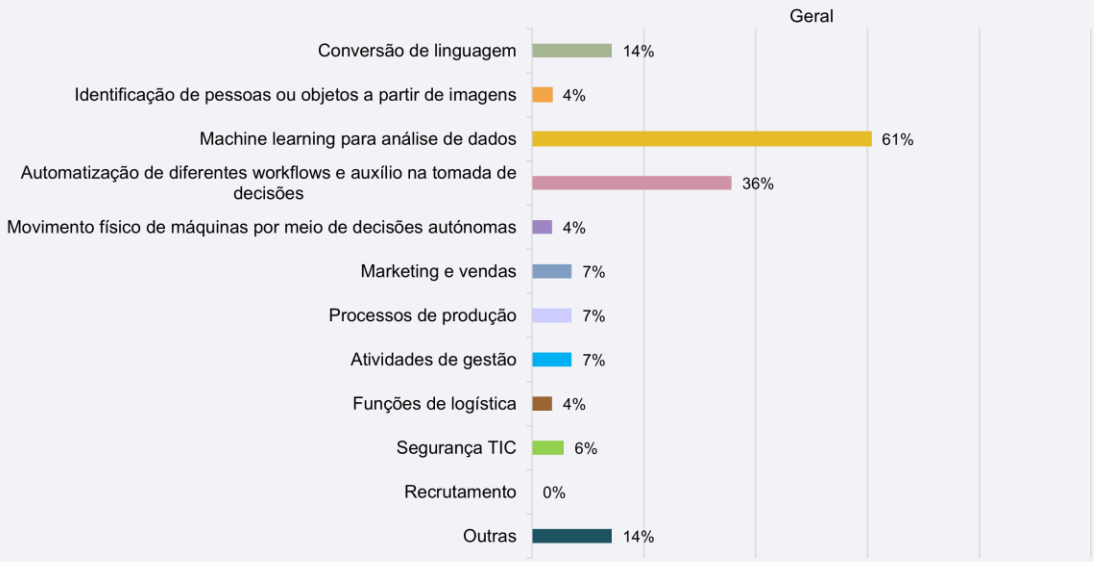
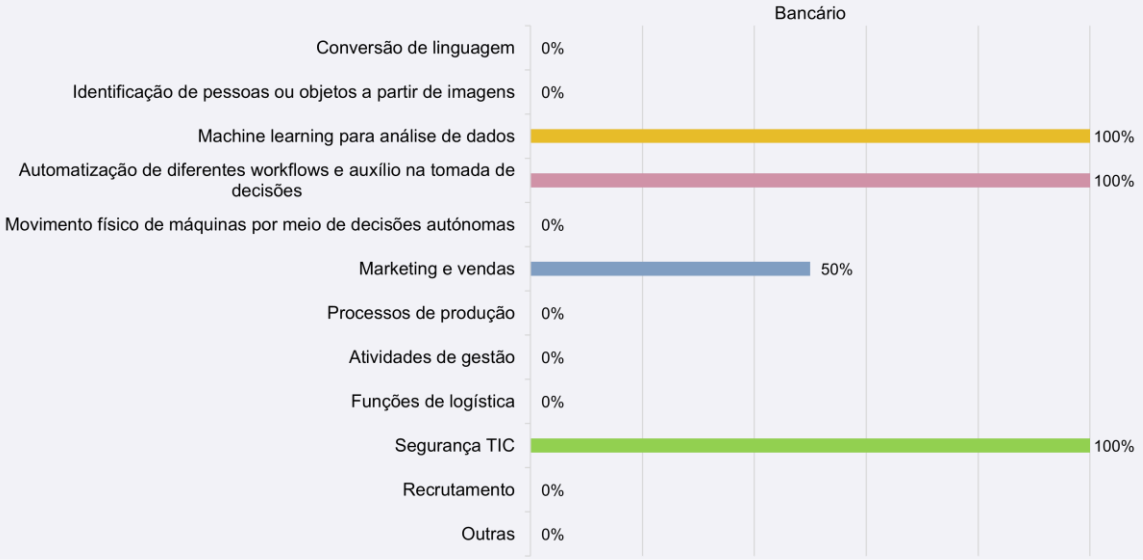


Gráfico 65.1 - Funções para as quais utilizam IA



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

apenas 15% ou menos dos OSE que já recorrem a IA. Curiosamente, não se registou o recurso a Inteligência Artificial em processos de recrutamento entre os OSE inquiridos.
No setor bancário a totalidade dos operadores inquiridos mencionaram utilizar IA em *machine learning* para análise de dados, na automatização de diferentes *workflows* e auxílio na tomada de decisões bem como na segurança TIC e apenas 50% mencionou utilizar IA para marketing e vendas.

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

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

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

Gráfico 66 - Medidas de proteção contra ameaças de cibersegurança

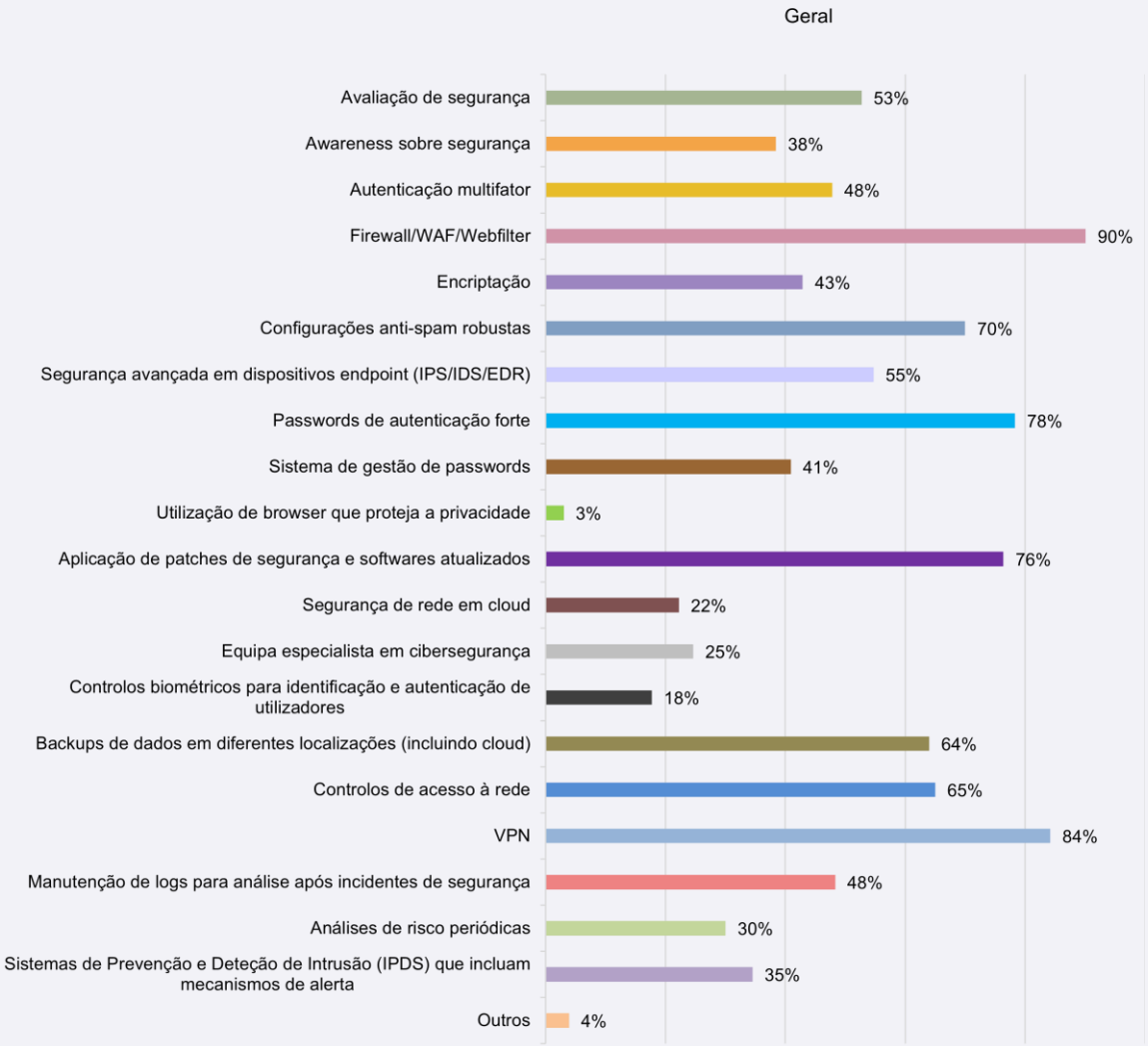
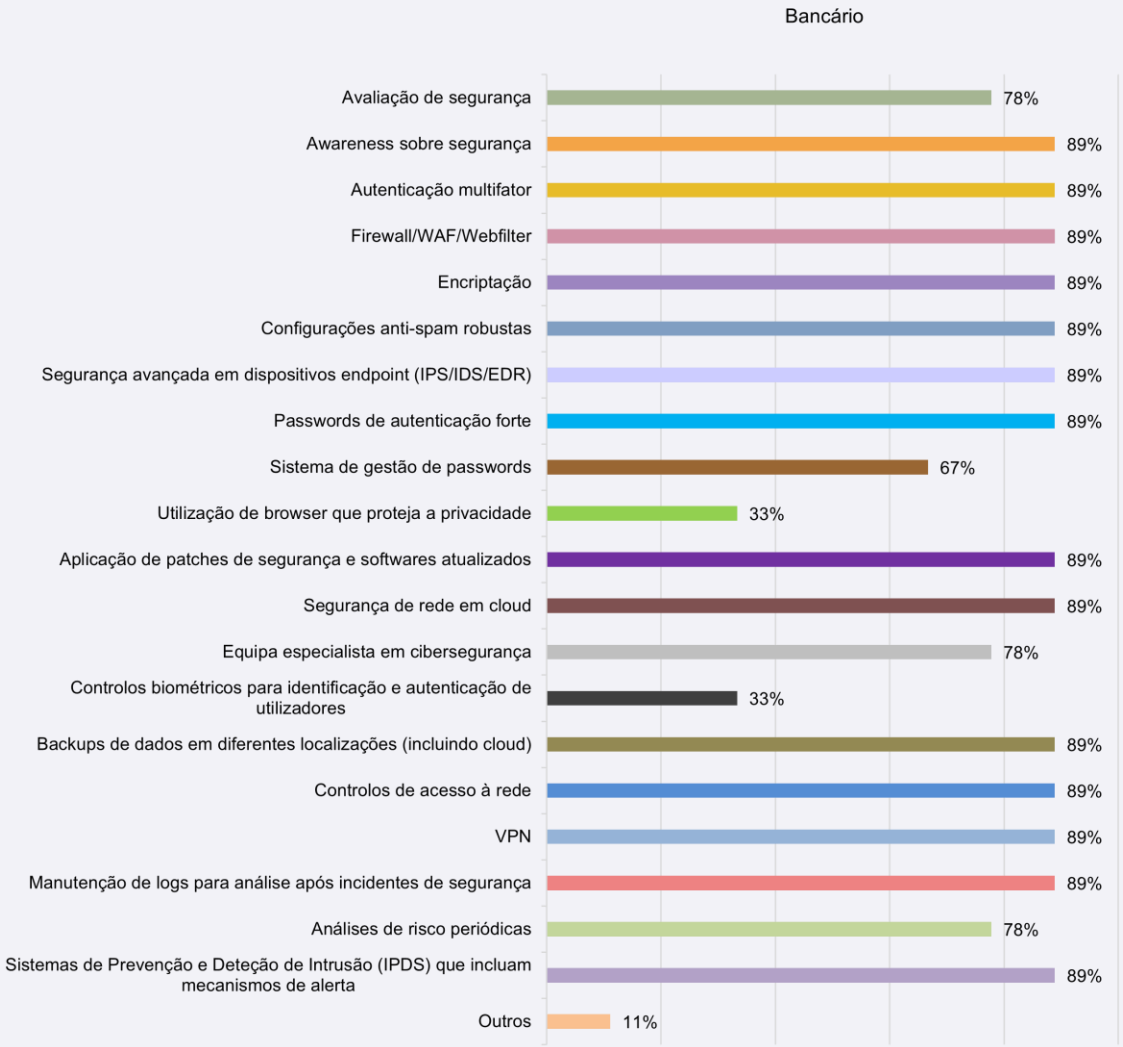


Gráfico 66.1 - Medidas de proteção contra ameaças de cibersegurança



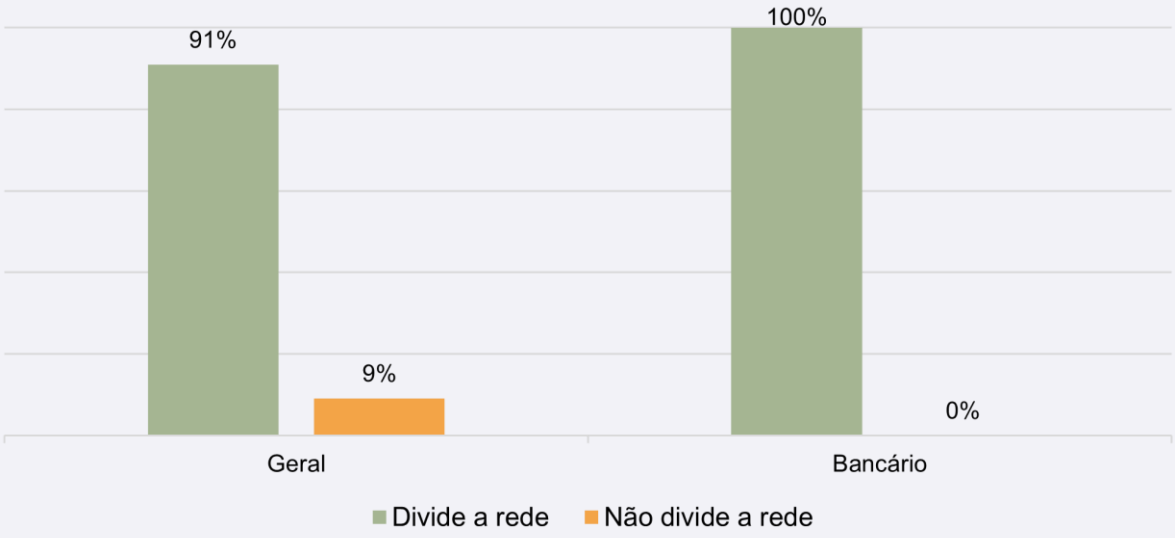
Na análise geral das medidas de segurança utilizadas pelos operadores, é possível verificar que medidas técnicas como a utilização de Firewall/WAF/Webfilter, utilização de VPN, palavras-passe de autenticação forte, aplicação de patches de segurança, a atualização dos softwares e backups de dados em diferentes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

Segundo o IUTICE de 2022, no que respeita às principais medidas de segurança das TIC utilizadas em 2021, 84,0% das empresas procedem à autenticação através de uma palavra-passe segura,

73,7% utiliza o *backup* de informação em local distinto (incluindo *backup* para a *cloud*), 62,5% efetua o controlo de acesso à rede (gestão dos direitos dos utilizadores na rede da empresa) e 53,8% conserva ficheiros de registo (histórico) que permitem a análise após incidentes de segurança das TIC. As restantes medidas de segurança utilizadas registam percentagens inferiores a 50%, sendo a autenticação através de métodos biométricos para aceder aos sistemas TIC da empresa a medida menos utilizada, com 12,3%[44].

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

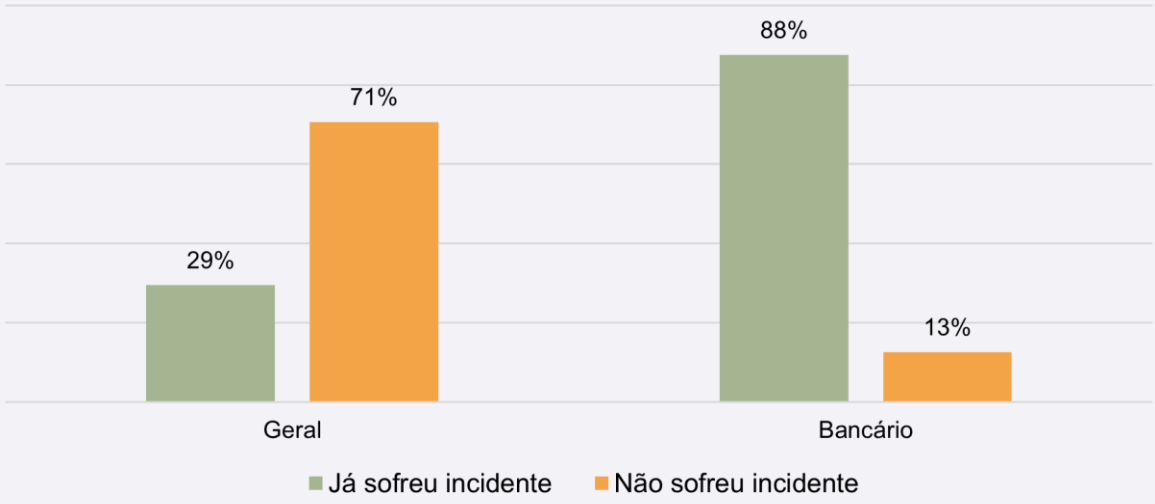
Gráfico 67 - Divisão entre rede dos colaboradores e rede para *guests*



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

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

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



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

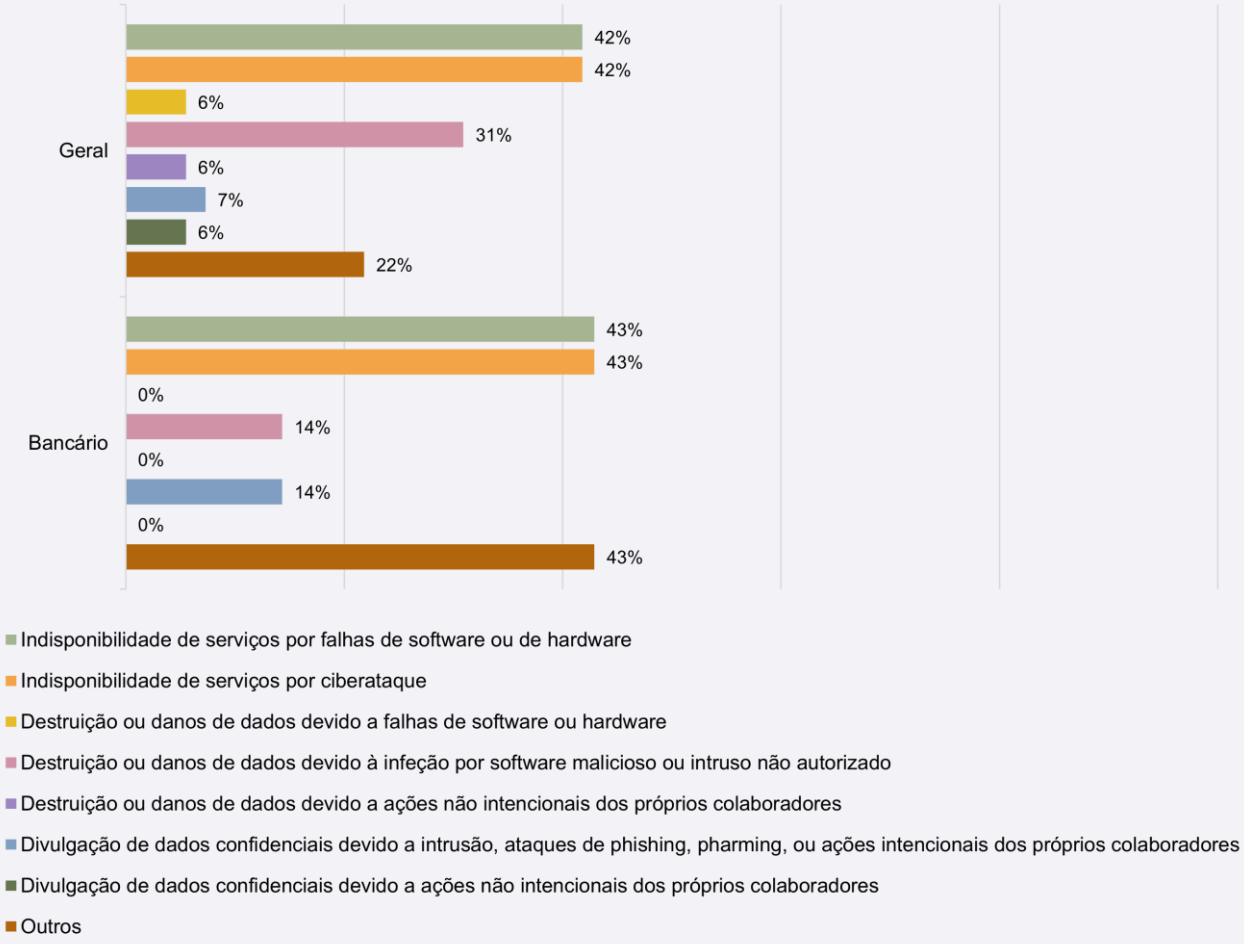
Sendo o IUTICE de 2022, Portugal registou a segunda menor proporção de empresas com incidentes de segurança das TIC na União Europeia (UE). Em 2021, 89,7% das empresas em Portugal, e 91,8% no total da UE, utilizaram pelo menos uma medida para garantir a integridade, a disponibilidade e a confidencialidade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

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

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

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

Gráfico 69 - Tipos de incidentes ocorridos



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

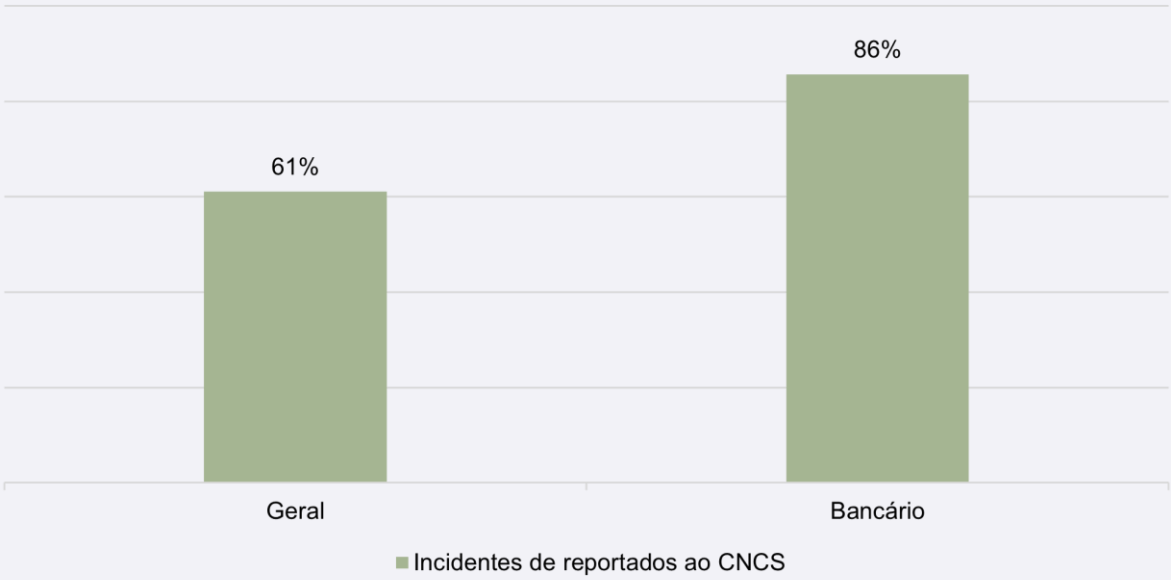
Nos "outros" incidentes ocorridos, referidos por os inquiridos que já sofreram incidentes, foram mencionados um acesso indevido a um computador empresarial na rede *guest*, fraude e compromisso dos prestadores de serviço, DDoS ou causados por terceiros bem como indisponibilidade de serviços por ataque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

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

se a destruição ou corrupção de dados devido a infeção de *software* malicioso ou intrusão não autorizada e devido a falhas de *hardware* ou *software* (2,1% e 1,8%, respetivamente)[48].

No estudo da Microsoft sobre o estado da cibersegurança em Portugal publicado em 2023, 70% dos inquiridos destaca o *phishing*, 63% dos inquiridos destaca os *softwares* maliciosos com cifragem de dados e pedido de resgate, 29% dos inquiridos destaca os ataques de negação de serviço DDoS pela sua capacidade de explorar vulnerabilidades nas redes e dispositivos programáveis da organização e, desta forma, perturbar os serviços e recursos das aplicações[49].

Gráfico 70 - Incidentes de cibersegurança reportados pelos OSE ao CNCS



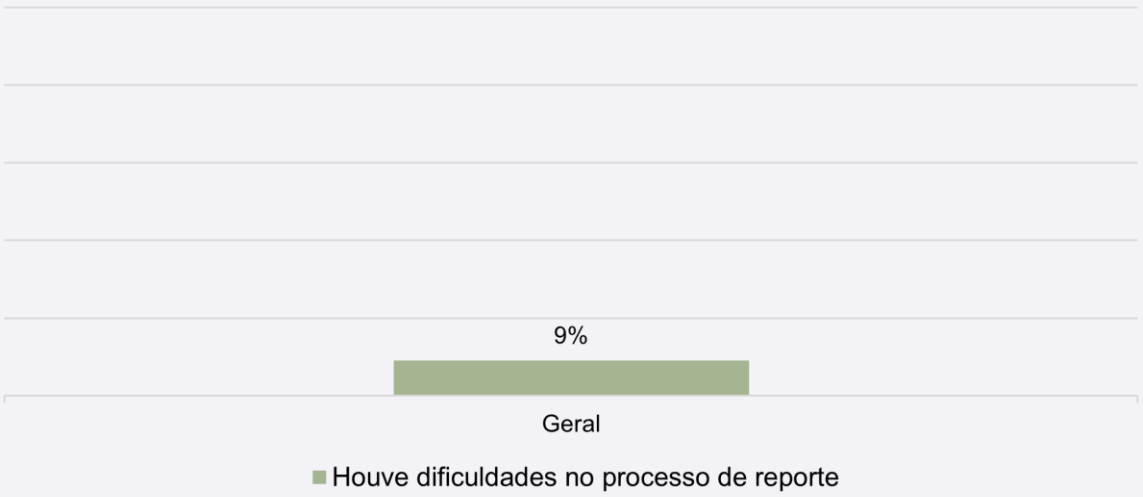
De forma geral, cerca de 60% dos operadores notificaram o CNCS dos incidentes sofridos. A não notificação de incidentes por quase 40% dos OSE, no entanto, não significa um incumprimento da sua parte. Segundo o disposto no n. º1 do artigo 16.º da lei n. º46/2018, de 13 de agosto, os OSE estão apenas obrigados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

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

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

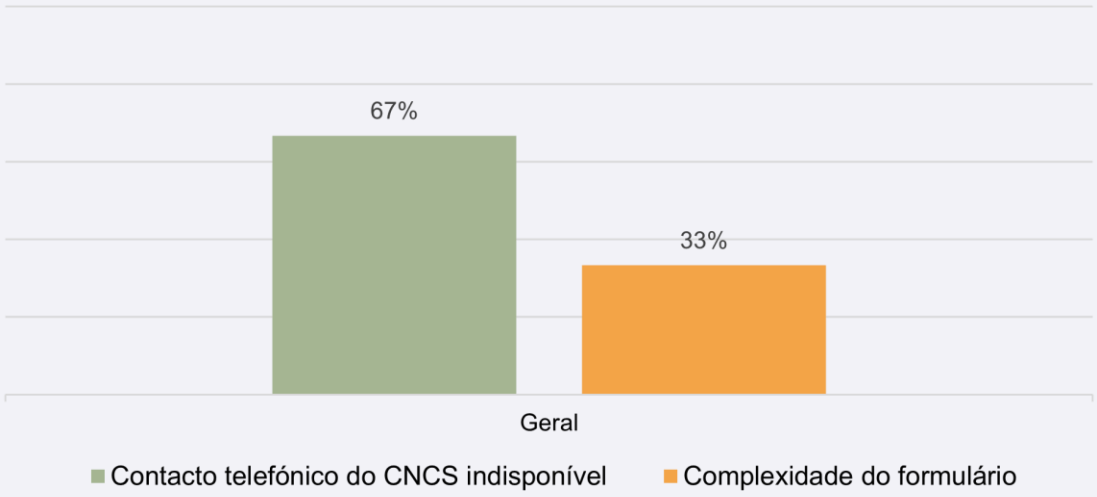
[49] Microsoft, "Estado da Cibersegurança em Portugal", 2023-2024, 6.

Gráfico 71 - Dificuldades no processo de notificação ao CNCS



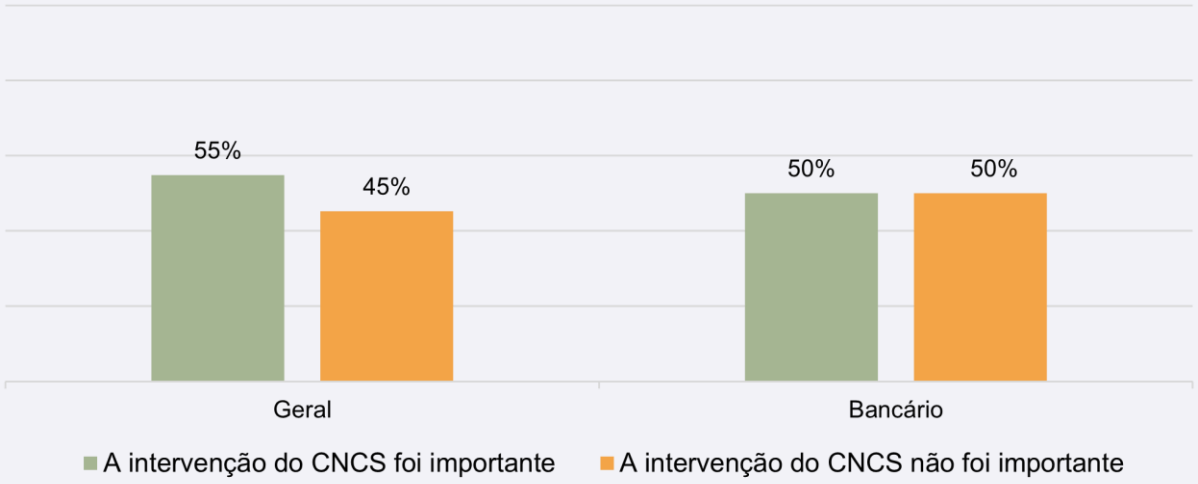
De modo geral, os operadores não tiveram dificuldades no processo de notificação de incidentes ao CNCS. No entanto, a nível geral, houve ainda cerca de 9% dos operadores a indicarem dificuldades na notificação. No setor da banca, não existiram dificuldades no processo de notificação ao CNCS.

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



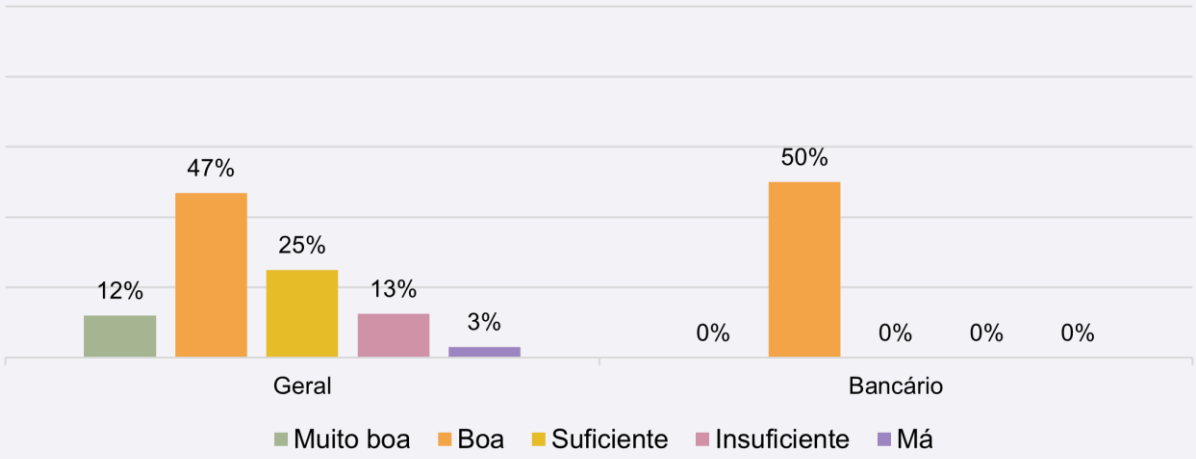
Entre os setores que identificaram dificuldades na notificação de incidentes ao CNCS, dois referiram que a principal dificuldade durante o processo de notificação foi a indisponibilidade do contacto telefónico e um atribuiu a principal dificuldade à complexidade do formulário de notificação. O setor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

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



A maioria dos operadores que notificou o CNCS de um incidente considerou que a intervenção deste foi importante na sua resolução (55%).
No setor bancário, metade dos inquiridos (50%) são da opinião que a intervenção do CNCS não foi relevante para a resolução do incidente notificado, enquanto a outra metade é da opinião que a intervenção foi importante.

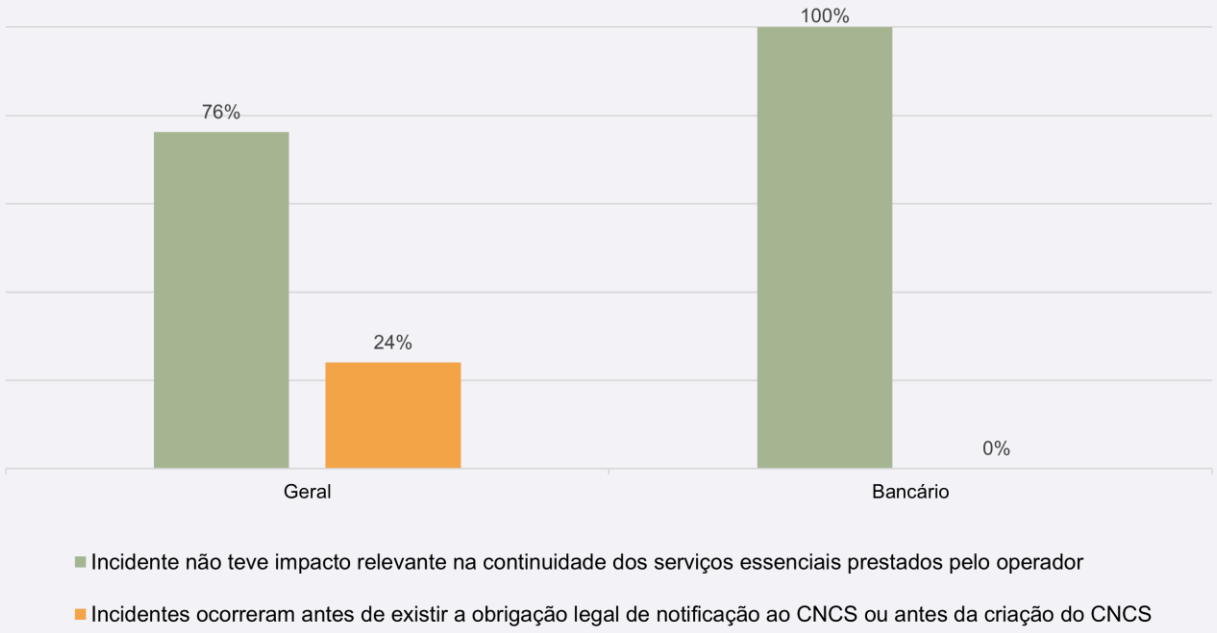
Gráfico 74 - Avaliação da resposta dada pelo CNCS



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

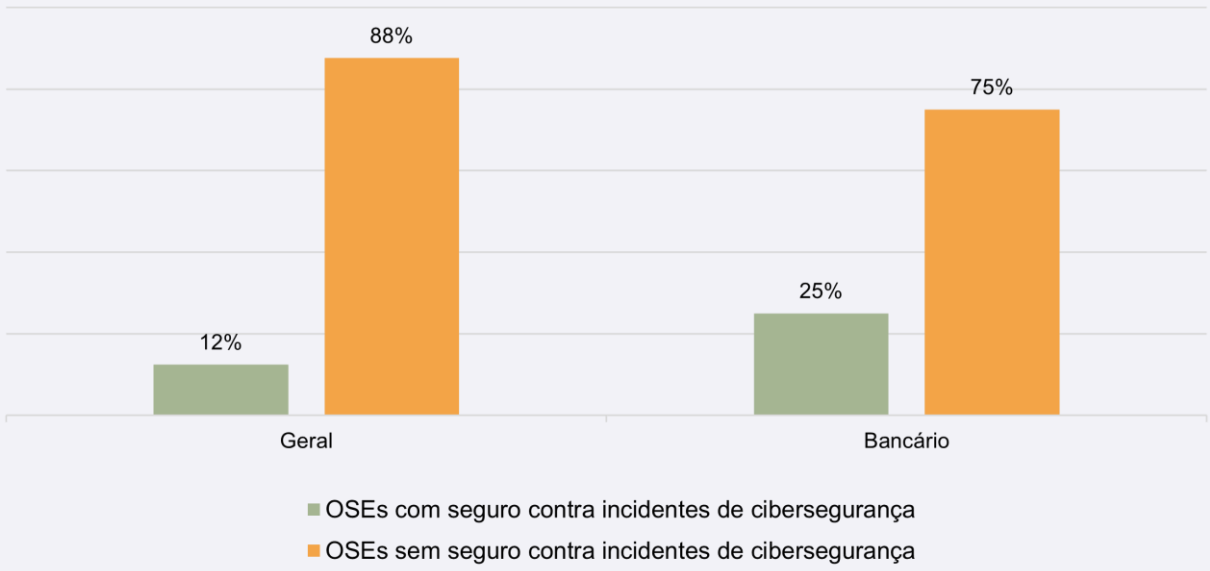
No setor bancário, a perspetiva geral é positiva. Os operadores afirmam a resposta ter sido ou boa (50%) ou suficiente (50%). Nenhum operador do setor classificou a resposta do CNCS como insuficiente ou má.

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



Como referido no **Gráfico 70**, a não notificação dos incidentes foi justificada. O principal motivo para a não notificação de incidentes de cibersegurança ao CNCS, segundo os OSE, foi o facto de o incidente não ter tido impacto na continuidade dos serviços essenciais por si prestados (76%). A totalidade dos inquiridos do setor bancário mencionou que o incidente não teve impacto.

Gráfico 76 - Seguro contra incidentes de cibersegurança

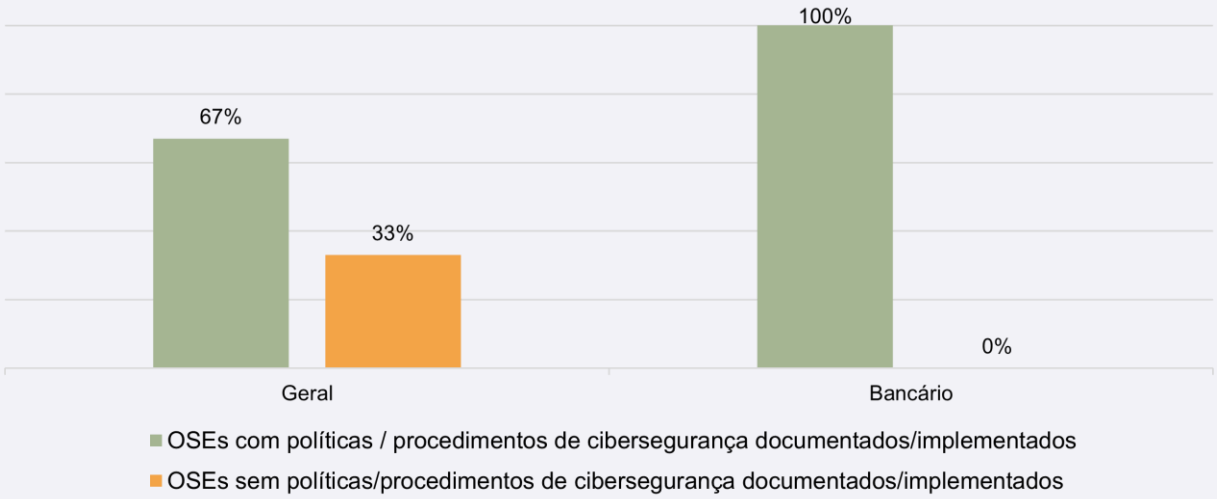


Verifica-se que cerca de 88% dos inquiridos não têm seguro contra incidentes de cibersegurança. A lógica geral mantém-se no setor bancário com a maior parte dos inquiridos a não possuírem este tipo de seguro.

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[50].

No inquérito elaborado pelo Fórum Económico Mundial, as empresas foram divididas em dois tipos: empresas com receita elevada e empresas com receita baixa, o que permite observar que as empresas do primeiro tipo tendem a adquirir seguros de cibersegurança - 75% das empresas com receita elevada fizeram-no. Já entre as empresas com receitas mais baixas, apenas cerca 25% destas adquiriram seguros de cibersegurança[51].

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

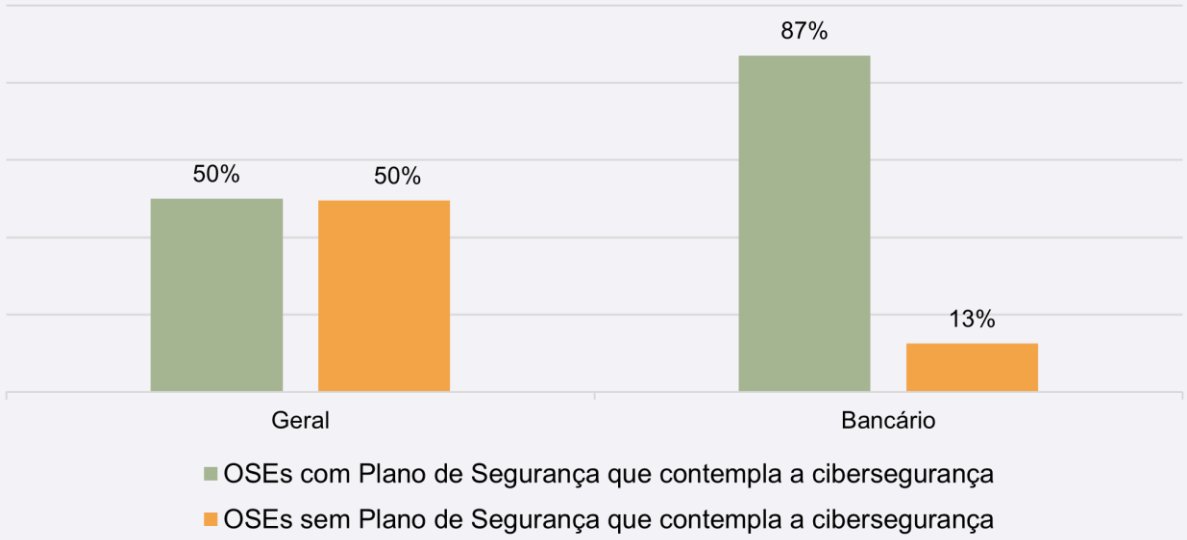


Dois terços (67%) dos operadores inquiridos referem ter políticas ou procedimentos de cibersegurança documentados e implementados. No setor bancário, todos os operadores referem ter políticas ou procedimentos de cibersegurança documentados ou implementados.

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

[50] ENISA, "NIS Investments", 2023, 16 e 24.
[51] Fórum Económico Mundial, "Global Cybersecurity Outlook 2024", 9.
[52] Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

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



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

No setor bancário, a maior parte dos operadores já tem um plano de segurança que contemple a área da cibersegurança.

Segundo um estudo realizado pela Microsoft, mais de 40% das empresas inquiridas têm projetado um investimento em cibersegurança. Destas empresas, cerca de 69% irá investir em avaliações regulares de risco de cibersegurança e 66% em auditorias de segurança e monitorização de ameaças em tempo real[53].

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

Gráfico 79 - Políticas incluídas no Plano de Segurança

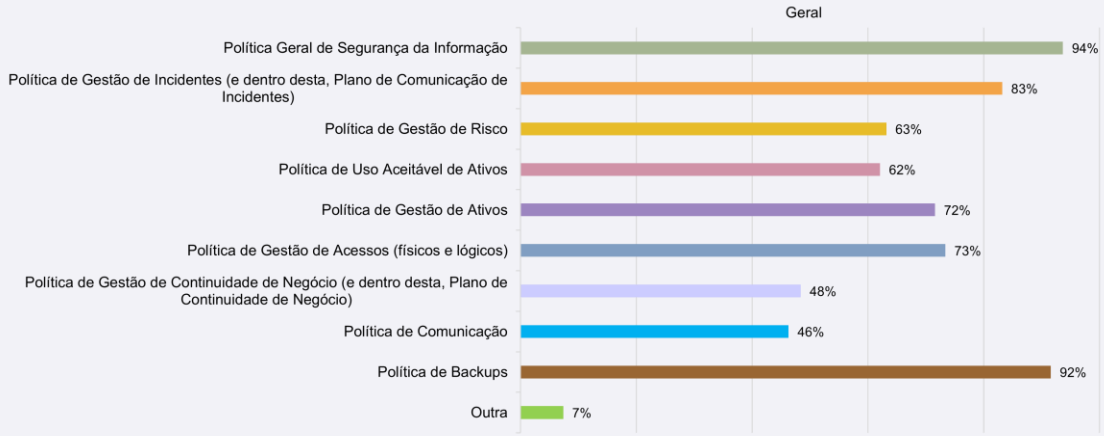
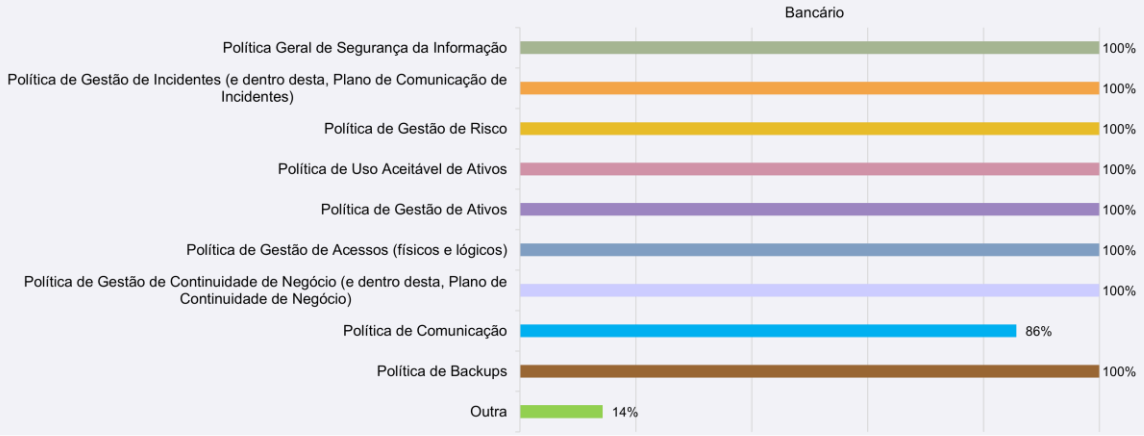
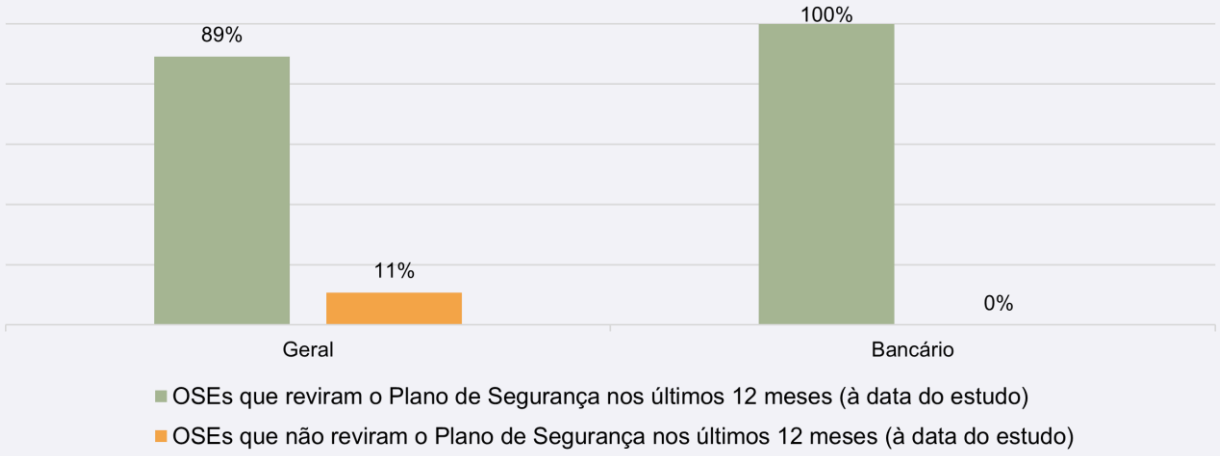


Gráfico 79.3 - Políticas incluídas no Plano de Segurança



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

Gráfico 80 - Revisão do Plano de Segurança



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

Segundo dados do IUTICE 2022, a maioria (61,7%) das empresas definiu ou fez uma revisão aos documentos sobre medidas, práticas ou procedimentos de segurança nos últimos 12 meses[54].

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

Mais de 60% dos operadores inquiridos dos diferentes setores referem realizar procedimentos de deteção e gestão de vulnerabilidades.
O setor bancário surge uma vez mais em destaque, uma vez que todos os operadores inquiridos realizam também procedimentos de deteção e gestão de vulnerabilidades.

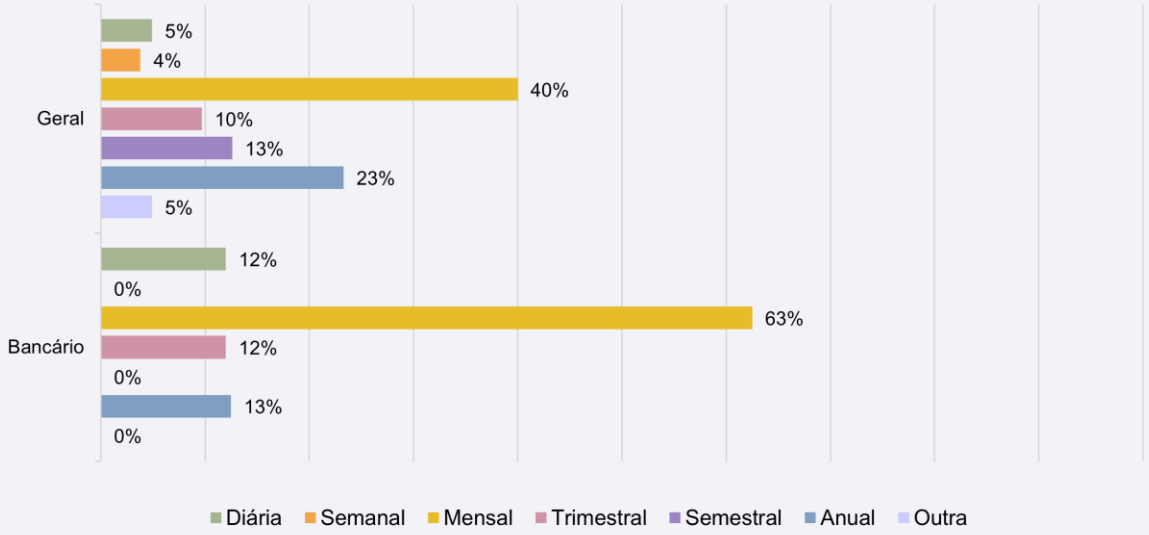
54 Instituto Nacional de Estatística, "Inquérito à Utilização das TIC nas Empresas", 2022, 19-20.

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

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

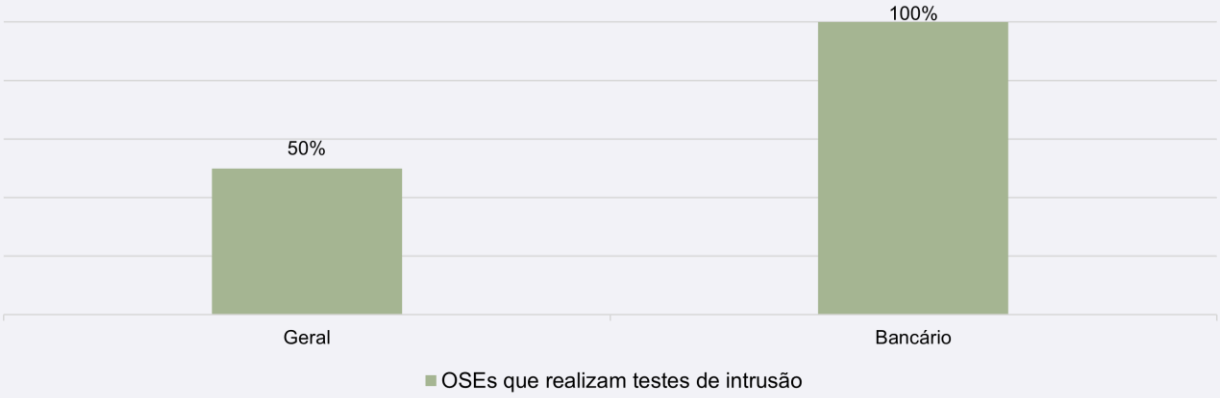
Sectorialmente, na banca, todos os operadores que já realizavam procedimentos de deteção e gestão de vulnerabilidades, fazem também a análise das mesmas.

Gráfico 83 - Frequência da análise de vulnerabilidades



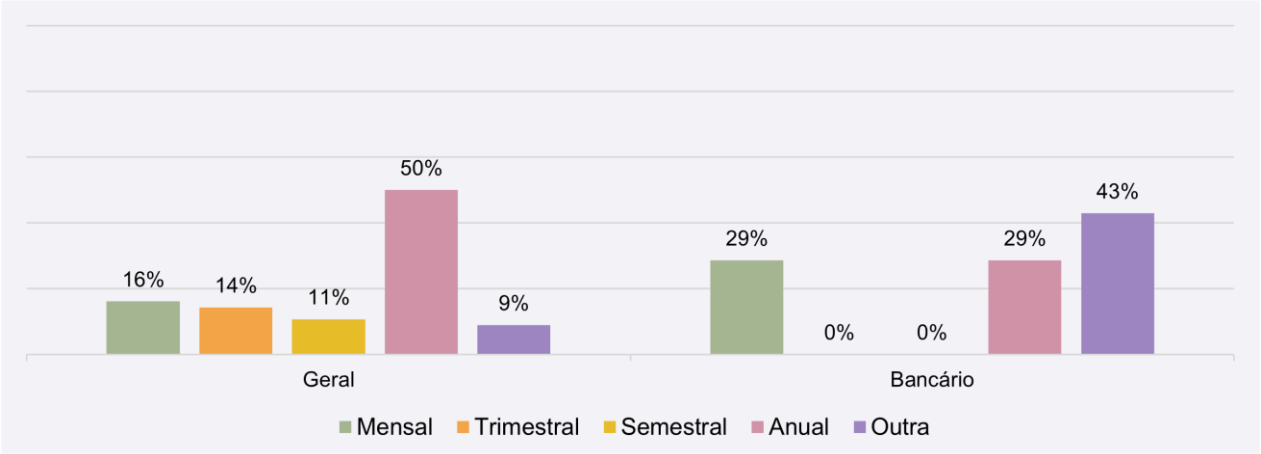
A frequência da análise de vulnerabilidades varia bastante entre os diferentes operadores e respetivos setores. Ainda assim, a frequência mais comum para a análise de vulnerabilidades entre os demais operadores é a frequência mensal, seguida da anual e semestral.
A frequência semanal e semestral é a menos observada, não tendo sido indicada por qualquer operador no setor bancário.

Gráfico 84 - Realização de testes de intrusão



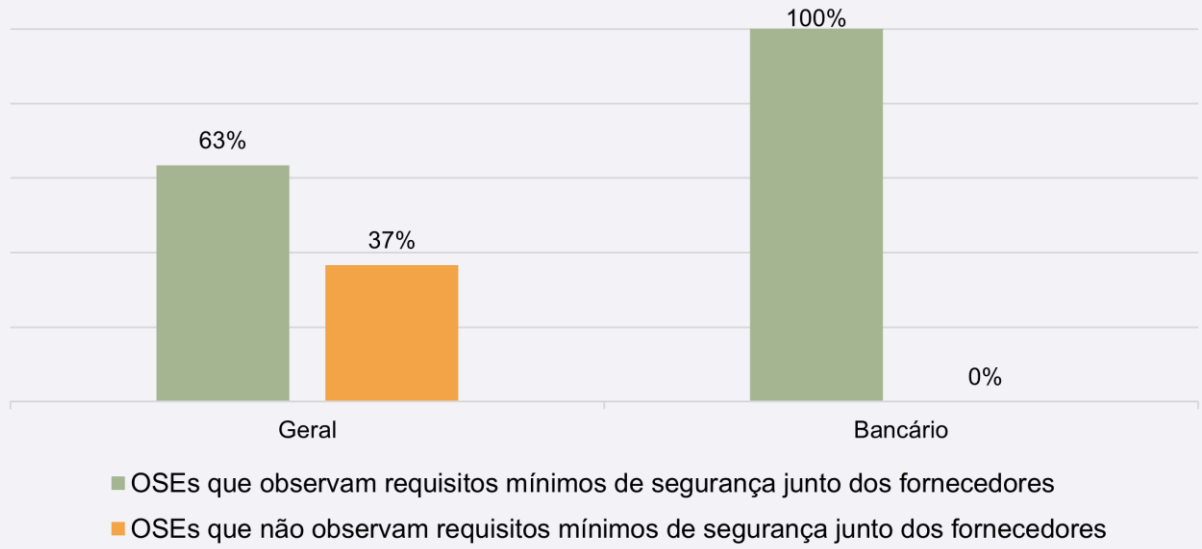
Na apreciação geral, é possível verificar uma igual divisão entre os operadores que realizam testes de intrusão e os que não realizam esses testes (50%-50%).
Há que destacar o setor bancário, onde todos os inquiridos referiram realizar testes de intrusão.

Gráfico 85 - Frequência de testes de intrusão



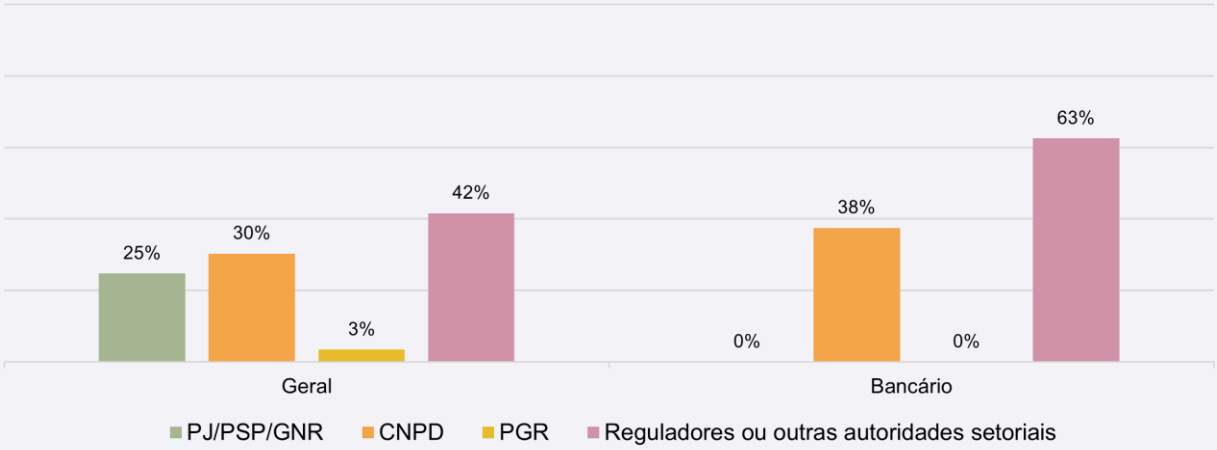
Com exceção dos operadores de serviços essenciais do setor bancário, os operadores dos setores tendem a realizar testes de intrusão anualmente.
Entre os inquiridos, uma minoria realiza testes de intrusão pelo menos trimestralmente, sendo que a maioria realiza mensalmente ou de forma ainda mais frequente, para que os testes possam ser realizados por secções ou áreas da organização.
Por sua vez, no setor bancário, 43% indicou realizar testes de intrusão com uma frequência também superior à mensal porque há operadores que os realizam de forma contínua, operadores que conduzem estes testes sempre que as versões das aplicações utilizadas são atualizadas e operadores que realizam estes testes sempre que novos ativos são introduzidos.
Nos restantes setores, embora prevaleça a periodicidade anual para estes testes, é possível verificar operadores a optar por períodos mais curtos entre cada momento de teste.

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



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

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



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

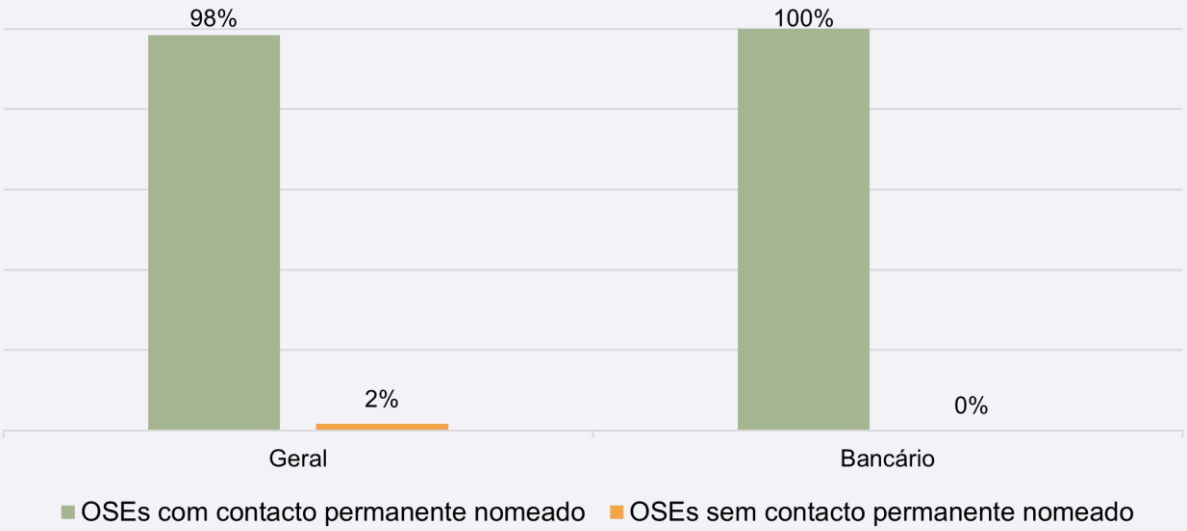
Apenas uma quantidade muito reduzida dos operadores tem previsto fazer qualquer tipo de notificação à Procuradoria-Geral da República (PGR).

A Comissão Nacional de Proteção de Dados (CNPD) surge em 2º lugar nas intenções de notificação em caso de ciberataque/incidente dos inquiridos, estando em 3º lugar as intenções de notificação à PJ/PSP/GNR.

Em caso de ciberataque os OSE concordam em contactar, para além do CNCS, os reguladores ou outras entidades setoriais. Verifica-se que contactar a PGR foi a opção com menos destaque seguida do CNPD.

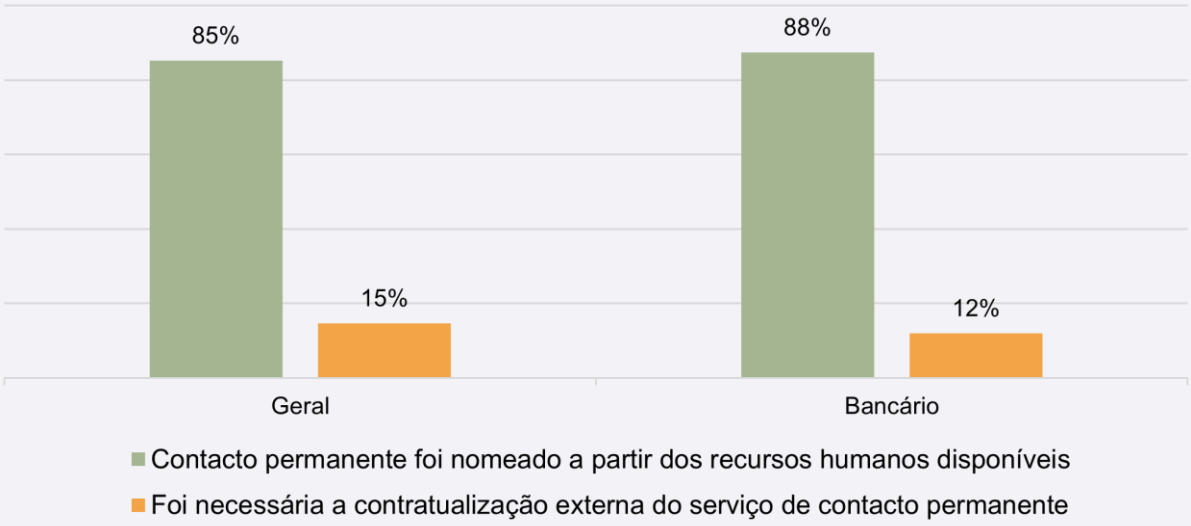
O setor da banca privilegia a notificação aos reguladores ou outras entidades setoriais em caso de ciberataque ou incidentes bem como a CNPD.

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



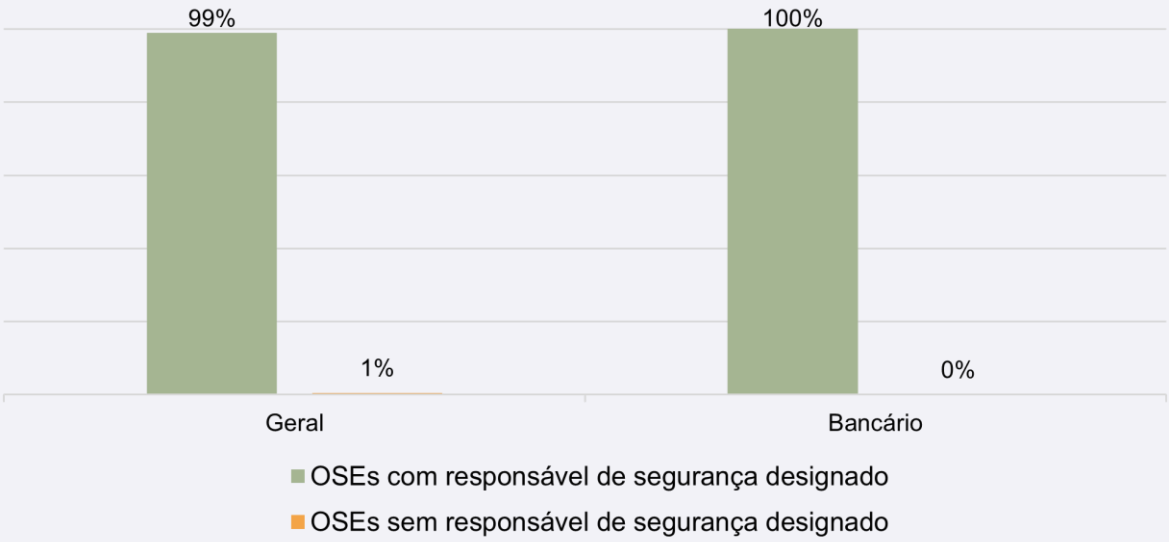
Cerca de 98% dos operadores inquiridos têm o seu contacto permanente com o CNCS nomeado. No setor inquirido em questão a totalidade dos operadores apresenta contacto permanente nomeado.

Gráfico 89 - Designação do contacto permanente



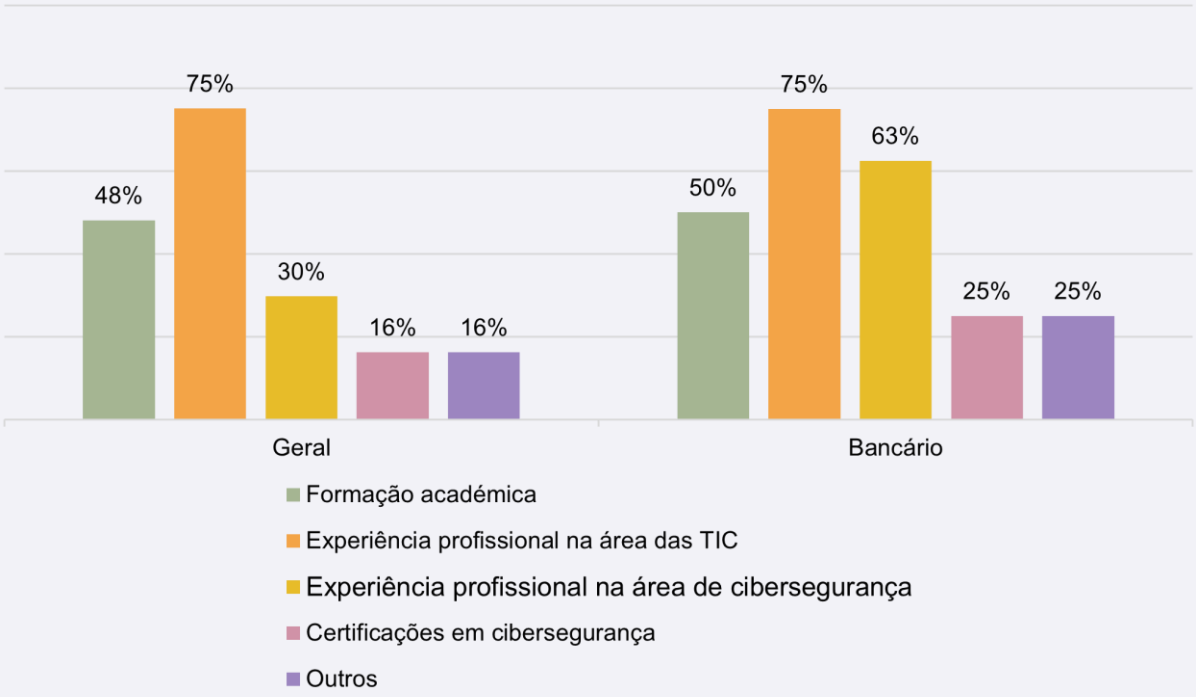
A vasta maioria dos operadores (85%) designou como contacto permanente alguém que já fazia parte da organização. No entanto, houve ainda alguns operadores que tiveram de recorrer à contratualização externa do serviço de contacto permanente, sendo o setor bancário um deles.

Gráfico 90 - Designação do responsável de segurança



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

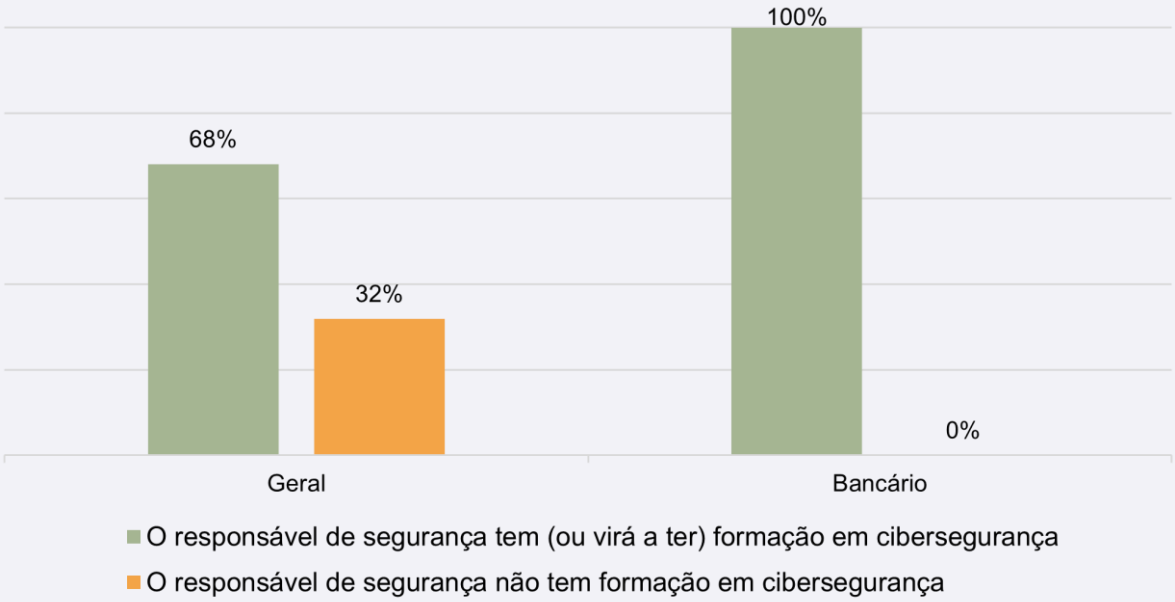
Gráfico 91 - Critérios utilizados para a designação do responsável de segurança



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

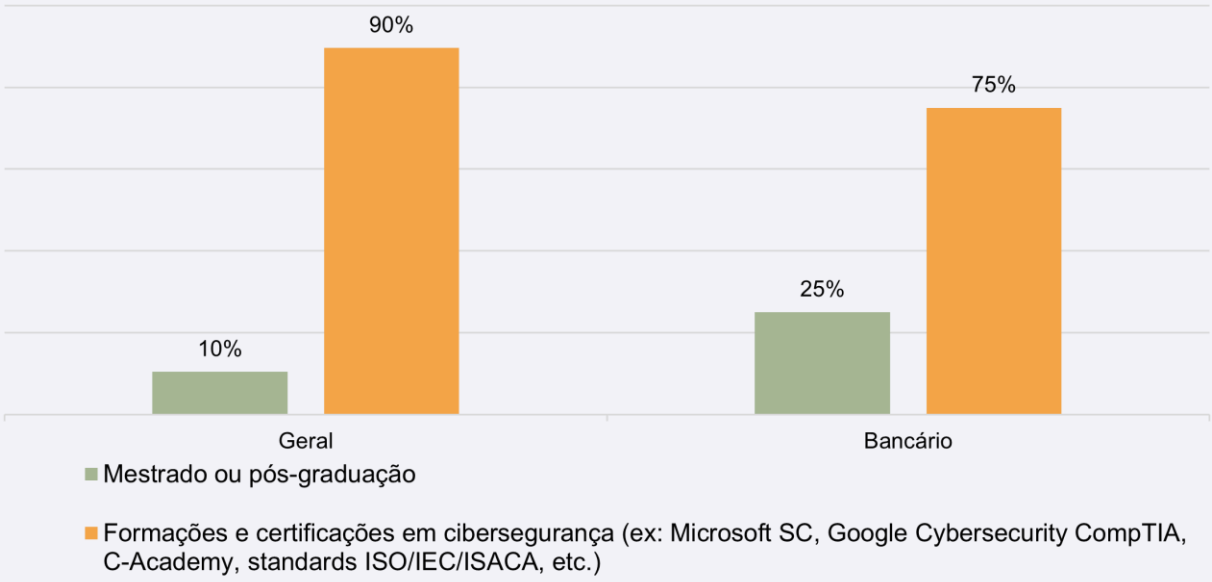
É também importante referir que se verificaram casos em que os critérios para a designação do responsável de segurança pouco se prenderam com a formação académica ou experiência profissional do mesmo, tendo este sido designado, por exemplo, por ser o responsável máximo da organização ou presidente de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

Gráfico 92 - Formação específica de cibersegurança do responsável de segurança



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

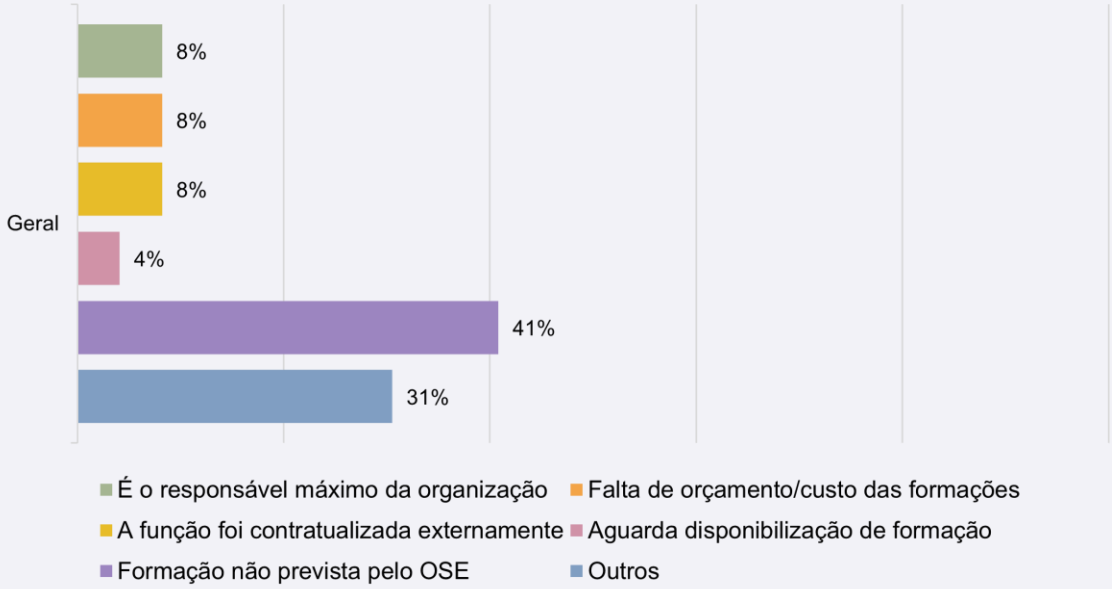
Gráfico 93 - Tipo de formação específica em cibersegurança



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

No setor da banca os responsáveis de segurança com mestrado ou pós-graduação em cibersegurança estabelecem-se acima dos 25%.

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



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

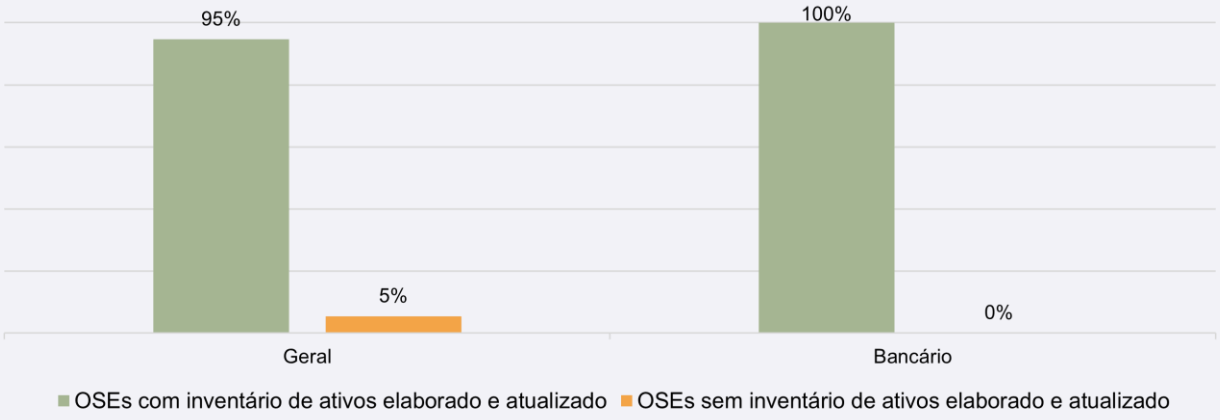
Em segundo lugar, surge a resposta "outros", dada por cerca de 30% dos OSE onde o responsável de segurança não tem formação em cibersegurança. Entre esses "outros" motivos, encontram-se explicações tais como a falta de oportunidade ou disponibilidade de realizar a formação; tentativas de incluir formação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

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

O motivo menos frequente foi a espera pela disponibilização da formação, indicado em menos de 5% dos casos. Como no setor bancário todos os operadores mencionam ter formação em cibersegurança a questão não se aplica.

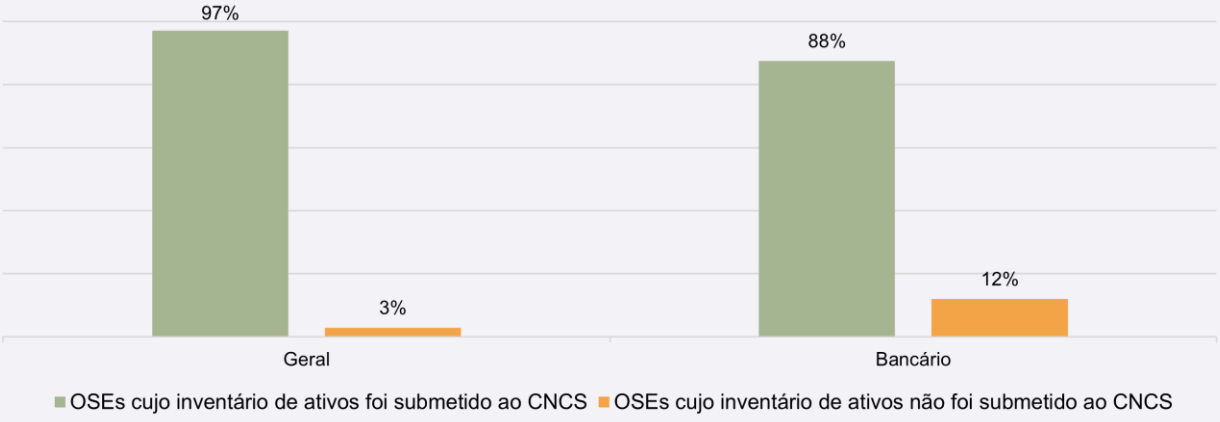
Tal como referido anteriormente, o Centro Nacional de Cibersegurança lançou um desafio denominado "Compromisso C-Academy" que consiste em fornecer um programa de formação avançada em cibersegurança para a administração pública e o setor privado. Através deste programa é possível aos responsáveis de segurança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

Gráfico 95 - Inventário de ativos essenciais elaborado e atualizado



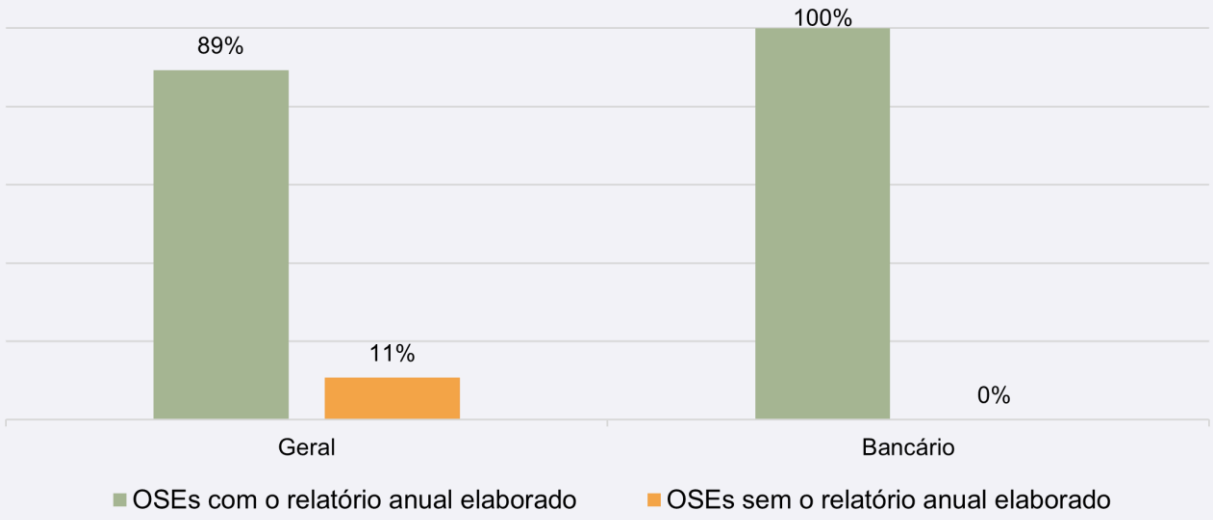
A larga maioria dos operadores inquiridos (95%) tem elaborado e atualizado o seu inventário de ativos essenciais. No setor da banca, todos os operadores têm o seu inventário elaborado e atualizado.

Gráfico 96 - Submissão do inventário de ativos ao CNCS



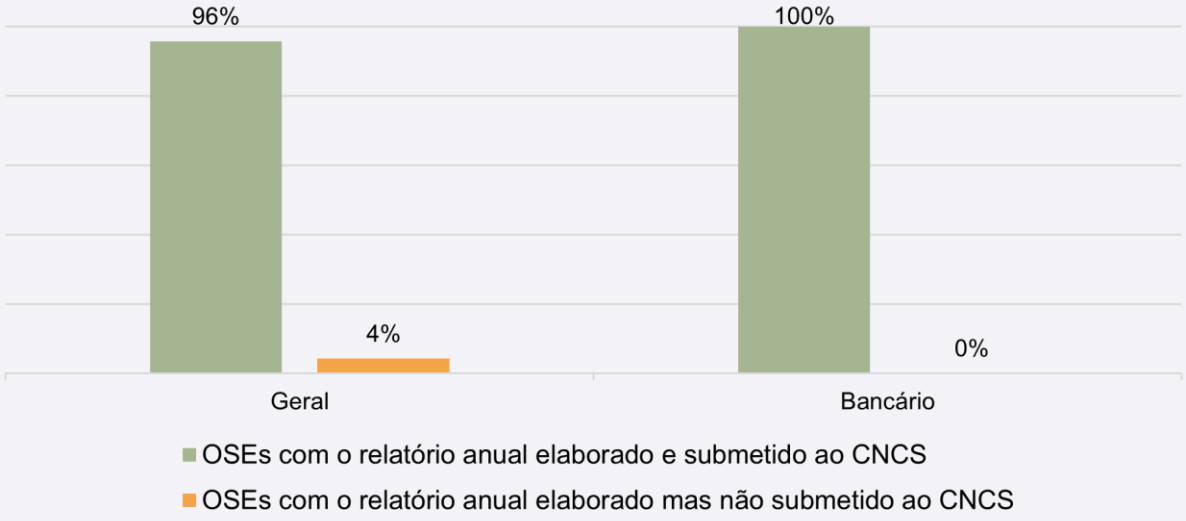
Verifica-se elevada conformidade relativamente à submissão do inventário de ativos essenciais ao CNCS por parte dos operadores que elaboraram esse inventário. 97% dos operadores que elaboraram o seu inventário de ativos submeteram-no ao CNCS em 2023. No setor bancário, 12% não submeteu o inventário.

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



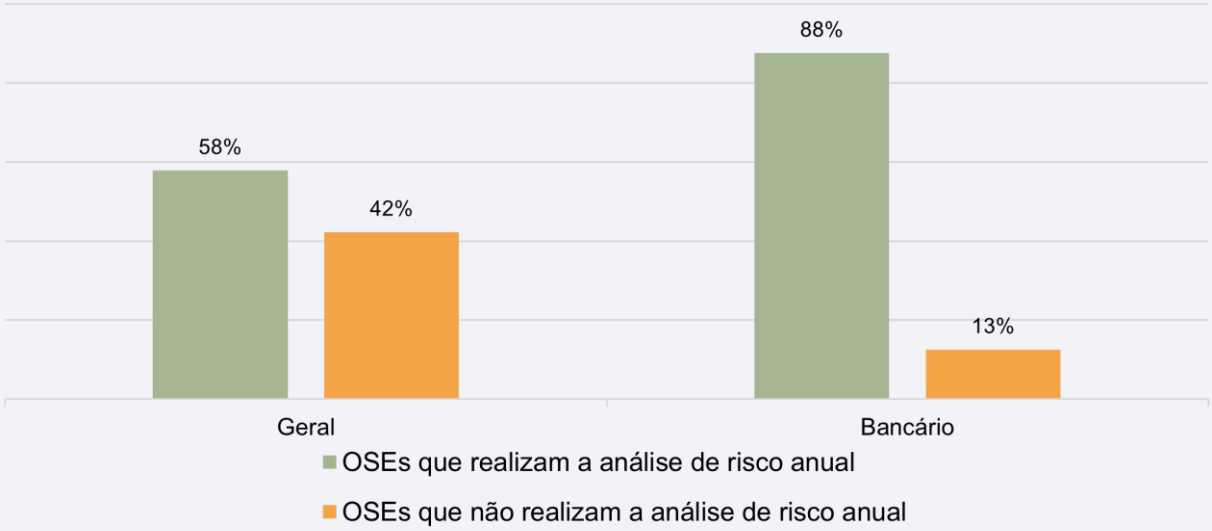
Em termos gerais, 89% dos operadores de serviços essenciais elaboram o relatório anual exigido pelo decreto-lei n.º 65/2021. O setor bancário é um dos únicos onde a totalidade dos operadores refere ter elaborado o relatório anual.

Gráfico 98 - Submissão do relatório anual ao CNCS



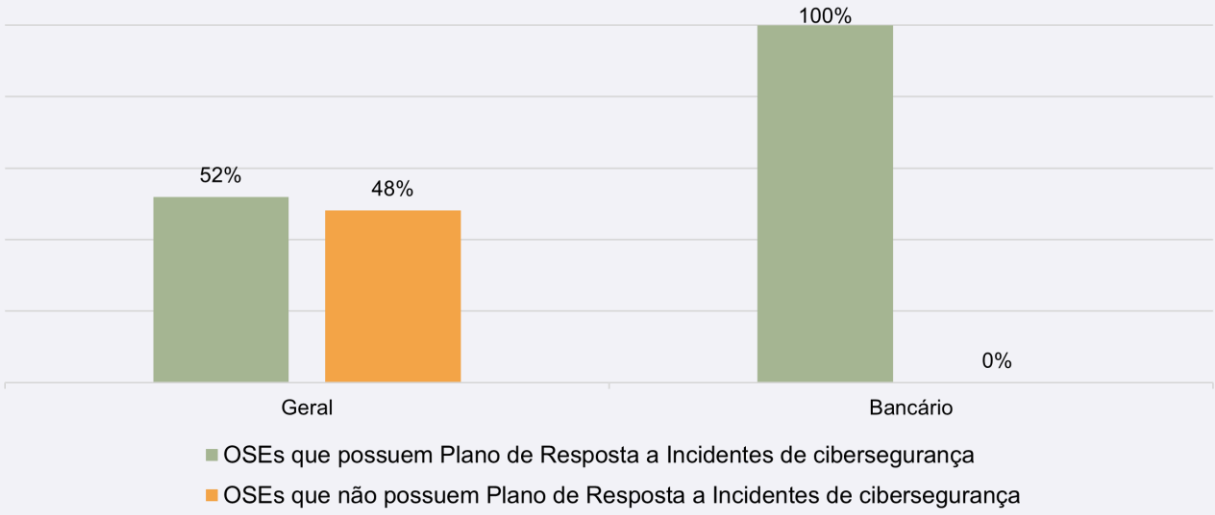
Entre os operadores que elaboraram o relatório anual exigido pelo decreto-lei, 97% submeteram-no ao CNCS. O bancário volta a ser novamente um dos únicos onde todos os operadores com relatório elaborado submeteram o mesmo ao CNCS.

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



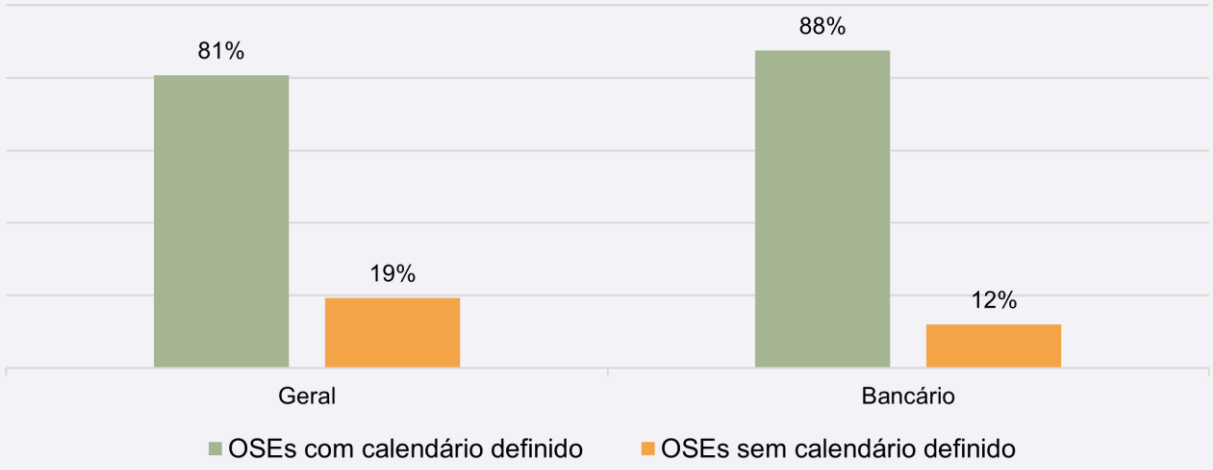
A realização anual de uma análise dos riscos relativos a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação utilizados pelos operadores de serviços essenciais é uma outra obrigação legal decorrente do decreto-lei n.º 65/2021. Apesar de esta análise de risco anual ter caráter obrigatório, cerca de 42% dos operadores não a realizam. No setor bancário, 88% dos OSE realiza a analise de risco anual.

Gráfico 100 - Plano de Resposta a Incidentes de Cibersegurança



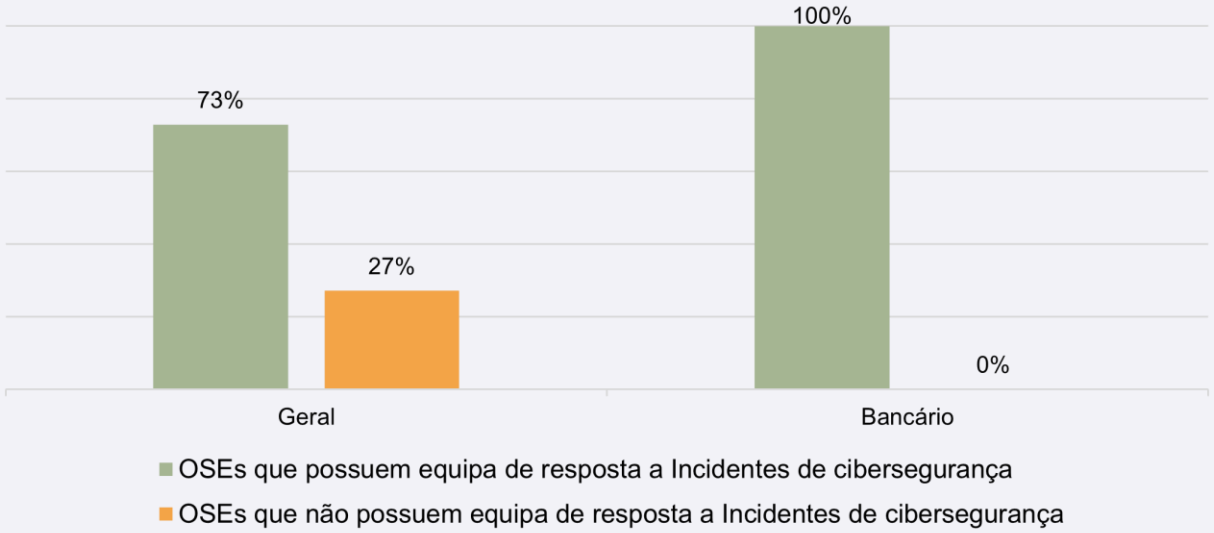
Somente pouco mais da metade dos operadores inquiridos (52%) indicou ter estabelecido um plano de resposta a incidentes de cibersegurança. Novamente, destaca-se o setor, no qual todos os inquiridos indicam possuir esse plano.

Gráfico 101 - Definição de calendário para cumprimento das obrigações decorrentes do decreto-lei n. º 65/2021, de 30 de julho



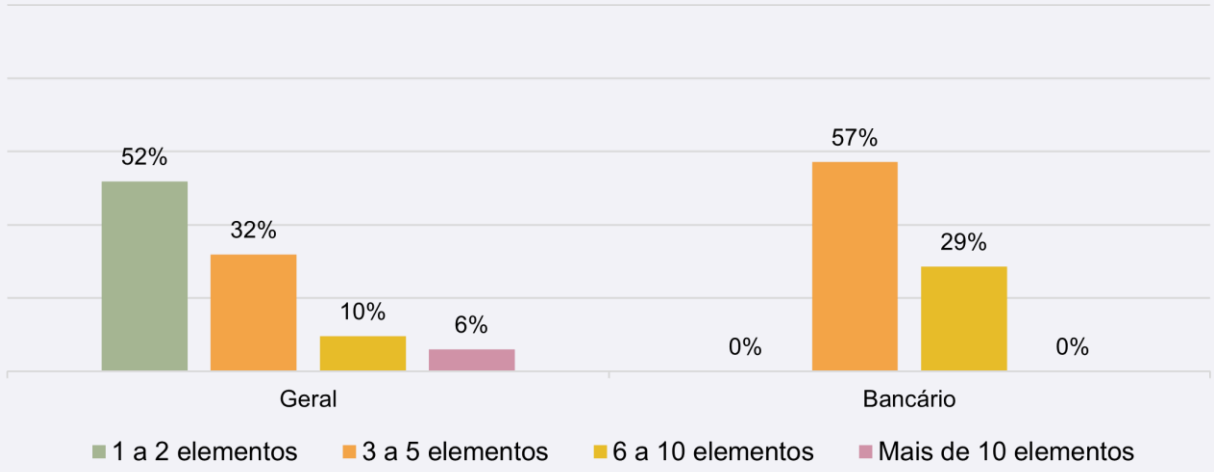
A vasta maioria dos operadores (81%) procura definir um calendário para os auxiliar no cumprimento das obrigações constantes do decreto-lei n.º 65/2021. No setor da banca, 12% dos operadores não define esse calendário. Há que salientar ainda que, tal como revelam os gráficos anteriores, mesmo com calendário definido, existem situações em que os operadores não elaboraram ou submeteram o seu inventário de ativos essenciais ou o seu relatório anual, como, por exemplo, no setor da energia.

Gráfico 102: Equipa de resposta a incidentes de cibersegurança



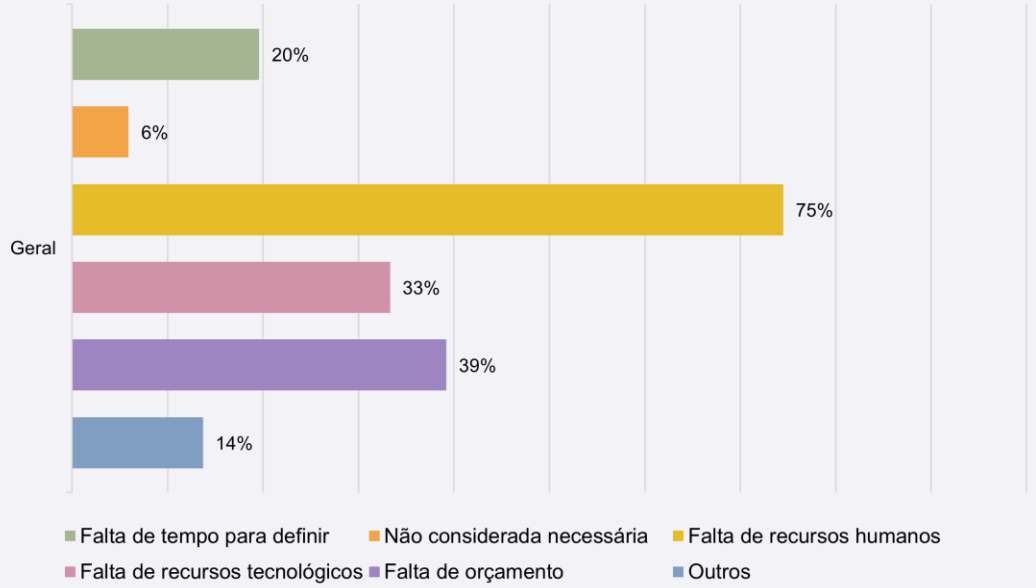
A nível geral, 73% dos operadores possuem equipa de resposta a incidentes de cibersegurança. A nível setorial, a percentagem de operadores que possui tal equipa é sempre superior a 60%. Destaca-se, mais uma vez, o setor bancário, onde todos os operadores inquiridos possuem equipa de resposta a incidentes de cibersegurança.

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



Na visão geral, 55% dos operadores com equipa de resposta a incidentes de cibersegurança conta com equipas compostas por 1 a 2 elementos. A nível setorial, O setor bancário é um dos setores nos quais a maioria das equipas de resposta dos operadores são compostas por 3 a 5 elementos (57%) e 6 a 10 elementos (29%), não apresentando equipas de 1 a 2 elementos nem de mais de 10 elementos.

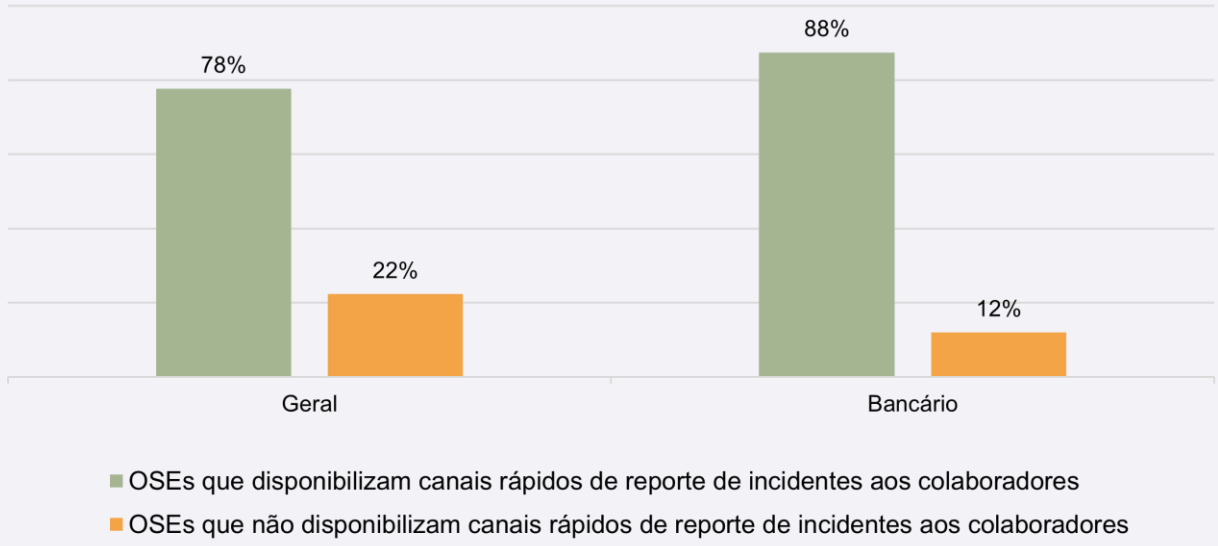
Gráfico 104 - Motivos para a não existência de equipa de resposta a incidentes de cibersegurança



O principal motivo para que os operadores não tenham equipa de resposta a incidentes de cibersegurança é a falta de recursos humanos, de acordo com 75% dos OSE que não possuem tal equipa. A falta de orçamento é o segundo motivo com maior prevalência, tendo sido apontado por quase 40% dos operadores sem equipa de resposta a incidentes. A falta de orçamento como um impedimento para que se possua equipa de resposta a incidentes é indicado por 50% dos operadores sem equipa, embora este motivo continue a figurar atrás da falta de recursos humanos. Por sua vez, a falta de recursos tecnológicos é apontada como motivo por um terço dos operadores sem equipa de resposta a incidentes.

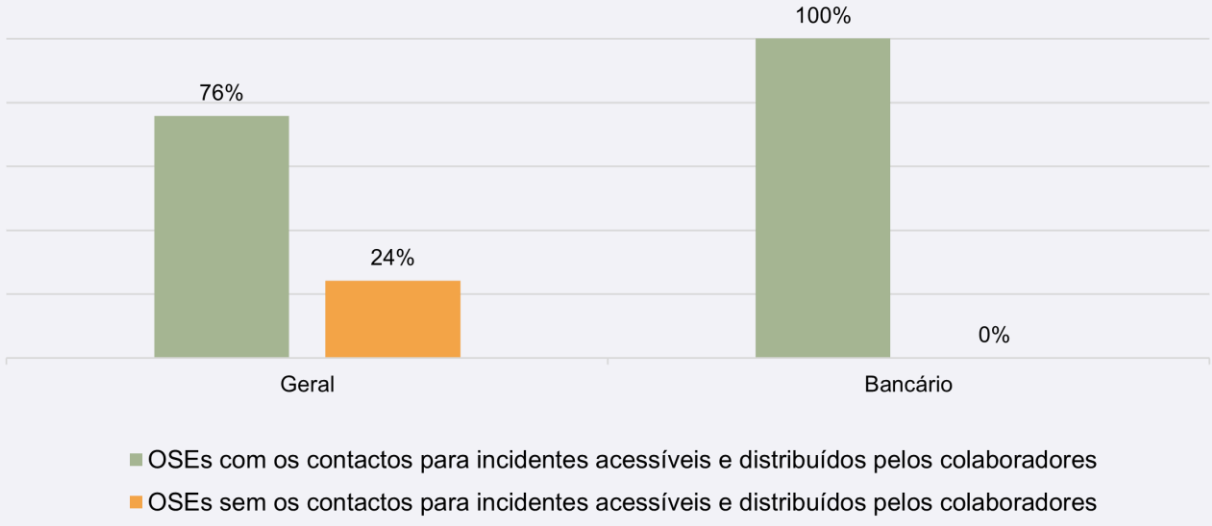
A falta de tempo para definir a equipa surge com menos expressividade, sendo indicada por 20% dos operadores sem equipa. Os operadores que não consideram necessária uma equipa de resposta a incidentes necessária são, no cômputo geral, menos de 10%. Os operadores que selecionaram a opção “outros” (14%) indicaram motivos tais como estar a ser planeada a criação da equipa, a equipa estar a receber formação, ou mesmo o descuido para com a área de cibersegurança. Esta questão não se aplica ao setor da banca visto que a totalidade dos operadores menciona ter equipa de resposta a incidentes.

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



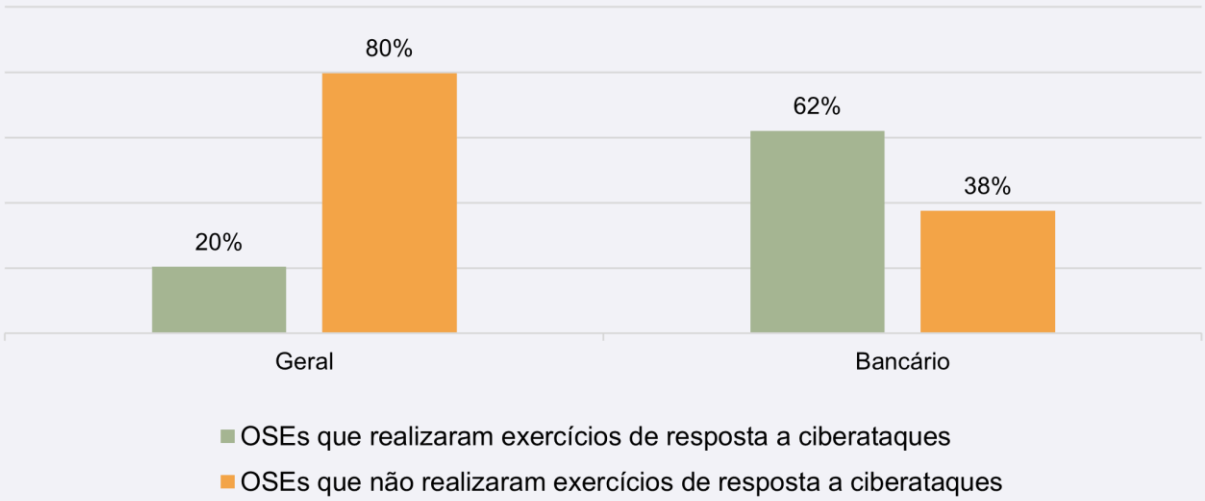
No âmbito geral, 78% dos operadores disponibiliza canais rápidos para a notificação de incidentes aos seus colaboradores. No setor bancário 88% dos operadores inquiridos disponibilizam tais canais aos seus colaboradores.

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



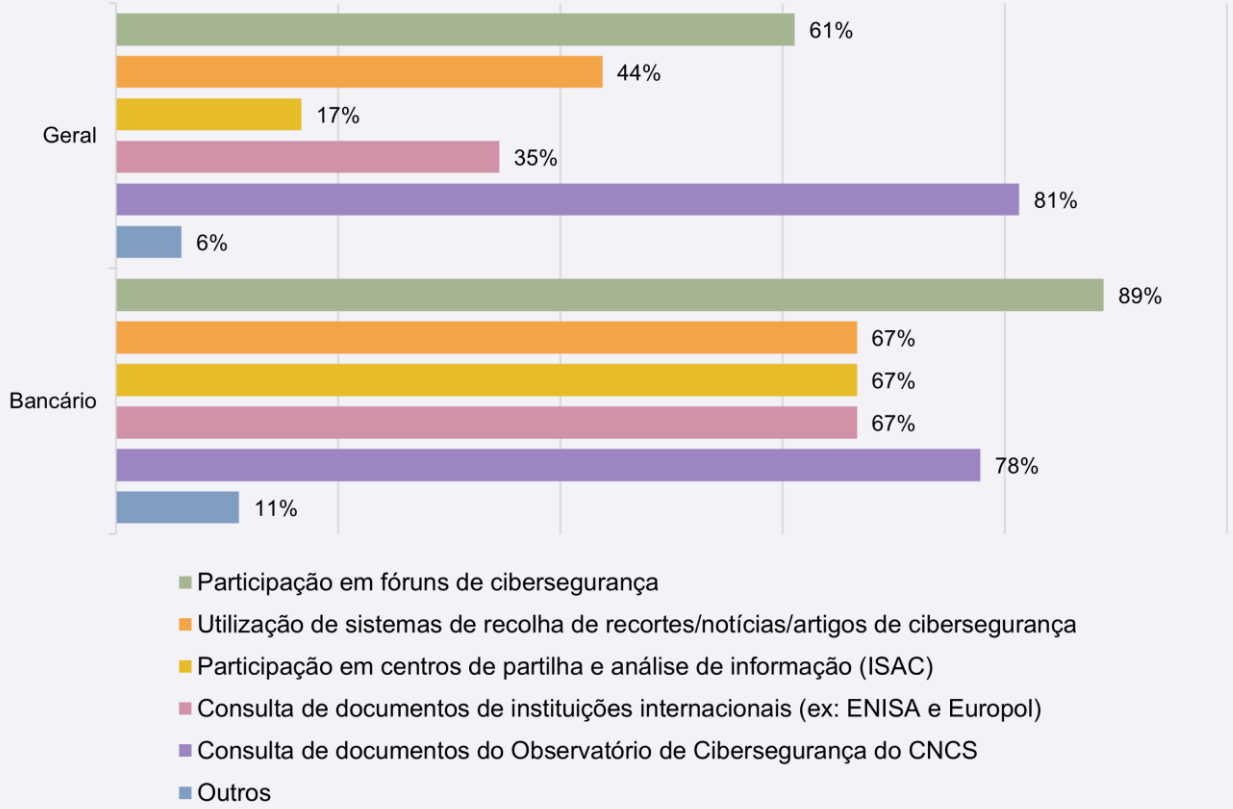
Na generalidade, mais de três quartos dos operadores (76%) têm informação sobre quem contactar em caso de incidente de cibersegurança distribuída e acessível a todos os colaboradores. No setor bancário, todos os inquiridos responderam positivamente a esta questão.

Gráfico 107 - Realização de exercícios de resposta a ciberataques



De acordo com as respostas obtidas, apenas 20% dos operadores inquiridos realizam exercícios de resposta a ciberataques. No entanto, há ainda três setores que se destacam por a maioria dos operadores realizar estes exercícios. Um desses setores é o setor bancário, com cerca de 62% dos inquiridos a realizar exercícios.

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



Independentemente dos métodos utilizados ou das fontes escolhidas para recolher informação sobre boas práticas relativas a riscos e incidentes de cibersegurança, verifica-se que a totalidade dos operadores inquiridos faz essa recolha. Os dois métodos mais comummente utilizados pelos operadores são a consulta de documentos do Observatório de Cibersegurança (cerca de 80%) e a participação em fóruns de cibersegurança (60%). Seguem-se a utilização de sistemas de recolha de notícias e artigos sobre cibersegurança, usada por 44% dos inquiridos, a consulta de documentos de instituições internacionais, como a ENISA e a Europol, praticada por cerca de 35% dos inquiridos. A participação em centros de partilha e análise de informação (ISACs) é a prática menos observada, sendo indicada por apenas 17% dos operadores inquiridos. Estes dados diferem grandemente dos registados pela ENISA, que dão conta de pelo menos 35% dos OSE em Portugal a participarem em ISACs[55].

Destaca-se o setor bancário por ser aquele que apresenta maior diversificação dos métodos e fontes de recolha de informação utilizados pelos seus operadores.

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

A baixa participação registada nos ISACs merece alguma reflexão. Estes centros de análise e partilha de informação "consistem em parcerias para troca de informação e experiência, assentes no pressuposto de que a partilha consistente de informação e análise de incidentes, ameaças, tendências e boas práticas favorece a resiliência digital individual e coletiva"[56]. O próprio CNCS dinamiza seis ISACs, nomeadamente nos seguintes setores: energia, águas, portos marítimos; *media*; retalho e distribuição; e saúde. O CNCS dinamiza também um ISAC regional na Região Autónoma dos Açores. Há ainda um outro ISAC do setor financeiro, do qual o CNCS é membro, mas não promotor[57].

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

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

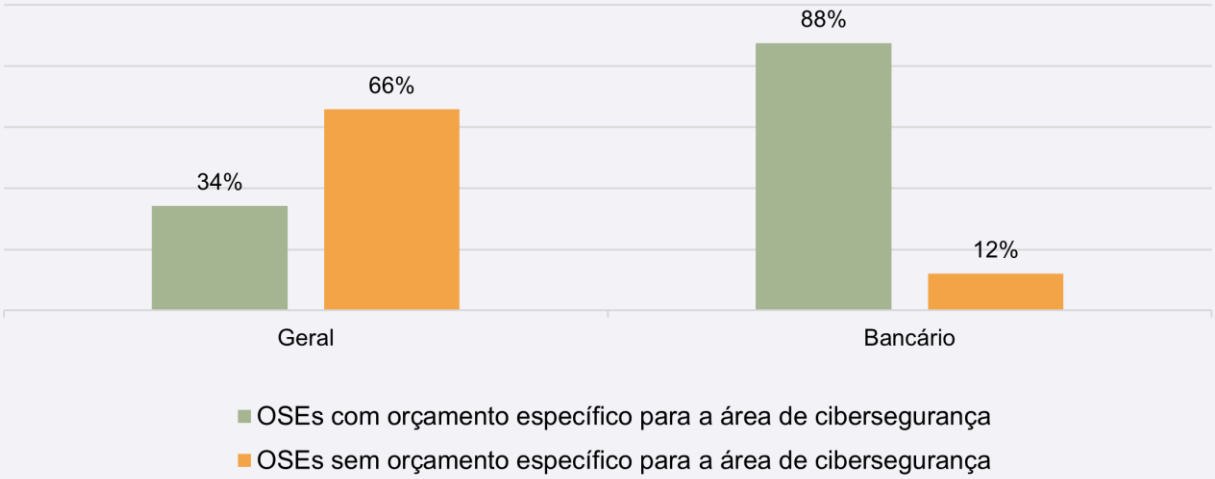
[57] CNCS, ISAC, https://www.cncs.gov.pt/pt/isac/.

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

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

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

Gráfico 109 - Orçamento específico para a área de cibersegurança



Praticamente dois terços dos operadores inquiridos (66%) não possuem orçamento específico para a área de cibersegurança. Contudo, no setor bancário são mais os operadores que possuem orçamento específico para essa área do que aqueles que não. Cerca de 88% dos inquiridos possuem esse orçamento.

O Relatório *NIS Investments* de 2021 foi o último relatório da série da ENISA a analisar a questão de um orçamento específico para a cibersegurança, tendo os últimos dois relatórios, de 2022 e 2023, orientado o seu foco para orçamentos dedicados a riscos terceiros (*third-party risk*) e à formação em cibersegurança, respetivamente. No relatório de 2021, os resultados verificados ao nível da UE são próximos dos obtidos a nível nacional no questionário realizado pelo CNCS: na UE, apenas cerca de 38% dos OSE inquiridos tinham orçamentos dedicados à cibersegurança[61], próximo dos 33% registados pelo CNCS. O mesmo relatório indica que a maioria dos OSE aloca fundos à cibersegurança a partir do orçamento dedicado à parte informática.

Importa também referir que a Diretiva NIS (RJSC) não obriga os OSE a ter orçamentos específicos para cibersegurança. No entanto, um estudo da Comissão Europeia e do Banco Europeu de Investimento (BEI) sobre a criação de uma plataforma de investimento em cibersegurança constatou que as ausências desses orçamentos específicos dificultam grandemente a análise do investimento realizado nesta área. Segundo o mesmo estudo, a própria UE não tinha, no ano de 2022, um orçamento dedicado ao financiamento da sua estratégia de cibersegurança[62]. Este orçamento surgiu apenas em 2023, no âmbito do Programa Europa Digital, com um orçamento global de 1,3 mil milhões de euros, dos quais 375 milhões são dedicados à cibersegurança no biénio 2023-2024[63]. No âmbito da investigação e inovação, surge também o programa Horizonte Europa, com um orçamento global de 95,5 mil milhões de euros a ser executado entre 2021 e 2027, alocando 1,9 mil milhões de euros neste período à área da cibersegurança[64].

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

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

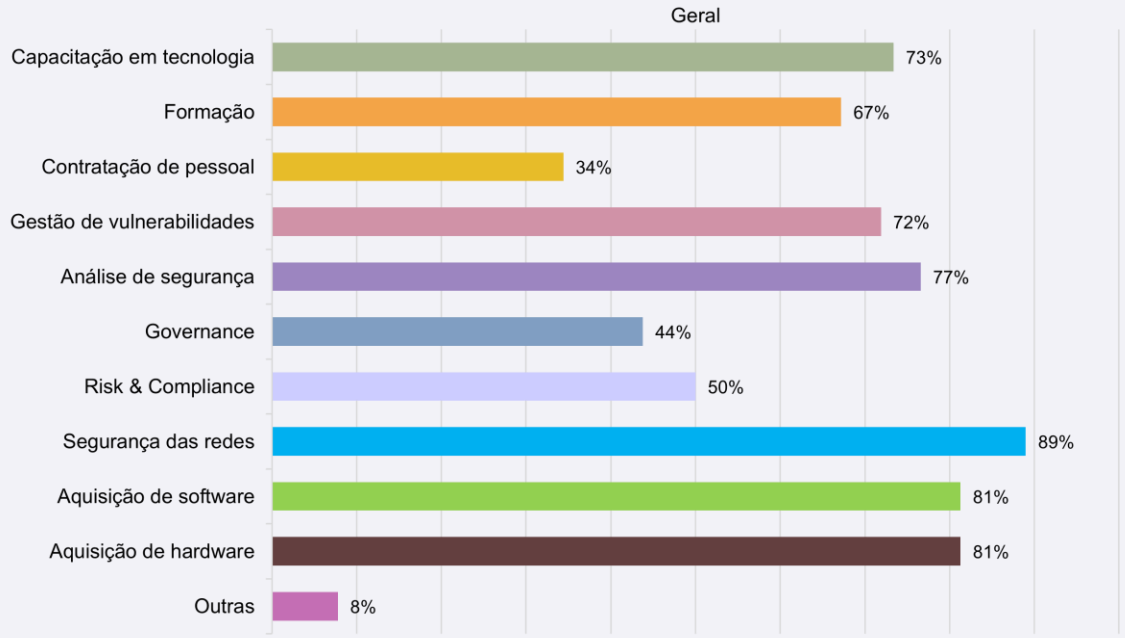
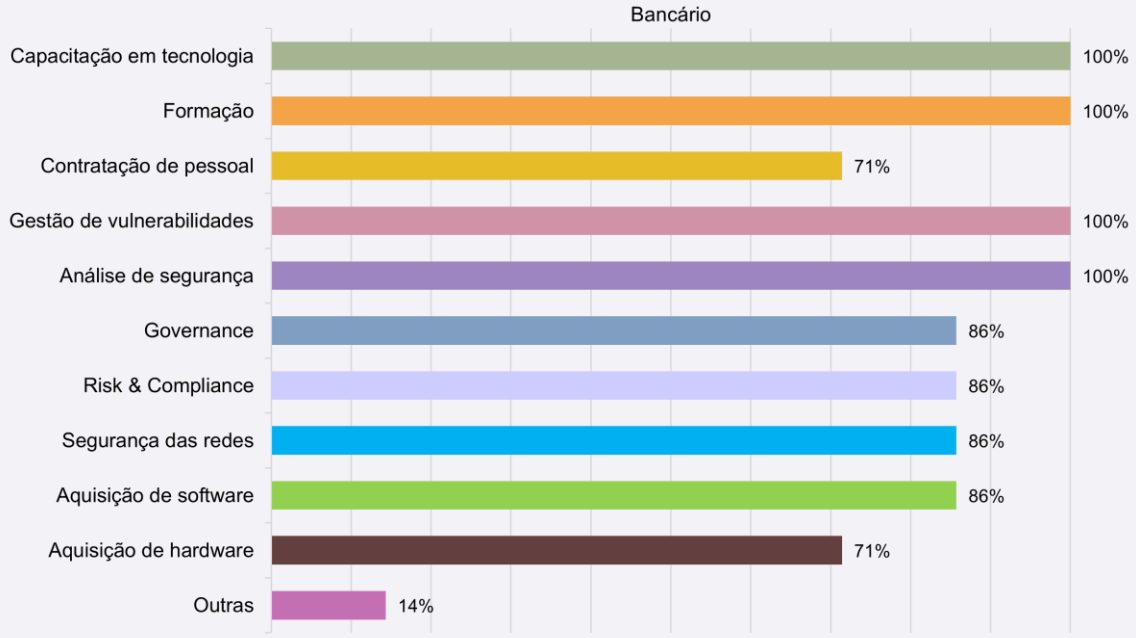


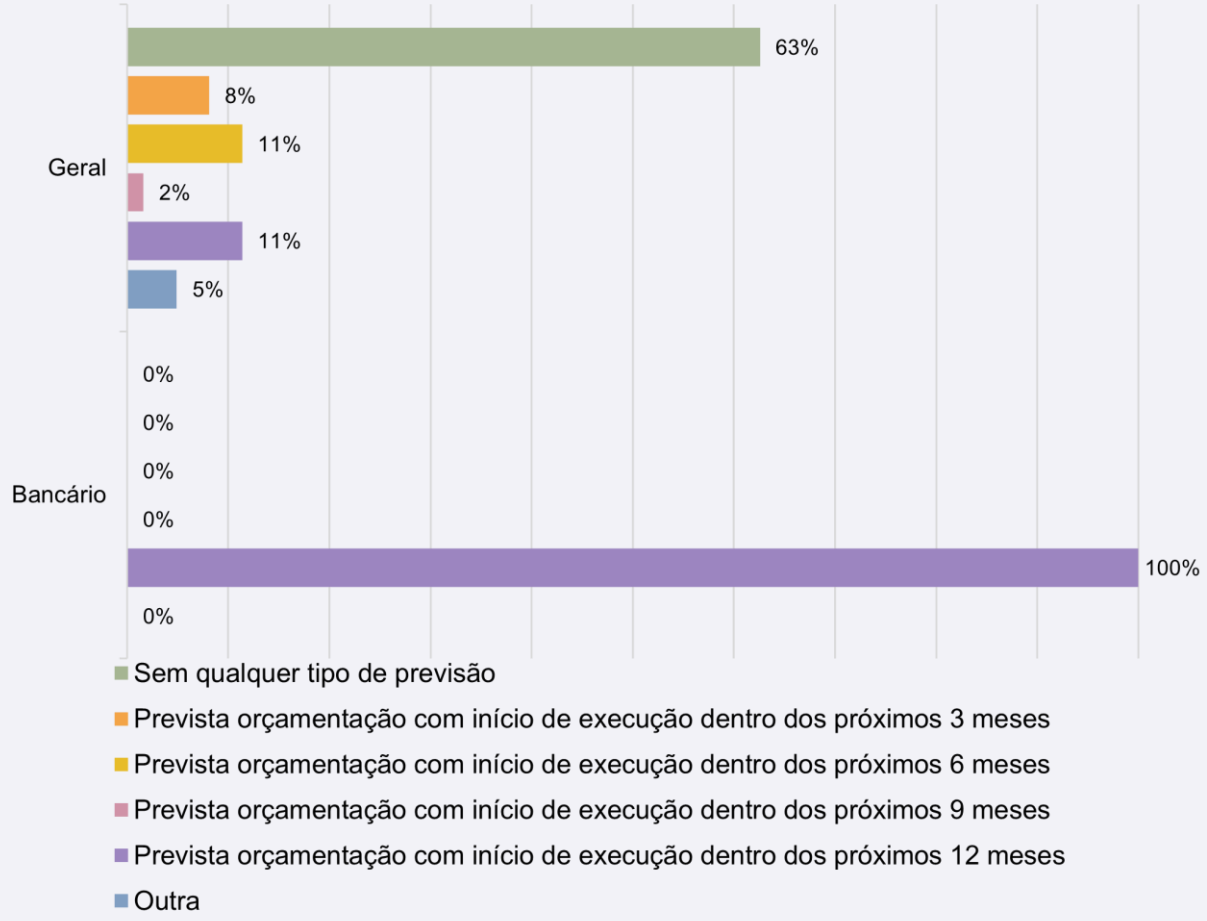
Gráfico 110.1 - Áreas de aplicação dos orçamentos específicos para cibersegurança



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

A ENISA realizou um inquérito a 251 organizações OSE e prestadores de serviços digitais (oriundas da França, Alemanha, Itália, Espanha e Polónia). Segundo o inquérito, o orçamento médio para a implementação da diretiva NIS é 175 mil euros. A maioria das organizações do inquérito priorizaram os domínios de *Governance, Risk & Compliance* e Segurança das Redes[65]. De acordo com um estudo da NIS de 2023, a média de impacto anual dos incidentes informáticos foi de 365 mil euros e a mediana de 250 mil euros, tendo sido estes dados recolhidos de 38 entidades[66].

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

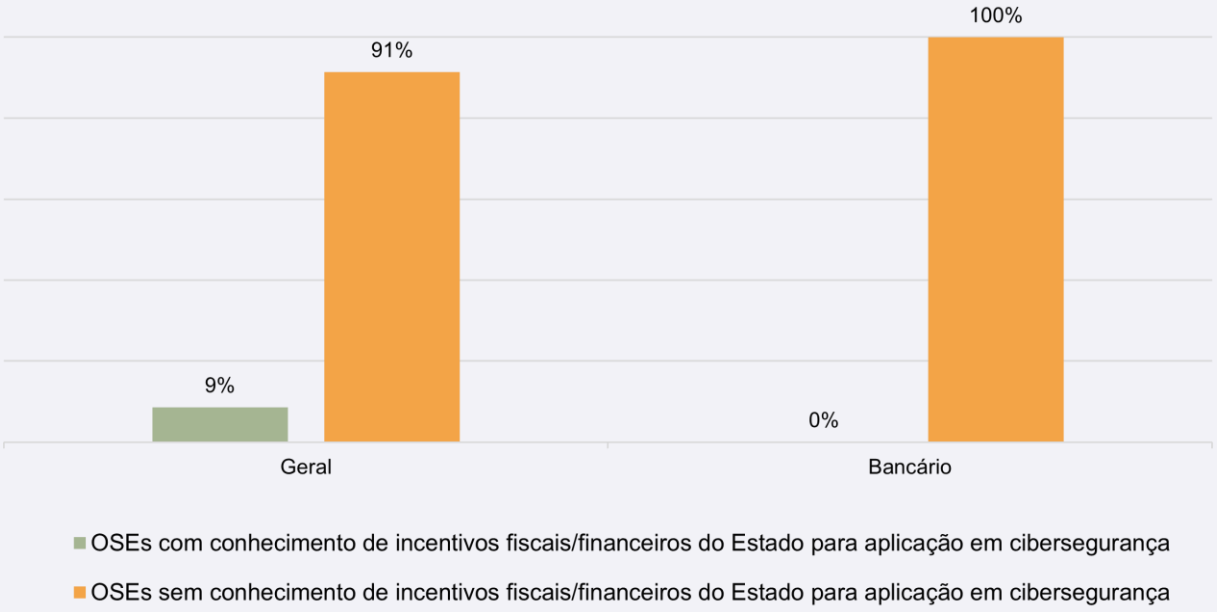


Foi questionado aos operadores sem orçamentos específicos para cibersegurança se estava previsto virem a ter qualquer orçamentação dedicada à área durante o último trimestre de 2023 ou a partir do ano de 2024. 63% destes não têm qualquer previsão de vir a ter tal orçamento. No setor bancário, todos os operadores sem orçamento específico para cibersegurança à data da realização do questionário tinham previsto iniciar a execução de um durante os 12 meses subsequentes, ou seja, até ao último trimestre de 2024. 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.

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

[66] ENISA, "NIS Investments", 2023

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

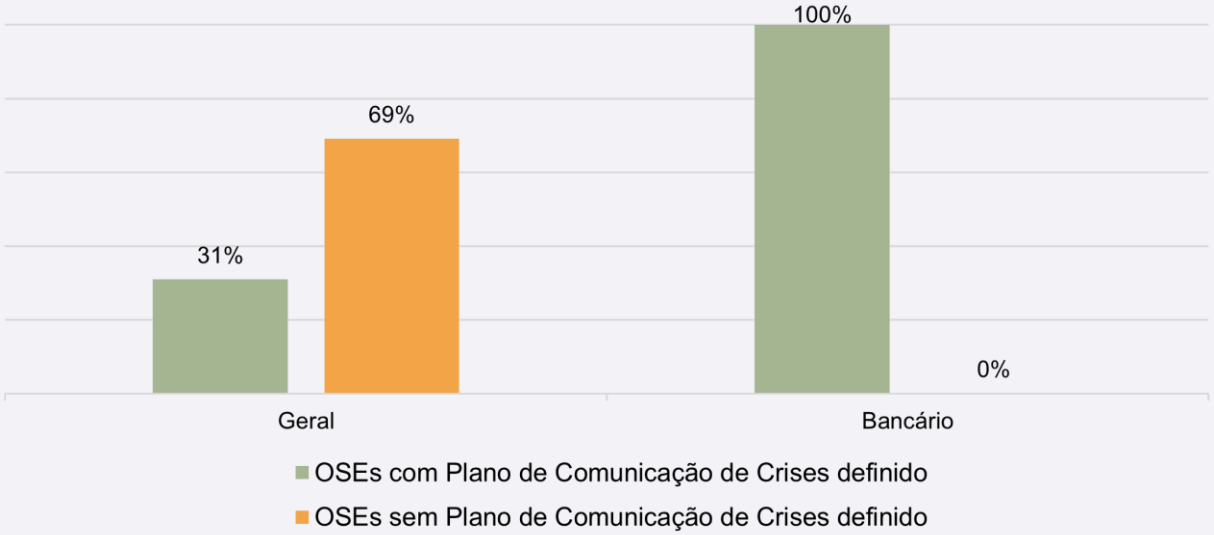


Cerca de 91% dos inquiridos não tinha qualquer conhecimento sobre incentivos fiscais ou financeiros provenientes do Estado para aplicação na área de cibersegurança. No setor bancário não foram registados quaisquer operadores com conhecimento desses incentivos.

Cabe assim recordar que o Estado português lançou, em 2022, a medida Cheque-Formação + Digital, integrada no Programa Emprego + Digital 2025, que permite aos trabalhadores portugueses candidatarem-se a um cheque de formação digital de até 750 euros que pode ser aplicado em formações de cibersegurança[67].

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

Gráfico 113 - Plano de Comunicação de Crises



Muitos dos operadores de serviços essenciais não têm definido um plano de comunicação de crises. Apenas 31% dos inquiridos referiram ter tal plano definido. No setor bancário, 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.

Gráfico 114 - Secções definidas no Plano de Comunicação de Crises

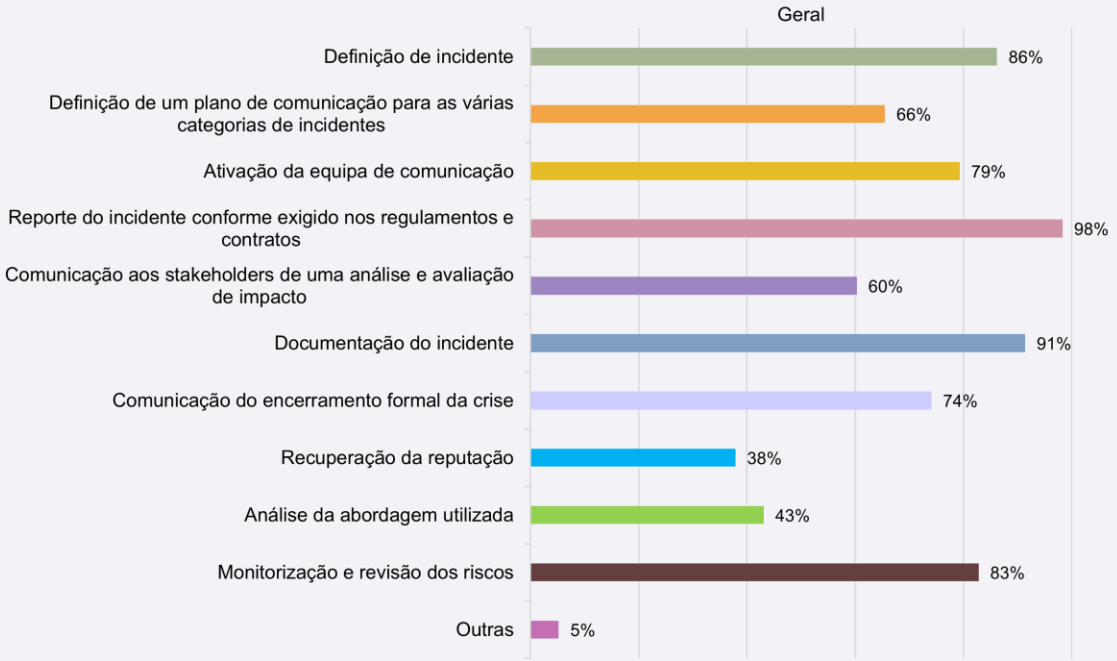
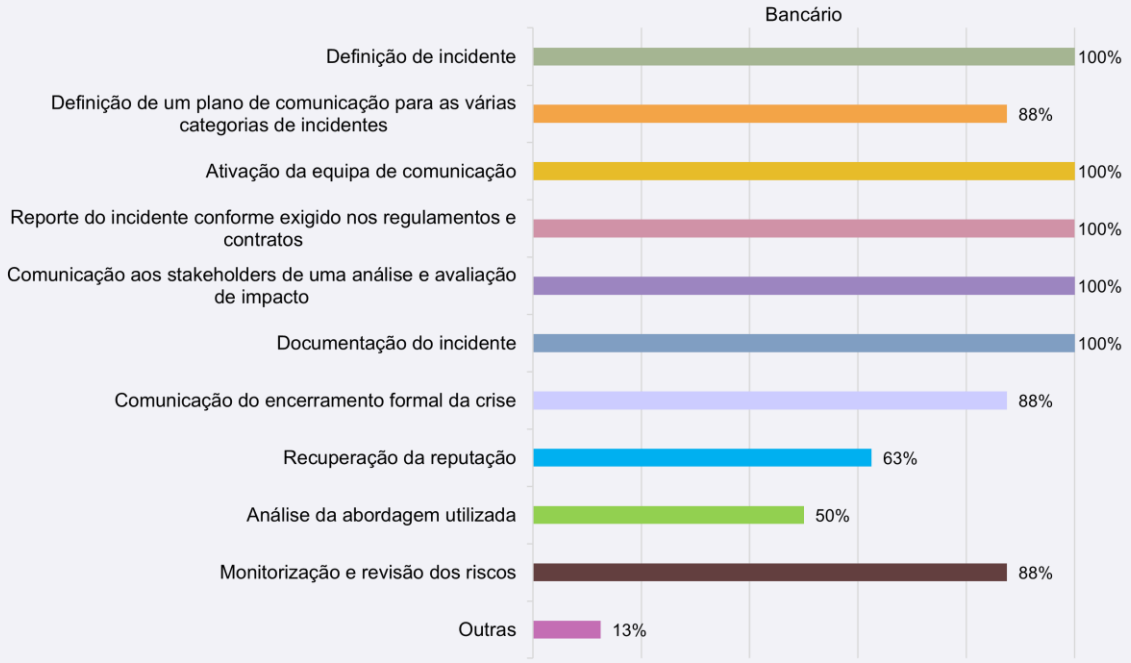


Gráfico 114.1 - Secções definidas no Plano de Comunicação de Crises

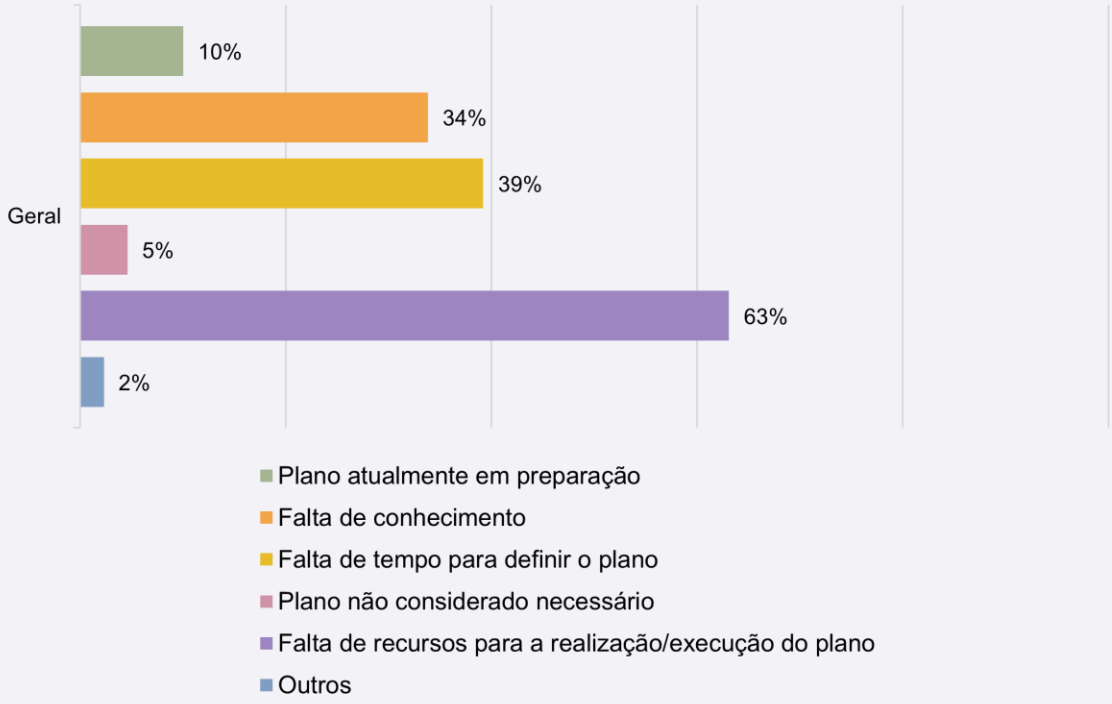


Na análise das secções incluídas nos planos de comunicação de crises, foram incluídas dez secções. Verifica-se que sete destas secções estão incluídas em pelo menos 60% dos planos já definidos. As sete secções mais presentes são a definição de incidente, a definição de um plano de comunicação para várias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

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

A nível setorial, a banca destaca-se, por ser um dos setores onde mais planos incluem as secções elencadas.

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



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

Outros motivos foram mencionados como estar prevista a implementação do plano para 2024/2025 ou mesmo o plano já se encontrar em elaboração. O setor bancário afirma já ter o plano definido. Desta forma a questão não se aplica.

Análise Setorial

1. Bancário

1.1. Contextualização setorial

A criação da banca moderna é largamente atribuída ao Renascimento italiano. O intenso comércio que se verificava nas cidades que mais beneficiavam das trocas marítimas feitas através do Mar Adriático, como Florença, Veneza e Génova, rapidamente passou a exigir muitas das operações ainda hoje praticadas pela banca, de modo a financiar viagens, importações e a produção artística do período renascentista.

Algumas das atividades que ainda hoje se verificam na banca moderna têm uma história de milénios. Por exemplo, relativamente aos depósitos, é possível ler, num texto com cerca de 4000 anos, da Babilónia (hoje Bagdad, Iraque), que "se um homem der a outro prata, ouro, ou qualquer outra coisa para salvaguardar, o que quer que ele dê deverá ser mostrado a testemunhas, e deverá preparar os contratos antes de realizar o depósito"[68], e deveriam ser pagos ao depositário um sessenta avos do tesouro depositado por esse serviço.

Na Antiguidade Clássica, gregos e romanos tinham também já implementado mecanismos de depósito de dinheiro e de bens. Em particular, o comércio e a "banca" romanos contavam já com a abertura de contas, emissão de notas de troca, cartas de crédito, empréstimos (com juros), hipotecas, e outras operações idênticas às que ainda hoje se verificam junto das entidades bancárias[69]. Crê-se que algumas destas práticas terão sido perdidas no Ocidente com a queda do Império Romano no século V, mas foram recuperadas e mais bem desenvolvidas durante o Renascimento, que lançaria as bases da banca moderna[70].

No caso de Portugal, o desenvolvimento da atividade bancária ficou também ligado ao comércio e à expansão marítima, iniciada em 1415, com a conquista de Ceuta, conduzindo à exploração da costa ocidental africana, e mais tarde, à descoberta do caminho marítimo para a Índia e ao estabelecimento de relações comerciais com o continente asiático[71]. A necessidade de dinheiro

[68] Noble Hogsson, *Banking through the Ages* (Nova Iorque: Dodd, Mead & Company, 1926), 33.

[69] Hogsson, *Banking through the Ages*, 40-41.

[70] Hogsson, *Banking through the Ages*, 63-64.

[71] António Farinha, "O Primeiro Banco em Portugal (1465)", *Estudos em Homenagem a Jorge Borges de Macedo*, (Lisboa: Instituto Nacional de Investigação Científica, Centro de Arqueologia e História da Universidade de Lisboa, 1992), 153.

para o financiamento das expedições, a necessidade de adquirir capacidade de navegação, através da compra de instrumentos de navegação e da contratação de astrónomos, engenheiros e cartógrafos estrangeiros e de fazer comércio com outros povos conduziu à criação das primeiras casas de câmbio e bancos em Portugal.

O primeiro banco de que há registo em Portugal é o banco de Mossém Rafael Vivas, fundado em 1465, durante o reinado de D. Afonso V, que "emergia, então, das necessidades cambiais, da exigência de pagamentos devidos à circulação das mercadorias e das pessoas e da vantagem em proceder a pagamentos à distância"[72].

Outras instituições bancárias foram surgindo ao longo dos anos, mas, ao contrário do que se verificava em repúblicas italianas, como a de Florença, em que os bancos eram essencialmente privados e de iniciativa de grandes famílias, os bancos em Portugal eram sobretudo criados, até finais do século XVIII, por desígnio régio, para responder a necessidades do reino.

Só a 19 de novembro de 1846 foi criado o Banco de Portugal (BdP). Consequência da fusão de outros bancos (Banco de Lisboa e Companhia Confiança Nacional), o BdP foi criado com duas funções: a função banco comercial e a função banco emissor. Até 1974, aquando da sua nacionalização, o BdP era maioritariamente privado e foi fundado com o estatuto de sociedade económica[73].

Bancos como o Banco Espírito Santo e Caixa Geral de Depósitos são posteriores à criação do BdP, tendo sido fundados em 1869 e 1876, respetivamente. Já bancos como o Banco Português de Investimento (BPI) ou o Banco Comercial Português (Millenium BCP) surgiram apenas na década de 80 do século passado, respetivamente, em 1981 e em 1985. À data da elaboração deste relatório, operavam em Portugal 1373 entidades autorizadas[74], com cerca de 3852 agências[75] em funcionamento.

O setor bancário é o principal responsável pela gestão dos depósitos dos seus clientes, pela circulação do dinheiro entre pessoas, empresas e Estado, pela intermediação financeira, pela concessão de crédito e pela disponibilização de meios cómodos e seguros de realizar diversas operações financeiras, como pagamentos, transferências e levantamentos, entre outros.

[72] Farinha, "O Primeiro Banco em Portugal", 167.

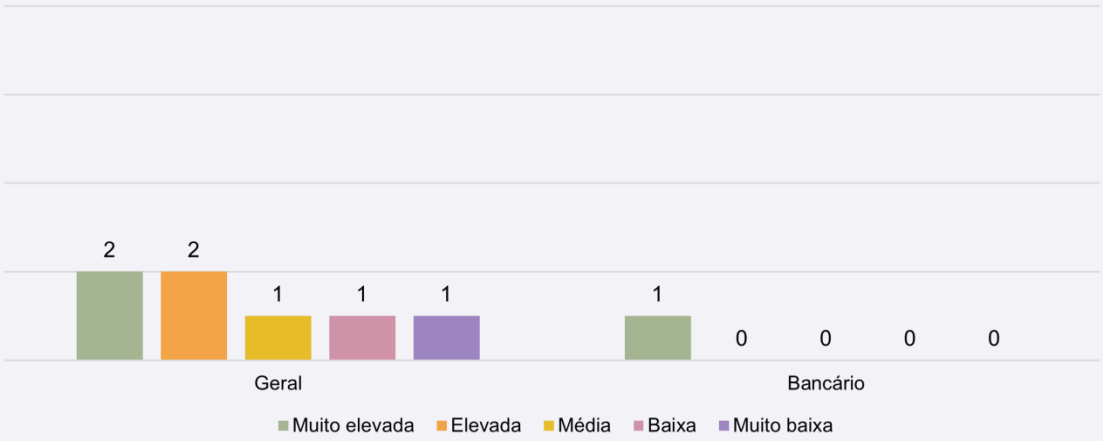
[73] "História do Banco de Portugal", Sobre o Banco, Banco de Portugal, https://www.bportugal.pt/page/historia-do-banco-de-portugal.

[74] "Instituições autorizadas", Banco de Portugal, última atualização em 23 de setembro de 2024, https://www.bportugal.pt/page/listagem-entidades-autorizadas.

[75] "Lista de agências", Banco de Portugal, agosto de 2024, https://www.bportugal.pt/sites/default/files/listaagencias.xls.

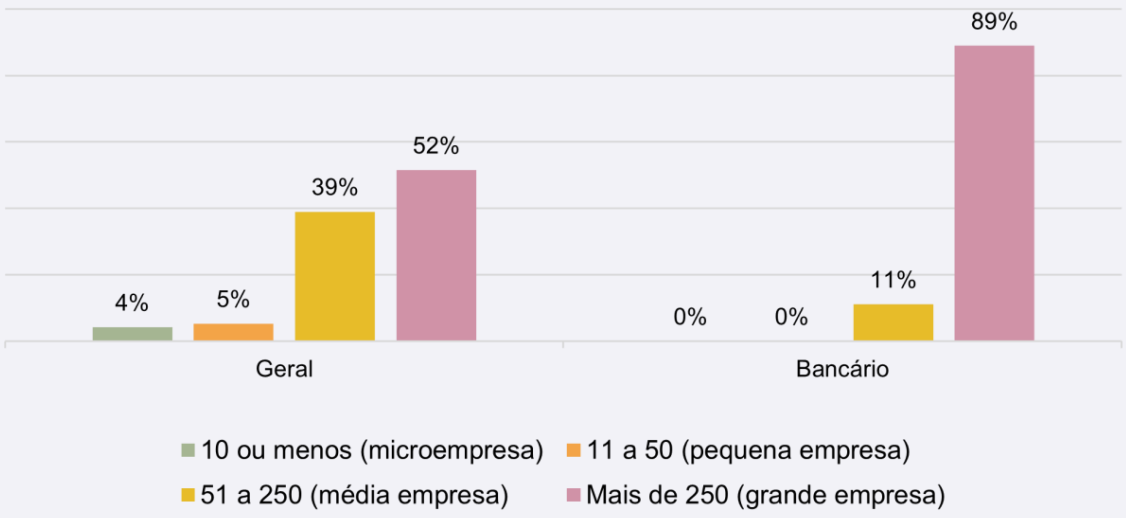
Atualmente, de acordo com o questionário realizado, o regulador do setor considera que a maturidade deste em cibersegurança é muito elevada e, no âmbito geral, não há reguladores com maior perceção de maturidade em cibersegurança (**Gráfico 9**).

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



O tecido empresarial dos OSE do setor bancário é sobretudo composto por grandes empresas, representando estas 90% dos operadores do setor, com os restantes 10% sendo médias empresas. Estes valores são superiores à média geral (**Gráfico 30**).

Gráfico 30 - Número de colaboradores na organização



Esta perceção pode ser suportada pelo número de operadores que disponibiliza formação em cibersegurança aos seus colaboradores (100% contra 65%) (vide **Gráfico 38**) e pelas medidas de cibersegurança adotadas (**Gráfico 66.3 A e Gráfico 66.3 B**). As medidas de proteção menos adotadas são: utilização de *browser* que proteja a privacidade e controlos biométricos para identificação e autenticação de utilizadores.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

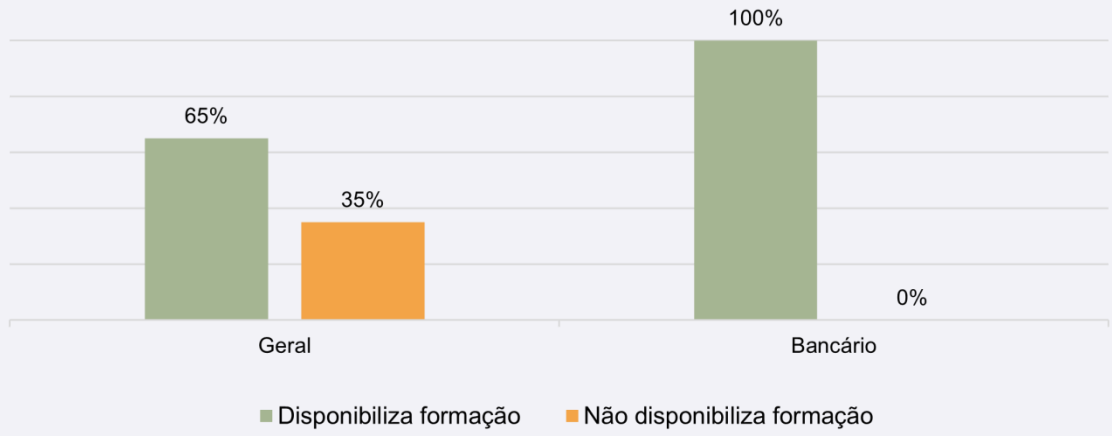
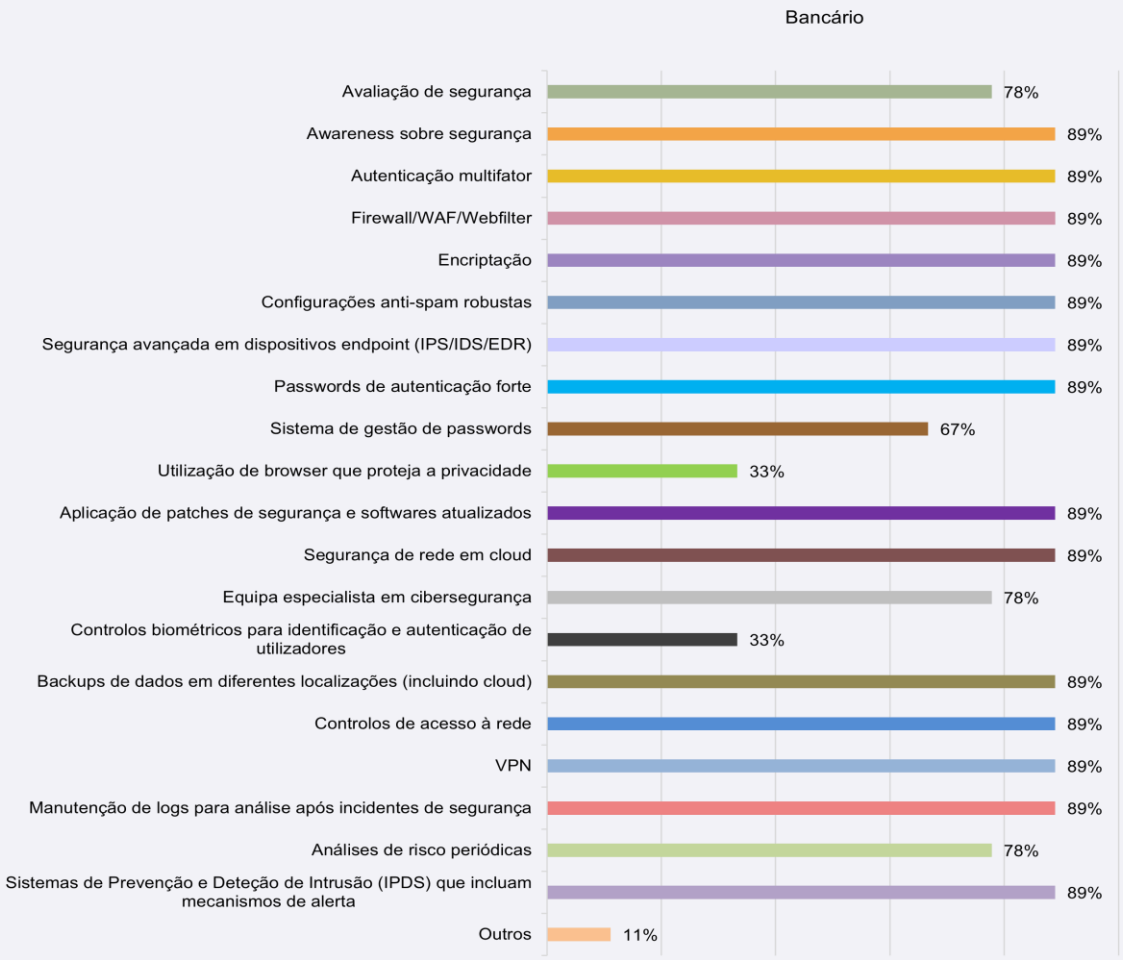
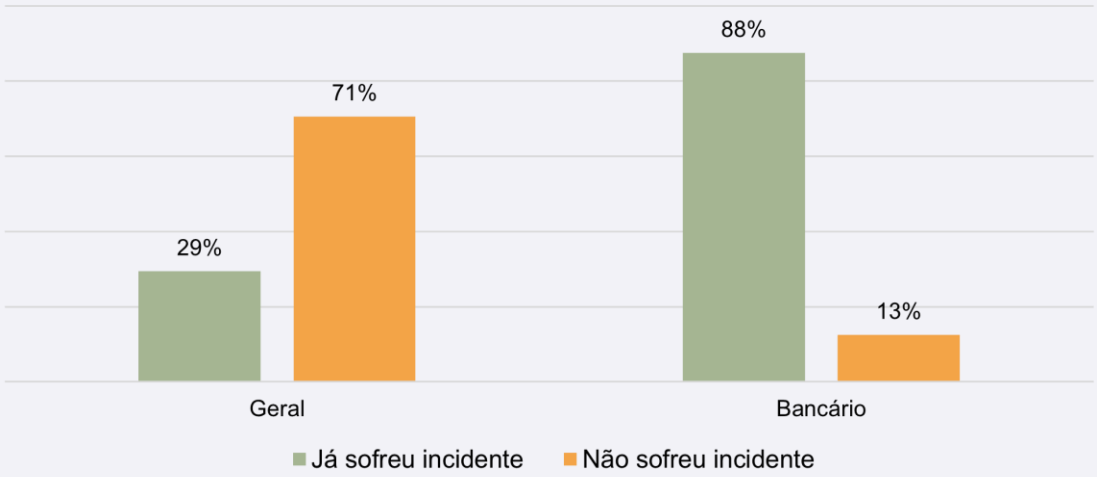


Gráfico 66.3 - Medidas de proteção contra ameaças de cibersegurança



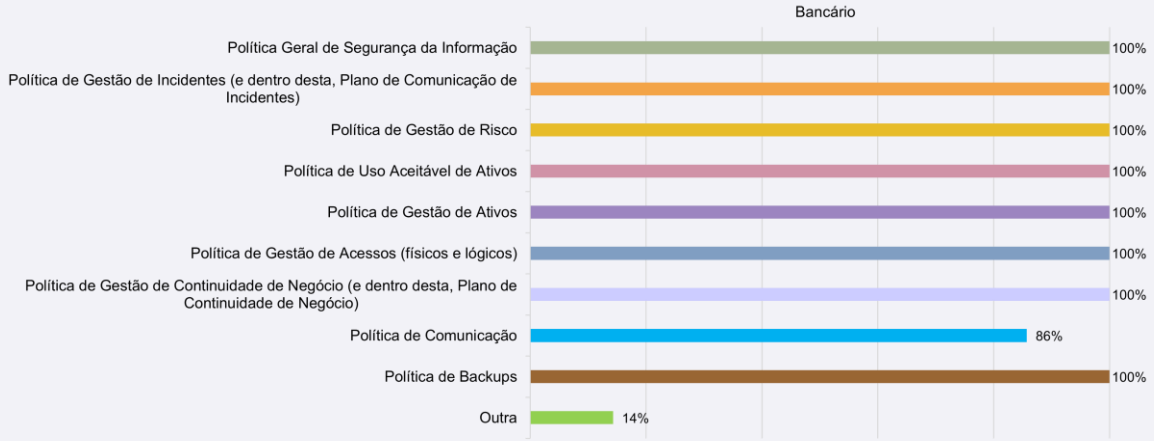
Mesmo sendo este um setor com uma elevada maturidade em cibersegurança, o setor bancário foi o setor onde mais operadores indicaram já ter sofrido incidentes de segurança (88% dos OSE - **Gráfico 68**), evidenciando-o como um alvo preferencial para ciberataques e estando acima dos 71% da média geral.

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



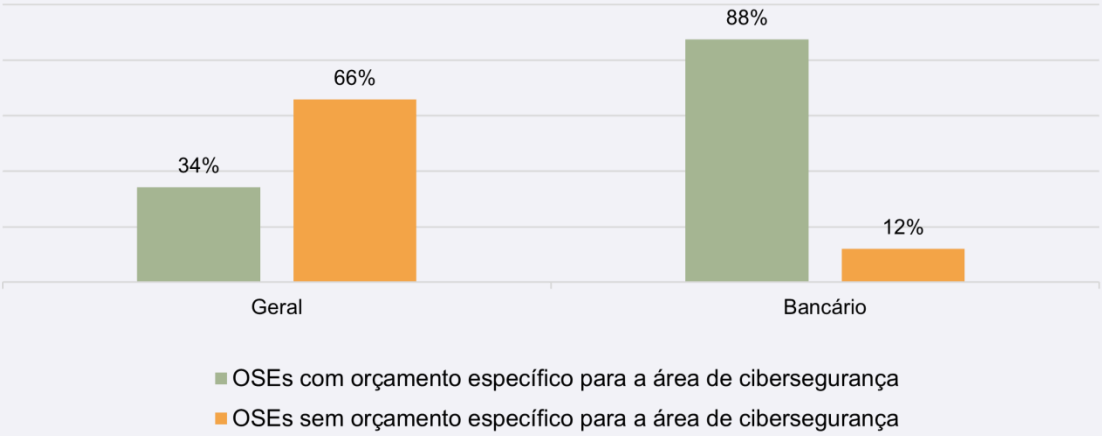
As políticas de cibersegurança e outras políticas relacionadas implementadas (**Gráfico 79.3**) também suportam a afirmação anterior. O plano de segurança tem todas as políticas incluídas, com exceção da política de comunicação que está apenas incluída em 86% dos planos de segurança.

Gráfico 79.3 - Políticas incluídas no Plano de Segurança



Neste setor, cerca de 88% dos OSE têm orçamento específico para a área de cibersegurança, sendo o valor, no geral, situado nos 34% (**Gráfico 109**).

Gráfico 109 - Orçamento específico para a área de cibersegurança



1.1.1. Impacto socioeconómico

O setor bancário desempenha um papel crucial na economia contemporânea, facilitando a intermediação financeira. Um processo de intermediação financeira envolve a captação de recursos, transferindo fundos de agentes económicos com excedente de capital para aqueles com necessidade de financiamento. Neste processo de intermediação financeira, os intermediários financeiros assumem o risco por conta própria pela aquisição de ativos financeiros ou contração de dívidas. Um setor bancário robusto e eficiente promove este tipo de ações que consistem na acumulação de poupança e respetiva alocação em investimentos mais produtivos, impulsionando a inovação e o crescimento económico. Na Europa, os bancos são os principais intermediários financeiros em todos os países do continente[76].

A banca tem também um papel fundamental para a economia portuguesa. Assim como a conjuntura económica de um país tende a afetar o setor bancário, também este setor exerce grande influência no bem-estar económico de um país no seu global.

Os meios de pagamento disponibilizados sobretudo pelo setor bancário, como é o caso dos cartões de débito e crédito e das contas correntes, são o que permite realizar de forma prática e segura um conjunto de operações necessárias no dia a dia, como transferências, pagamentos de bens e serviços, levantamentos ou débitos diretos. Por outro lado, a banca depende da confiança que os depositantes lhe atribuem quando lhes entregam as suas poupanças, para que sejam guardadas de forma segura"[77].

[76] Carlos Costa, "O Sistema Financeiro Português e o Papel do Banco de Portugal", (intervenção no Fórum na Área Financeira, Macau, 10 de outubro de 2012), 1.
[77] Barroso, "O fundamental papel da banca na saúde das economias", 6 de julho de 2023.

Quer estejamos perante uma recessão ou uma fase de crescimento económico, o banco deverá ter a capacidade de emprestar dinheiro, de garantir que os pagamentos são processados rapidamente, em segurança, a um valor reduzido e que os depósitos estão salvaguardados. A realização segura das diferentes transações financeiras a que todos os cidadãos estão sujeitos diariamente - como transferências, pagamentos de bens ou serviços e débitos diretos - depende diretamente do papel desempenhado pelos meios de pagamento fornecidos pelo setor bancário - como cartões de débito e crédito e contas correntes. Além da segurança destes serviços dever ser garantida pelos bancos, estes também contam com a confiança que os clientes depositam neles ao confiarem as suas poupanças. Por este motivo, e em qualquer contexto nacional, a decisão de deixar um banco falir nunca é tomada por um governo de forma leviana. Levar um banco a uma situação extrema como esta leva a situações de quebra de confiança que "podem provocar corridas aos depósitos, comprometer poupanças de uma vida e inviabilizar os fundos necessários à manutenção do funcionamento de operações de empresas, instituições públicas e tantas outras organizações"[78].

O setor bancário tem um papel fundamental na economia nacional e a sua atuação vai muito além da facilitação de transações[79]. Os seus principais papéis, em contexto de facilitação financeira, são os seguintes:

- **Intermediação financeira**: O banco assegura a intermediação financeira através da canalização de fundos dos aforradores para os investidores[80]. Este processo contribui para a estimulação do investimento e consequentemente, do crescimento económico.
- **Disponibilização de crédito bancário**: O banco disponibiliza crédito bancário que é utilizado para financiar as necessidades dos agregados familiares, através da regulação do seu padrão de consumo ao longo do tempo e ajudando-os a investir em bens que impulsionam o desenvolvimento da economia.
- **Contribuição para a estabilidade financeira do país**: Um setor bancário sólido e eficiente incentiva à acumulação de poupança e permite a realização de investimentos mais produtivos, apoiando assim a inovação, o crescimento económico e a estabilidade financeira[81].

Tendo todas estas valências em conta, o setor bancário é responsável pela movimentação de centenas de milhares de milhões de euros. Segundo o Relatório dos Sistemas de Pagamentos de 2022, publicado pelo BdP, foram transacionados em Portugal, durante esse ano, cerca de 655,5 mil milhões de euros, o equivalente a 1,8 milhões de euros por dia[82].

O setor bancário tem-se mostrado lucrativo também. Em 2022, os sete maiores Bancos portugueses – CGD, BCP, Novobanco, Santander Totta, BPI, Crédito Agrícola e Banco Montepio – lucraram 2.761 milhões de euros[83]. Em 2023, os lucros da CGD, BCP, Santander Totta, BPI e Novobanco, superaram os 4,4 mil milhões de euros[84]. Em sede de IRC, a banca gerou aproximadamente 1,47 mil milhões de euros para os cofres do Estado no mesmo ano[85].

---

78 Barroso, "O fundamental papel da banca na saúde das economias", 6 de julho de 2023.

79 Comissão Europeia, "Ficha temática sobre o semestre europeu: Setor Bancário e estabilidade financeira", 16 de outubro de 2017, 1, https://commission.europa.eu/system/files/2021-01/european-semester_thematic-factsheet_banking-sector-financial-stability_pt.pdf.

80 Comissão Europeia, "Setor Bancário e estabilidade financeira", 16 de outubro de 2017, 1.

81 Comissão Europeia, "Setor Bancário e estabilidade financeira", 16 de outubro de 2017, 1.

82 Banco de Portugal, "Relatório dos Sistemas de Pagamentos 2022", 11.

83 Maria Alves, "Bancos privados com 3,3 mil milhões de lucros em 2023 a subirem 74,2% face ao ano anterior", *Jornal Económico*, 5 de março de 2024, https://leitor.jornaleconomico.pt/noticia/bancos-privados-com-3-3-mil-milhoes-de-lucros-em-2023-a-subirem-74-2-face-ao-ano-anterior.

84 Alberto Teixeira, "Banca com lucros recorde em 5 gráficos", *Eco*, 15 de março de 2024, https://eco.sapo.pt/2024/03/15/banca-com-lucros-recorde-em-5-graficos/.

85 Mariana Dias, "Cinco maiores bancos pagaram 17% do IRC total arrecadado em 2023", *Diário de Notícias*, 25 de março de 2023, https://www.dn.pt/3384889811/cinco-maiores-bancos-pagaram-17-do-irc-total-arrecadado-em-2023/.

Quanto ao emprego, o setor bancário era responsável, em 2022, por quase 60 mil postos de trabalho. O número de empregos no setor tem, no entanto, vindo a diminuir ao longo dos anos. Ao passo que entre os anos de 2008 e 2014 o setor empregava quase 80 mil pessoas, a empregabilidade reduziu em cerca de 20 mil postos de trabalho desde então[86].

As principais atividades do setor bancário impactam tanto a economia nacional como a vida em sociedade. A disponibilização de formas de transação, permitindo a realização de operações, tais como transferências, pagamentos, de bens, serviços, ou levantamento de dinheiro, de forma prática, rápida e segura geraram a possibilidade de realizar tudo isso sem que seja necessário ir a um balcão ou até mesmo a um terminal multibanco (com exceção dos levantamentos). A maioria das operações referidas podem hoje ser realizadas em praticamente qualquer lugar, desde que se tenha um dispositivo como um computador ou um *smartphone* e acesso à Internet.

A concessão de crédito, como referido, é também o que permite a uma larga porção da população a realização de certos desígnios, como a compra de habitação, de carro, de pagar estudos, ou iniciar um negócio. A melhoria no acesso aos serviços financeiros tem permitido que cada vez mais pessoas tenham acesso a estes, sendo possível observar uma crescente inclusão de cidadãos que eram, até então, ignorados pelos sistemas, o que favorece um movimento de democratização global[87].

Naturalmente, existe também o "reverso da medalha". Isto é, quando uma ou várias entidades do setor bancário obtêm maus resultados, esses resultados tendem a refletir-se na economia e na sociedade. O crescimento económico e a criação de riqueza podem abrandar ou até mesmo ser invertidos quando o setor bancário não consegue ter um bom desempenho. Ao nível social, o agravamento de taxas de juro, de prestações de crédito tende a colocar uma pressão económica e financeira sobre aqueles que contraíram empréstimos, podendo mesmo levar ao abandono do objetivo para que o empréstimo foi contraído.

1.1.2. Especificidades tecnológicas

Relativamente ao âmbito tecnológico, têm-se vindo a verificar diversas mudanças no setor financeiro impulsionadas por tecnologias como a IA, IoT, *Cloud*, o 5G ou a computação quântica. Estas inovações tecnológicas têm contribuído para a reformulação dos serviços financeiros, sugerindo novas e diferentes oportunidades quer para empresas, quer para consumidores[88].

O setor bancário tem-se reinventado para dar resposta às exigências da era digital, sendo o surgimento das empresas de *fintech* (*Financial Technology*) uma das consequências dessa adaptação[89]. Este termo pode referir-se à tecnologia financeira ou às entidades ou empresas que, a operar no setor financeiro (bancário ou segurador, com o termo *Insurtech*), implementam modelos de negócio baseados naquelas novas tecnologias. O objetivo é agilizar procedimentos e inovar nas suas práticas de negócio com vista a melhorar a experiência do cliente. As *fintech* atuam em diferentes áreas como serviços de informação de contas, serviços de pagamento, ativos e moedas virtuais, atividade de intermediação de crédito, entre outros[90].

---

[86] "Banco de Portugal atualiza séries longas do setor bancário português", BPStat, Banco de Portugal, 26 de julho de 2023, https://bpstat.bportugal.pt/conteudos/noticias/1955.

[87] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023, https://observador.pt/2023/11/29/inovacao-e-setor-financeiro-simplificar-e-a-regra/.

[88] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023.

[89] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023.

[90] "Fintech: o que são e o que fazem", Saldo Positivo, Caixa Geral de Depósitos, 4 de abril de 2023, https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/o-que-sao-fintech.aspx

O surgimento de inovações tecnológicas como o *homebanking* ou a tecnologia de verificação de identidade (através de biometria, impressão digital ou reconhecimento facial) constituem ferramentas fundamentais para um aumento do conforto dos clientes ao permitirem a realização de um grande número de operações bancárias, quando lhes for mais conveniente e de forma tão segura quanto possível[91].

Os desenvolvimentos tecnológicos neste setor não se limitam à melhoria da experiência dos utilizadores, passando também por aumentar o nível de proteção dos dados dos clientes e das transações realizadas, considerando a sensibilidade dos dados que estas implicam. Os bancos utilizam, atualmente, soluções de segurança como a criptografia de dados, a 2FA, o 3D *Secure* ou a monitorização contínua de atividades suspeitas[92]. O 3D *Secure* reforça a segurança dos serviços de compras na *internet* no momento de utilização de cartão de crédito. Este cenário permite, através de um código de validação que os clientes recebem no seu número de telemóvel, registado no seu banco, que confirmem que são os titulares do cartão. Esta ação diminui a possibilidade de atividade fraudulenta através da confirmação do titular do cartão a ser utilizado na respetiva compra. Consequentemente, aumenta a confiança no serviço prestado no *site* em que a compra está a ser realizada[93]. O 3D *Secure* acaba por ser um formato de 2FA, uma vez que, de forma a garantir a autenticidade da identificação de um cliente, são mais utilizadas duas combinações de dois fatores: uma palavra-passe juntamente com um código enviado por SMS para um número de telemóvel registado ou utilização de identificação facial ou impressão digital com código enviado para o telemóvel[94].

Os *chatbots* e os assistentes virtuais são outras tecnologias que têm sido exploradas neste setor permitindo que os clientes obtenham apoio por parte dos bancos e dos serviços durante todo o ano e durante 24 horas por dia[95].

A utilização de IA é particularmente relevante neste setor ao nível da cibersegurança, onde torna possível identificar ataques e ciberameaças às bases de dados de clientes. Além disso, contribui muito para a transformação digital do setor, através de funções de processamento massivo de dados e algoritmos[96]. A IA também desempenha um papel crucial na deteção e prevenção de fraudes no setor bancário. Especialistas explicam que, por meio de análises avançadas de dados e *machine learning*, os sistemas de IA são capazes de identificar padrões suspeitos ou anómalos em transações financeiras. Isso assegura uma abordagem proativa na proteção das contas dos clientes contra fraudes e atividades maliciosas[97].

[91] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023.

[92] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023.

[93] "A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor", *Business IT*, 21 de outubro de 2022, https://business-it.pt/2022/10/21/a-tecnologia-e-a-banca-as-inovacoes-que-estao-a-permitir-digitalizar-o-sector/.

[94] ""A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor", *Business IT*, 21 de outubro de 2022.

[95] "Inovação e setor financeiro: simplificar é a regra", *Observador*, 29 de novembro de 2023.

[96] "A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor", *Business IT*, 21 de outubro de 2022.

[97] Flávia Magalhães, "IA e o setor financeiro: A revolução da tecnologia", *Consumidor Moderno*, 29 de fevereiro de 2024, https://consumidormoderno.com.br/ia-e-o-setor-financeiro-a-revolucao-da-tecnologia/.

Outra das tecnologias que impactaram de forma significativa o contexto de utilização de IA no setor bancário foi o aumento da utilização de robôs de investimento - "*robo-advisors*". Esta tecnologia consiste em sistemas automatizados que "utilizam algoritmos complexos para tomar decisões de investimento com base em objetivos, tolerância ao risco e dados do mercado". Algumas empresas oferecem plataformas que recorrem a IA com capacidade para gerir portfólios de investimentos. Este tipo de serviços permite consultoria financeira personalizada mais acessível que consultoria tradicional humana[98].

[98] Magalhães, "IA e o setor financeiro", 29 de fevereiro de 2024.

1.2. Ameaças

As ameaças à cibersegurança são transversais a todo o setor bancário, não havendo correlação entre a dimensão da instituição financeira e as perdas de informação devido a uma ameaça, segundo o relatório ""Cyber Risk for the Financial sector: A framework for Quantitative Assessment", publicado pelo International Monetary Fund (IMF) em 2020. A perda de informação e as possíveis consequências dessas perdas podem ter resultados desastrosos no normal funcionamento da instituição, independentemente da dimensão que a instituição apresente. Ao considerar as ameaças mais comuns direcionadas às instituições bancárias, é possível identificar 3 categorias: **Fraude, *Data Breach* e *Business Disruption***, sendo que cada uma destas ameaças/eventos causa um impacto diferente nas instituições[99]:

- As ameaças integradas no contexto de **Fraude** têm como objetivo aceder a informação confidencial dos clientes, incluindo as credenciais usadas pelos próprios em compras *online*, resultando em transferências de dinheiro não autorizadas e perdas de montantes. De acordo com o BCE, este tipo de eventos desceu 11% em 2021[100] e o valor total ascendeu a 4 mil milhões de euros em 2022 e a 2 mil milhões na primeira metade de 2023[101];
- Como já referido, uma ***data breach*** corresponde a um incidente onde há um ataque intencional por parte de um agente criminoso que lhe permite ganhar acesso não autorizado e divulgar dados sensíveis, confidenciais e protegidos. Este tipo de incidente, por ser mais complexo de detetar, pode ser apenas detetado e reportado meses ou anos após o início do incidente;
- ***Business Disruption*** é um incidente onde, através de ataques de DDoS, o agente malicioso impede o normal funcionamento das atividades da empresa, danificando a reputação da empresa e de recursos monetários[102].

Segundo o artigo "Cyber Risk: A Growing Concern for Macrofinancial Stability", publicado em abril de 2024, em 2020 houve uma estimativa de perdas de 1000 milhões de dólares, já em 2021 este número aumentou para 2500 milhões. Em 2019 o valor tinha sido de quase 2000 milhões. Podemos verificar que entre 2019 e 2020 ocorreu uma diminuição, mas em 2021 ocorreu um grande aumento tendo atingido o máximo nos últimos 4 anos[103].

De acordo com o *Threat Landscape Report* de 2023 da ENISA, os principais ataques passam pelo comprometimento da disponibilidade dos serviços e da informação (ataques de negação de serviço: "*Denial of Service", DoS*), ataques de *ransomware*, contando-se ainda ameaças relativas a dados (*data breaches* e furto de dados)[104].

---

[99] Antoine Bouveret, "*Cyber Risk for the Financial sector: A framework for Quantitative Assessment*", *Working Paper* do Fundo Monetário Internacional, junho de 2018, 4-5, https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.

[100] "Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures", European Central Bank, maio de 2023, https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html

[101] "ECB and EBA publish joint report on payment fraud", European Central Bank, agosto de 2024, https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html

[102] Bouveret, "*Cyber Risk for the Financial sector*", junho de 2018, 4-5.

[103] "Cyber Risk: A Growing Concern for Macrofinancial Stability", International Monetary Fund, abril de 2024, 7, https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3onlineannex.ashx

[104] ENISA, "ENISA Threat Landscape 2023", 19 de outubro de 2023, 14, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.

Em fevereiro de 2020, Christine Lagarde, presidente do Banco Central Europeu, veio a público, alertar que um ciberataque poderia originar uma crise financeira, afirmações estas que foram corroboradas pelo FSB (Financial Stability Board)[105]. De acordo com o Fórum Económico Mundial, o risco de ciberataques e de perdas monetárias subiu. Em 2017 houve cerca de 8 mil incidentes e em 2021 houve cerca de 11 mil incidentes[106].

O artigo "Cybersecurity threats in the banking sector" publicado em maio de 2022 refere que, no primeiro semestre de 2021, os ataques de chantagem aumentaram cerca de 1300 por cento em relação ao ano anterior. Este artigo também refere que os ataques digitais mais comuns no setor bancário são o furto ou o comprometimento de credenciais. Outro ataque muito comum são os ataques de *Phishing*, sendo este tipo de ataque muito complicado de gerir porque, normalmente, tem como alvos funcionários. O terceiro ataque mais comum são os ataques de *Ransomware* e, estes, tem como objetivo bloquear o acesso dos funcionários aos seus e dados aos dados da empresa, pedindo, normalmente, alguma quantia financeira para voltarem a ter acesso a estes[107].

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

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

[107] Oliver Gulyas e Gabor Kiss, “Cybersecurity threats in the banking sector”, junho de 2022, 1070 e 1071, https://ieeexplore.ieee.org/abstract/document/9804140.

De seguida, são abordados cinco dos maiores ataques de cibersegurança no setor bancário. Estes incidentes não só tiveram um impacto significativo nas instituições financeiras envolvidas, mas também revelaram vulnerabilidades nos seus sistemas:

- O ataque à JPMorgan Chase em 2014 foi um dos maiores comprometimentos de dados na história do setor financeiro. *Hackers* conseguiram invadir a rede da empresa, aceder a informações de cerca de 76 milhões de contas de clientes e 7 milhões de empresas. Foi explorada uma vulnerabilidade de segurança, o que permitiu furtar dados pessoais tais como: nomes, endereços, números de telefone e emails[108].
- Em fevereiro de 2016, um ciberataque ao Banco Central de Bangladesh resultou no furto de 81 milhões de dólares devido a uma vulnerabilidade no *software* SWIFT. Investigadores descobriram que os atacantes instalaram um *malware* no sistema SWIFT do banco, permitindo-lhes apagar registos de transferências fraudulentas. Embora a maioria das transações tenha sido bloqueada, uma parte significativa dos fundos foi desviada para as Filipinas. A SWIFT lançou uma atualização de *software* para mitigar o ataque e alertou os bancos para reforçar a segurança interna. O ataque foi altamente sofisticado e personalizado para a infraestrutura do Bangladesh Bank, os criminosos utilizaram credenciais administrativas comprometidas.[109]
- Cerca de 130 milhões de cartões de crédito e débito foram furtados em janeiro de 2018 do *website* da Heartland, através de um ataque de injeção de *SQL*. Os dados comprometidos no ataque foram: número de cartões de crédito, expiração dos mesmos e o nome dos titulares[110];
- Em setembro de 2017 ocorreu um comprometimento de dados na Equifax e cerca de 147 milhões de clientes foram afetados. Este comprometimento deveu-se a uma vulnerabilidade não corrigida no *Apache*. Os dados comprometidos no ataque foram: nome, data de nascimento, número da segurança social, carta de condução e números de cartões de crédito[111];
- Em maio de 2019, mais de 800 milhões de registos financeiros foram furtados devido a um erro no website da First American Financial Corp Data. Os dados comprometidos no ataque foram: nome, email e números de telemóvel dos compradores[112];
- Em 2019, a Capital One sofreu um ataque significativo quando um hacker conseguiu explorar uma falha numa configuração de segurança do servidor na nuvem. Este acesso indevido resultou numa exposição de dados de mais de 100 milhões de clientes, incluindo informações pessoais e financeiras, como números de contas e dados de crédito. A vulnerabilidade foi um erro na configuração da firewall[113];

[108] Jessica Silver-Greenberg, Matthew Goldstein e Nicole Perlroth, "JPMorgan Chase Hacking Affects 76 Million Households", The New York Times, outubro de 2014, https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.

[109] "Bangladesh Bank hackers compromised SWIFT software, warning issued", Reuters, 25 de abril de 2016, https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW/.

[110] Julia S. Cheney, "Heartland Payment Systems: Lessons Learned from a Data Breach", janeiro de 2010, 4, https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/d-2010-january-heartland-payment-systems.pdf?la=en&hash=EEAF5C96513D6E176D6C5312E4007061.

[111] "Equifax Data Breach Settlement", Federal Trade Commission, fevereiro de 2024, https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.

[112] AJ Dellinger, "Understanding The First American Financial Data Leak: How Did It Happen And What Does It Mean?", Forbes, maio de 2019, https://www.forbes.com/sites/ajdellinger/2019/05/26/understanding-the-first-american-financial-data-leak-how-did-it-happen-and-what-does-it-mean/.

[113] Shaharyar Khan et al., "A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned", novembro de 2022, https://dl.acm.org/doi/10.1145/3546068.

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[114], 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[115].
- **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[116].
- ***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[117].
- **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[118]. No caso, consideraram-se os colaboradores internos maliciosos.

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

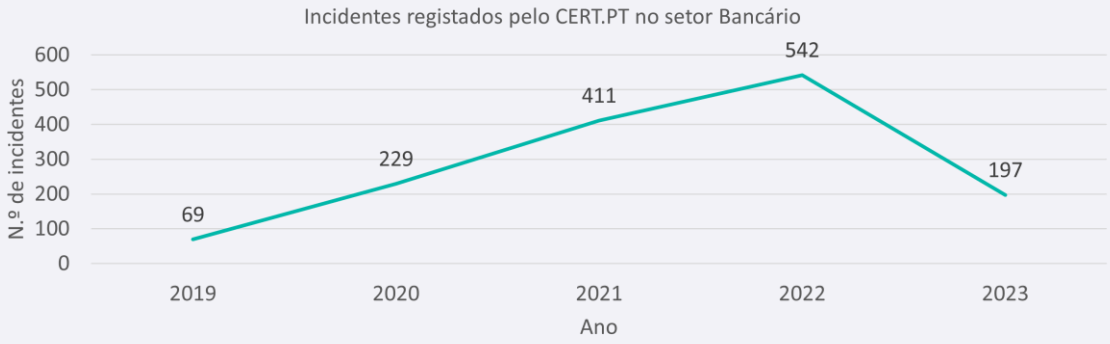
Tabela *5* - Agentes de ameaça mais prováveis (Bancário)

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

Legenda:
■ - Agente de ameaça provável

A atratividade do setor bancário para ciberataques é comprovada pelo número de ataques que o setor tem sofrido em Portugal. Segundo dados do CERT.PT, registaram-se, entre 2019 e 2023, 1448 ataques, sendo o setor que sofreu mais ataques[119].

Figura 1 - Número de incidentes no setor Bancário anualmente



(Fonte: CNCS, "Incidentes e Setores: 2019-2023", Conhecimento Situacional: Estatísticas, última atualização em 18 de setembro de 2024, https://www.cncs.gov.pt/pt/estatistica/)

[119] CNCS, "Incidentes e Setores", Conhecimento Situacional: Estatísticas, https://www.cncs.gov.pt/pt/estatistica/#cert.pt

1.3. Capacitação

No que diz respeito à formação e consciencialização em matéria de cibersegurança no setor bancário, a European Banking Authority (EBA) dinamiza sessões de formação e *workshops* para entidades supervisoras e reguladoras pertencentes aos Estados-Membros. Adicionalmente, inclui nos requisitos para os reportes de riscos exigidos às entidades supervisionadas a inclusão de riscos relacionados com tecnologias de informação e comunicação (TIC) e cibersegurança, tornando-se temáticas abordadas com frequência nos relatórios de avaliação de riscos publicados. O *FinTech Knowledge Hub,* pertencente à EBA, contribui também para a formação das autoridades competentes nestas áreas.

Também a Federação Bancária Europeia (EBF, no inglês) contribui para a formação e sensibilização em contexto de cibersegurança. O seu grupo de trabalho de cibersegurança promove campanhas e iniciativas de sensibilização com o objetivo de melhorar as capacidades de cibersegurança no *staff* das empresas do setor. Promove também eventos e iniciativas de diversos tipos com o objetivo comum de contribuir para uma melhor cibersegurança.

No contexto português, a sensibilização para as questões de cibersegurança no setor bancário tornou-se uma preocupação, principalmente, para o BdP, autoridade supervisora e reguladora do sistema financeiro. Desenvolve mecanismos de sensibilização em conjunto com a EBA. O BdP apresenta na sua página um separador dedicado inteiramente à sensibilização e segurança aquando da utilização dos diferentes canais digitais, nomeadamente quando estes são usados para efetuar pagamentos, transações ou outro tipo de operações bancárias.

Os tópicos abordados neste separador estão descritos mais detalhadamente na tabela seguinte:

Tabela *6* - Capacitação no setor Bancário

Tópico	Descrição
Risco	*Phishing* *Pharming* *Spyware* *SIM card swap* *Shoulder surfing*
Cuidados a ter	Cuidados a observar na realização de operações bancárias através de canais digitais Cuidados especiais a observar no homebanking Cuidados especiais a observar em pagamentos na internet
Big Data	Riscos para os consumidores Precauções a tomar pelos consumidores

A título de exemplo, o BdP lançou, a 7 de fevereiro de 2023, a campanha *#ficaadica,* que tem como principal objetivo o de sensibilizar o público em geral, nomeadamente a população jovem e adulta, para os riscos de aceder a produtos e serviços bancários digitais. Para tal, o BdP preparou uma brochura e vídeos explicativos dos riscos a evitar durante a navegação online, em especial, assuntos relacionados com os pagamentos e transferências online[120].

Na brochura acima mencionada, é possível encontrar tópicos como: conhecer os riscos que podem surgir durante a navegação na Internet; como aceder corretamente e de forma segura a conta bancária online; como abrir uma conta bancária à distância de forma segura e como fazer compras online de forma segura[121]. Na análise do "Plano Estratégico do BdP 2021-2025", é possível entender que existe preocupação relativamente à proteção do mercado bancário (leia-se em Orientação Estratégica 2). Nesta orientação, o BdP define várias prioridades estratégicas como acompanhamento da evolução dos modelos de negócio das instituições com foco em dimensões como a transformação digital e resiliência operacional; revisão de modelos de análise de risco de BCFT do setor financeiro ou dinamização de um estratégia médio/longo prazo de literacia financeira digital para Portugal, promovendo a inclusão financeira através da utilização adequada e segura dos canais digitais no acesso a produtos bancários de retalho[122].

Em 2021, espelhado no relatório de Atividades e contas do BdP, foram realizadas diferentes atividades em conjunto com as entidades financeiras: um workshop relativo à temática de inovação digital com especialistas e indústria, a criação de um Fórum com a Indústria para a Cibersegurança e Resiliência Operacional - com representantes do setor bancário, do prestador de serviços críticos de pagamento e da autoridade nacional de cibersegurança - e ações de diálogo com as instituições supervisionadas para apresentar as novidades legislativas em matéria de planeamento da resolução. Foi também iniciada a implementação do quadro de referência europeu para a realização de testes de intrusão em Portugal (TIBER-EU)[123].

[120] Banco de Portugal, "Campanha #ficaadica. Banco de Portugal divulga brochura com conselhos sobre o acesso a produtos e serviços bancários digitais", 7 de fevereiro de 2023. https://www.bportugal.pt/comunicado/campanha-ficaadica-banco-de-portugal-divulga-brochura-com-conselhos-sobre-o-acesso.

[121] Banco de Portugal, "Campanha #ficaadica".

[122] Banco de Portugal, "Plano Estratégico 21-25", 14.

[123] Banco de Portugal, "Relatório do Conselho de Administração - Atividade e Contas 2021", 43.

1.4. Investimento em cibersegurança

O relatório "*NIS Investments*" de 2023, elaborado pela ENISA, indica que o setor bancário tem sido, a nível europeu, o que mais investe em segurança da informação, em comparação com os restantes setores. Em média, cada OSE do setor bancário europeu tem investido, por ano, cerca de 10 milhões de euros em segurança da informação. A mediana desse investimento, no entanto, ronda os 2 milhões de euros de investimento anual por OSE[124]. A ENISA opta por apresentar os dois valores (média e mediana) por considerar que a mediana oferece uma visão mais próxima do que é a realidade de investimento da maioria dos OSE, uma vez que o valor da média é de certo modo "deturpado" pelas entidades bancárias de maior dimensão e que realizam investimentos mais avultados[125]. O mesmo relatório indica ainda que o investimento realizado em segurança da informação por este setor tem representado, de 2020 a 2022, cerca de 7% do investimento global realizado nas TIC[126].

A nível nacional, as demonstrações financeiras e relatórios de contas tendem a não mencionar o investimento específico em cibersegurança, mas sim os gastos com equipamento ou serviços de informática. Por exemplo, o Relatório de Contas do Novo Banco indica gastos com serviços de informática na ordem de quase 44 milhões de euros em 2022 e de 46,4 milhões de euros em 2023[127]. O mesmo relatório indica que o valor do equipamento informático enquanto ativo tangível foi avaliado em praticamente 118 milhões de euros em 2022 e em 126 milhões de euros em 2023[128].

No caso do banco Santander Totta, o Relatório Anual de 2023 indica a despesa realizada com a manutenção de *hardware* e de *software*. Em 2022, esta despesa foi de cerca de 74 milhões de euros e, em 2023, de cerca de 88 milhões de euros[129].

No relatório de contas do Banco Montepio é referenciada uma rubrica destinada a serviços especializados em informática que totalizou os 13,2 milhões de euros em 2022 e 16,4 milhões de euros em 2023[130].

Em relação ao Banco Português de Investimento (BPI), contabilizaram-se 46,7 milhões de euros em 2022 e 65,5 milhões de euros em 2023 destinados a serviços de comunicações e informática[131].

No que diz respeito à Caixa Geral de Depósitos, verifica-se que as despesas com serviços de informática totalizaram em 2022, 47,6 milhões de euros e, em 2023, 42,77 milhões de euros[132]. A estas acrescem ainda as despesas com serviços de informações, que representaram gastos de 4,44 milhões de euros em 2022 e gastos de 4,56 milhões de euros em 2023[133].

---

[124] ENISA, "NIS Investments", novembro de 2023, 21, https://www.enisa.europa.eu/publications/nis-investments-2023.

[125] ENISA, "NIS Investments", 16.

[126] ENISA, "NIS Investments", 24.

[127] Novo Banco, "Relatório e Contas 2023", 28 de fevereiro de 2024, 349, https://www.novobanco.pt/content/dam/novobancopublicsites/docs/pdfs/divulga%C3%A7%C3%B5es-financeiras/2023/relat%C3%B3rio-e-contas/RC%20novobanco%202023.pdf.coredownload.inline.pdf.

[128] Novo Banco, "Relatório e Contas 2023", 370.

[129] Banco Santander Totta, "Annual Report 2023: Proposal", 17 de maio de 2024, 180, https://www.santander.pt/pdfs/investor-relations/santander-totta-sa/relatorio-e-contas/2023/BST_Annual_Report_2023_non_official_non_audited.pdf.

[130] Banco Montepio, "Relatório e Contas 2023", 15 de abril de 2024, 183, https://www.bancomontepio.pt/content/dam/montepio/pdf/institucional/investor-relations/relatorios-comunicados-e-informacao-financeira/2023/informacao-anual/relatorio-contas-anual-banco-montepio-2023.pdf.

[131] Banco Português de Investimento, "Relatório e Contas 2023", 368, https://www.bancobpi.pt/contentservice/getContent?documentName=PR_UCMS02106736.

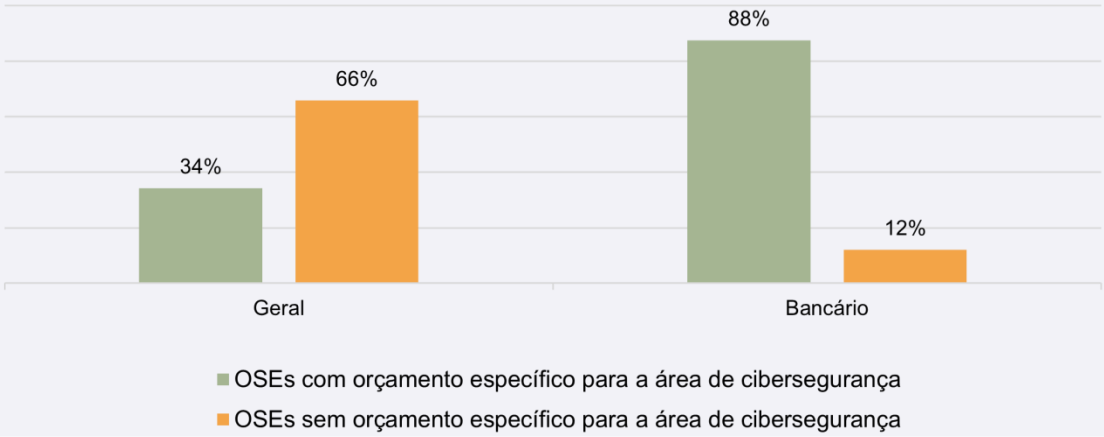
[132] Caixa Geral de Depósitos, "Relatório de Gestão e Contas 2023", 203, https://www.cgd.pt/Investor-Relations/Informacao-Financeira/CGD/Relatorios-Contas/Pages/Relatorios-Contas-CGD.aspx.

[133] Caixa Geral de Depósitos, "Relatório de Gestão e Contas 2023", 203.

Apesar de estes relatórios não indicarem os montantes específicos alocados à cibersegurança, é possível verificar que esta tem sido incluída nos objetivos e estratégias definidos para os próximos anos, e que têm sido também realizadas apostas na certificação das entidades bancárias em *standards* internacionais, como a ISO 27001 ou CMMI[134], bem como na formação dos colaboradores. Por exemplo, o relatório do Banco Montepio indica terem sido contabilizadas mais de cinco mil horas de formação em cibersegurança e outras mais de cinco mil horas de formação no âmbito da Continuidade de Negócio durante o ano de 2023[135], e o relatório da CGD indica ter realizado sessões de formação em cibersegurança especialmente dedicadas à temática do *ransomware*, entre outras[136].

De acordo com o questionário realizado, cerca de 88% 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



[134] Banco Português de Investimento, "Relatório e Contas 2023", 138.
[135] Banco Montepio, "Relatório e Contas 2023", 34.
[136] Caixa Geral de Depósitos, "Relatório de Gestão e Contas 2023", 710.

Relativamente às áreas de aplicação do orçamento de cibersegurança, 89% aplica na segurança das redes, 81% na aquisição de *hardware* e *software,* 77% na análise de segurança, 73% na capacitação em tecnologia e 72% na gestão de vulnerabilidades (**Gráfico 110 e 110.3**).

Gráfico 110 - Áreas de aplicação dos orçamentos específicos para cibersegurança

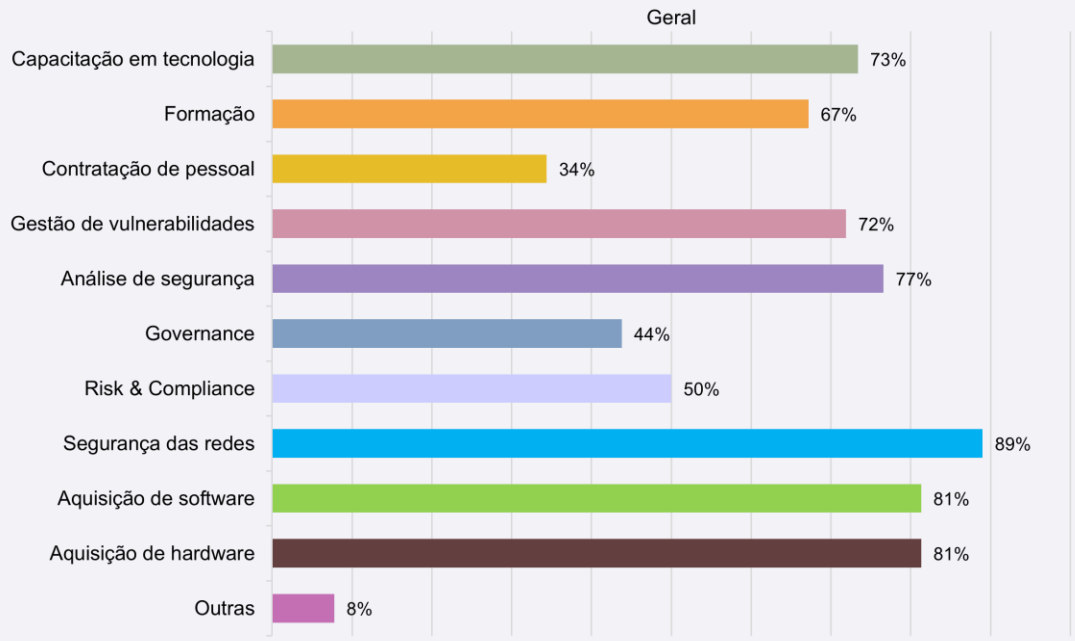
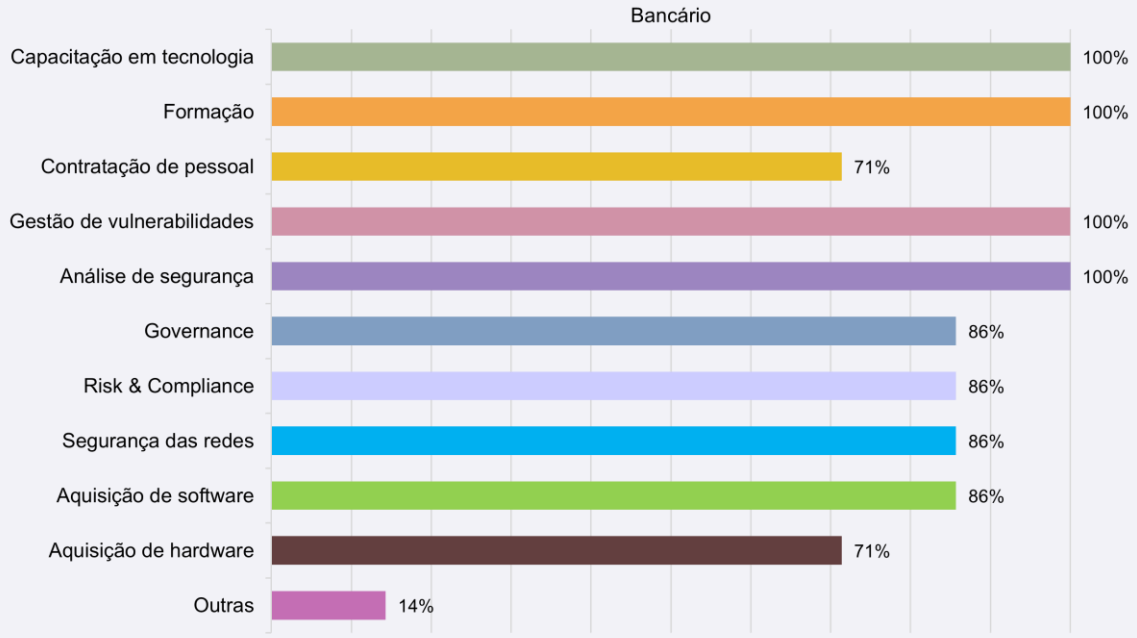
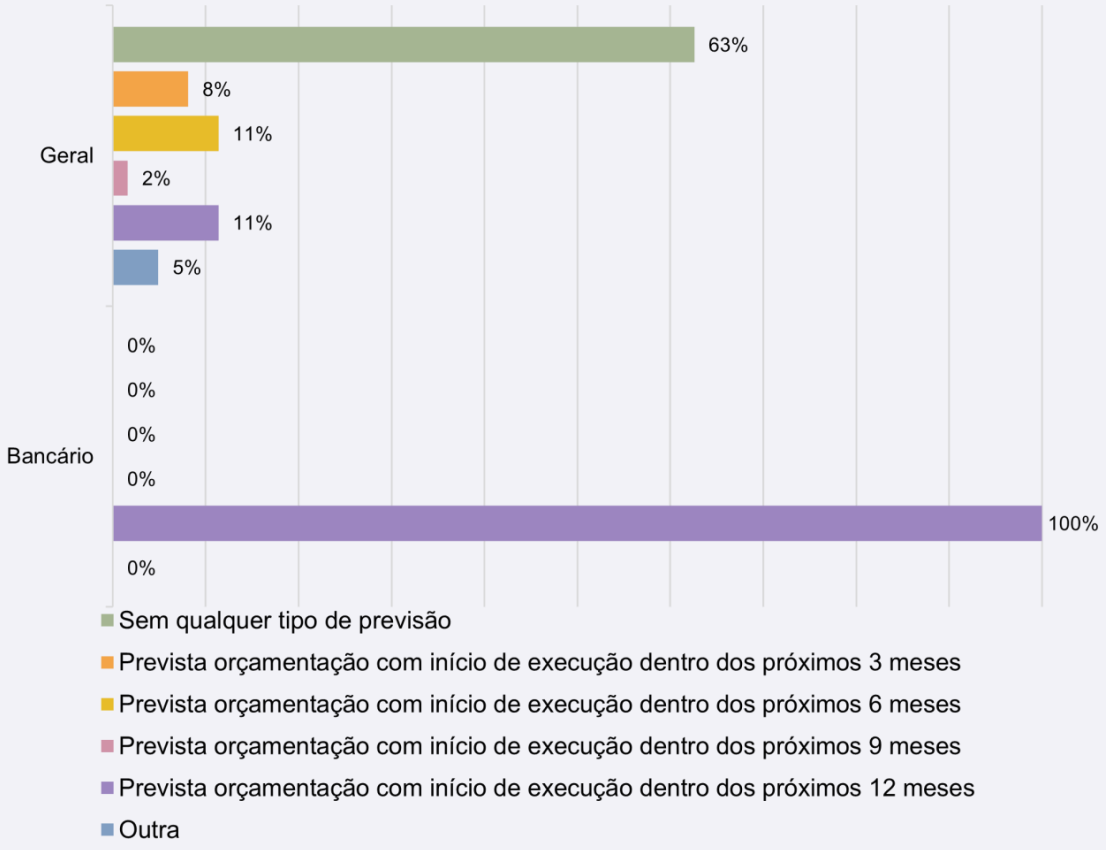


Gráfico 110.3 - Áreas de aplicação dos orçamentos específicos para cibersegurança



Por fim, das entidades que não possuem orçamento específico para a área de cibersegurança, 100% tem previsto a orçamentação dentro dos próximos 12 meses (**Gráfico 111**).

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



Embora não se tenham verificado, nos documentos mencionados, rubricas destinadas especificamente à cibersegurança, algumas ações enquadradas na orçamentação de informática contribuem para uma maior resiliência digital e operacional tais como manutenção de sistemas informáticos, atualização de *hardware* e *software,* controlo de acessos, promoção de reportes a autoridades de supervisão, entre outros.

1.5. RJSC e legislação setorial

O setor bancário, pelo papel que desempenha na economia e na sociedade, e pela gestão de avultados volumes de capital e informações sensíveis que realiza, tanto a nível individual como empresarial, tem forçosamente de ser um setor seguro em várias vertentes. O cumprimento de normas de segurança e transparência é essencial para garantir a proteção dos depósitos, a resiliência contra fraudes e ataques, bem como a continuidade dos serviços. O setor obedece assim a um quadro regulatório e legal rigoroso, no qual é contemplada a cibersegurança.

O principal diploma que rege o setor bancário é o Decreto-Lei n.º 298/92, de 31 de dezembro (1992), também conhecido como Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF). Embora o principal foco do diploma seja a supervisão das instituições de crédito e sociedades financeiras, são também incluídas disposições acerca da necessidade de informar o Banco de Portugal sobre os "processos de segurança e controlo no domínio informático"[137], de manter um inventário "pormenorizado e descrição dos principais sistemas de informação de gestão utilizados (...) incluindo os destinados à gestão de risco, (...) com discriminação por entidades, funções críticas e linhas de negócio estratégicas"[138], e ainda "medidas de gestão de risco", nas quais se incluem as medidas de gestão do risco relacionadas com a cibersegurança.

Em 2007, a Diretiva 2007/64/CE, relativa aos serviços de pagamento no mercado interno (ou Diretiva dos Serviços de Pagamento - PSD), criada para regular os serviços de pagamento na UE, impôs também obrigações de segurança relativamente aos pagamentos, tais como o de garantir formas de autenticação segura, de modo que "apenas o utilizador de serviços de pagamento que tenha direito a utilizar o referido instrumento"[139] o utiliza. Dito de outra forma, a Diretiva impôs obrigações de segurança ao nível da autenticação dos utilizadores.

Em 2015, esta Diretiva foi atualizada através de uma outra, a Diretiva (UE) 2015/2366, de 25 de novembro (PSD 2), de modo a responder às novas realidades digitais, como o crescimento do comércio eletrónico e a emergência de novos atores no setor dos pagamentos, como as *fintechs*. Ao nível da cibersegurança, a Diretiva veio reforçar as obrigações relativas à autenticação segura dos clientes, impondo a necessidade da "autenticação forte do cliente (...) baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é)"[140], ou seja, autenticação de dois passos ou autenticação multifator (MFA), de modo a prevenir acessos e transações não autorizadas, bem como fraudes.

[137] Decreto-Lei n.º 298/92, de 31 de dezembro, "Regime Geral das Instituições de Crédito e Sociedades Financeiras - RGICSF", artigo 120.º, alínea h), *Diário da República*, https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1992-70072322.

[138] Decreto-Lei n.º 298/92, artigo 138.º-AH, alínea, q).

[139] Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007 relativa aos serviços de pagamento no mercado interno, artigo 57.º, n.º1, alínea a), *Jornal Oficial da União Europeia*, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32007L0064.

[140] Diretiva (UE) 2015/2366 do Parlamento europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, artigo 4.º, n.º 30, *Jornal Oficial da União Europeia*, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366.

No ano seguinte, 2016, foi publicada a Diretiva (UE) 2016/1148, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União[141], também conhecida como Diretiva SRI ou Diretiva NIS, cuja transposição para o ordenamento jurídico nacional, através da Lei n.º 46/2018, de 13 de agosto, estabeleceu o Regime Jurídico da Segurança do Ciberespaço (RJSC)[142]. Foi o RJSC que identificou o setor bancário como um setor de operadores de serviços essenciais e lhe impôs obrigações ao nível do cumprimento de medidas técnicas e organizativas adequadas para a gestão dos riscos relativos à segurança das redes e da informação, bem como de adoção de medidas para evitar incidentes e minimizar os impactos dos mesmos. Esta mesma legislação impôs a obrigatoriedade de reporte de incidentes de impacto relevante ao CNCS[143]. O RJSC viria a ser depois complementado em 2021 através do Decreto-Lei n.º 65/2021, de 30 de julho, que o regulamenta, ou seja, estabelece como determinadas normas do RJSC devem ser cumpridas. Deste Decreto-Lei decorrem obrigações como a designação de um ponto de contacto permanente pelas entidades abrangidas para comunicação com o CNCS, a designação de um responsável de segurança; a necessidade de elaborar e manter atualizado um inventário de ativos; um plano de segurança, que deve incluir a política de segurança e medidas de segurança adotadas; a elaboração de um relatório anual com informações sobre as atividades desenvolvidas ao nível da segurança e estatísticas semestrais de todos os incidentes e análise agregada dos incidentes de segurança com impacto relevante ou substancial[144]. É também imposta a necessidade de realizar análises de risco anuais e são definidos os tempos para a notificação de incidentes de impacto relevante ao CNCS[145].

Depois, em 2022, foi publicado o Regulamento (UE) 2022/2554, relativo à resiliência operacional digital do setor financeiro, mais conhecido como Regulamento DORA (*Digital Operational Resilience Act*). Este regulamento abrange diversas entidades. Para além das bancárias, o Regulamento DORA abrange ainda entidades como as que compõem as infraestruturas do mercado financeiro (plataformas de negociação e contrapartes centrais), empresas de seguros, instituições de crédito, instituições de pagamento, empresas de investimento, entre várias outras[146]. A estas "entidades financeiras", como são comummente designadas no Regulamento DORA, são impostas diversas obrigações, que passam pela gestão do risco associado às tecnologias da informação e comunicação (TIC), gestão dos serviços e ferramentas TIC prestados por terceiros, gestão de sistemas, protocolos e ferramentas TIC, atividades de proteção e prevenção, deteção, resposta e recuperação em situação de incidente, reporte de incidentes, testes de resiliência operacional (como análises de vulnerabilidades, avaliações da segurança das redes, análises da segurança física, revisões do código fonte, entre outros) e ainda testes de intrusão com base em ameaças (*Threat-Led Penetration Testing - TLPT*), testes que exigem uma ampla recolha de informações sobre ameaças (*Threat Intelligence*) às quais uma entidade financeira possa estar exposta[147].

---

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

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

[143] Lei n.º 46/2018, artigo 13.º.

[144] Decreto-Lei n.º 65/2021, de 30 de julho, artigos 4.º a 8.º, *Diário da República*, https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

[145] Decreto-Lei n.º 65/2021, artigo 10.º e artigos 11.º a 15.º.

[146] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro, artigo 2.º, *Jornal Oficial da União Europeia*, https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554.

[147] Regulamento (UE) 2022/2554, artigos 6.º a 27.º.

Essa recolha deverá passar tanto pelas informações sobre ameaças cedidas pelas próprias entidades, como pela investigação, por exemplo, de informações confidenciais, como credenciais de utilizadores, divulgadas ou expostas na *dark web*[148]. A conformidade com o Regulamento DORA será obrigatória a partir de 17 de janeiro de 2025.

Para além desta legislação, verificam-se ainda as recomendações, circulares e instruções das entidades reguladoras para o setor. Embora a autoridade reguladora do setor seja o BdP, podem surgir recomendações conjuntas para todo o setor financeiro, publicadas pelo Conselho Nacional de Supervisores Financeiros (CNSF), composto pelo BdP, pela Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) e pela Comissão do Mercado de Valores Mobiliários (CMVM). A título de exemplo, o CNSF aprovou, em 2021, as Recomendações sobre a Gestão da Continuidade de Negócio, que atualizam as Recomendações aprovadas em 2010. Nestas Recomendações é possível encontrar orientações destinadas à gestão do risco das TIC, à sua resiliência em situações de catástrofes naturais, como incêndios, inundações, falhas graves de energia; às infraestruturas alternativas, aos planos de continuidade de negócio, recuperação de desastres, e de comunicação, bem como à realização de testes, simulações e treinos no âmbito da continuidade de negócio[149].

Depois de seis anos passados desde a publicação da Diretiva NIS, foi publicada em 2022 a Diretiva (UE) 2022/2555[150], mais comummente conhecida como NIS 2, de modo a atualizar a Diretiva anterior. A nova Diretiva visa agora dois tipos de setores: "setores de importância crítica"[151] e "outros setores críticos"[152]. 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.

Apesar de a Diretiva NIS 2 abranger mais entidades nalguns setores, tal não acontece no setor bancário. As entidades visadas continuam a ser as mesmas já abrangidas pela Diretiva anterior. 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[153]. 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[154].

---

148 Banco Central Europeu, "TIBER-EU Guidance for Target Threat Intelligence Report", julho de 2020, 7, https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.

149 Banco de Portugal, "Recomendações sobre Gestão da Continuidade de Negócio", Carta Circular n.º CC/2021/00000047, 2021, 21, https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares//463107899_6.docx.pdf.

150 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

151 Diretiva (UE) 2022/2555, Anexo I.

152 Diretiva (UE) 2022/2555, Anexo II.

153 Diretiva (UE) 2022/2555, artigo 20.º, n.º 1.

154 Diretiva (UE) 2022/2555, artigo 21.º, n.º 2.

A nova Diretiva encoraja ainda a que sejam celebrados, entre as entidades abrangidas, de forma voluntária e quando pertinente, acordos de partilha de informações, através dos quais possam proceder ao intercâmbio de informações sobre cibersegurança. O Regulamento DORA inclui provisões semelhantes incentivando este tipo de acordos para o intercâmbio de "informações específicas e sensíveis relativas a ciberataques, nomeadamente indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração"[155]. Já a Diretiva NIS 2 estabelece que as informações partilhadas à luz destes acordos podem ser relacionadas com "ciberameaças, quase incidentes, vulnerabilidades, técnicas e procedimentos, indicadores de exposição a riscos, táticas hostis, informações específicas sobre perpetradores de ameaças, alertas de cibersegurança e recomendações relativas à configuração das ferramentas de cibersegurança para a deteção de ciberataques"[156].

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

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

1.6. Standards e boas práticas aplicáveis

A tabela seguinte sumariza os *standards* e boas práticas aplicáveis ao setor bancário, segundo a ENISA[157]:

Tabela 7 - Standards e Boas Práticas (Bancário)

Standards	Boas práticas
• ISO/TR 13569:2005; • Gramm–Leach–Bliley Act; • Sarbanes–Oxley Act; • Payment services (PSD 2) - Directive (EU) 2015/2366; • EBA on the security of internet payments; • ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services; • American National Standards Institute (ANSI) X9 series.	• Payment Card Industry Data Security Standard (PCI DSS); • Basel II; • Draft Guidelines on the security measures for operational and security risks of payment services under PSD2; • CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure; • SEC OCIE Cybersecurity.

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

- **ISO/TR 13569:2005**: Orientações para o desenvolvimento da segurança da informação das instituições da indústria financeira[158];
- **Gramm–Leach–Bliley Act:** Lei dos EUA que exige que instituições financeiras protejam a confidencialidade e a segurança das informações dos clientes[159];
- **Sarbanes–Oxley Act:** Lei dos EUA com disposições que afetam a governação das empresas, a gestão de riscos, auditorias e os relatórios financeiros das empresas públicas, incluindo disposições destinadas a dissuadir e punir a fraude e a corrupção[160];
- **Payment services (PSD 2) - Directive (EU) 2015/2366:** Diretiva da UE com o objetivo de modernizar os serviços de pagamento na Europa, promovendo a inovação e aumentando a segurança nas transações[161];
- **EBA on the security of internet payments:** Orientações da EBA para melhorar a segurança dos pagamentos pela Internet, reduzindo riscos de fraude e aumentando a proteção ao consumidor[162];

[157] ENISA, "Mapping of OES Security Requirements", 2.

[158] "ISO/TR 13569:2005", ISO, novembro de 2005, https://www.iso.org/standard/37245.html

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

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

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

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

- **ISO/IEC 27015:2012 Information technology - Security techniques – Information security management guidelines for financial services**: Fornece orientações específicas para a gestão da segurança da informação no setor financeiro. Tem como foco assegurar que as instituições financeiras implementem controlos adequados de forma a proteger dados sensíveis contra ameaças de cibersegurança[163];
- **American National Standards Institute (ANSI) X9 series:** Conjunto de normas que definem padrões de segurança para transações financeiras, garantindo a integridade e confidencialidade das mesmas[164];
- **Payment Card Industry Data Security Standard (PCI DSS):** Conjunto de padrões de segurança para proteger as informações dos cartões de pagamento e evitar fraudes[165];
- **Basel II:** Acordo internacional que estabelece normas para a regulação bancária[166];
- **Draft Guidelines on the security measures for operational and security risks of payment services under PSD2:** Orientações preliminares para medidas de segurança e gestão de riscos operacionais nos serviços de pagamento sob a PSD2[167];
- **CPMI-IOSCO Guidance on cyber resilience for financial market infrastructure:** Diretrizes para aumentar a resiliência de cibersegurança das infraestruturas dos mercados financeiros[168];
- **SEC OCIE Cybersecurity:** Diretrizes da SEC (Securities and Exchange Commission - EUA) para avaliar a postura de cibersegurança das empresas financeiras[169].

De forma complementar à legislação aplicável, entidades pertencentes ao setor têm ainda de cumprir com *standards* nacionais e internacionais que fornecem orientações mais específicas e concretas na gestão de temáticas relacionadas com NIS.

A utilização destes *standards* permite melhorar as medidas de segurança nas entidades abrangidas e facilita a supervisão por parte das autoridades supervisoras e regulatórias, permitindo-lhes aferir a efetiva aplicação dos regulamentos e políticas.

163 "ISO/TR 27015:2012", ISO, dezembro de 2012, https://www.iso.org/standard/43755.html

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

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

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

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

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

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

Outros exemplos de *standards* nacionais e internacionais aplicáveis ao setor bancário são os seguintes:

- ***Minimum Requirements for Risk Management* da *German Federal Financial Supervisory Authority***: a Autoridade Supervisora da Alemanha Financeira Federal *(German Federal Financial Supervisory Authority)* fornece uma *framework* para a gestão de riscos em institutos financeiros alemães. A *framework* endereça as responsabilidades da gestão de topo, requisitos gerais para a gestão de riscos e de recursos (incluindo recursos humanos, sistemas, instalações técnicas, processos e planos de contingência)[170].
- ***Banking Act* da *German Federal Financial Supervisory Authority:*** a Autoridade Supervisora da Alemanha Financeira Federal (BaFin) utiliza o *Banking Act* como instrumento de supervisão bancária. O *Banking Act* define as regras que instituições bancárias devem cumprir no decurso da sua operação. As regras são definidas por forma a permitir o funcionamento adequado do sistema bancário, incluindo um conjunto de requisitos alto-nível[171].
- ***National Banking Act* do Banco Nacional da Suíça:** o *Banking Act* do Banco Nacional da Suíça obriga a que este supervisione os sistemas que operam compensações, liquidações e outros instrumentos financeiros. A legislação também se aplica a operadores que têm sede no estrangeiro, desde que partes substanciais da operação ou *stakeholders* chave estejam sedeados na Suíça[172].
- ***Management of operational risk*, *standard* da Autoridade de Supervisão Financeira da Finlândia (*Finnish Financial Supervisory Authority*):** este *standard* define requisitos para a gestão de riscos operacionais em organizações financeiras. Nele são detalhadas instruções como: gestão de processos, recursos humanos, sistemas de informação e pagamentos, segurança da informação, planeamento de continuidade e riscos legais. Preocupa-se com os sistemas e serviços de pagamento, identificando oito controlos que o banco deverá implementar, como caracterização dos sistemas de pagamentos, meios de pagamento, princípios para a transferência de fundos nos sistemas de pagamentos, garantia de controlos internos de eficiência e a segurança dos serviços de pagamentos[173].

No setor bancário e em todo o setor financeiro, a ENISA tem um papel ativo no apoio aos estados-membro da UE na resposta a crises decorrentes de incidentes de cibersegurança. O apoio prestado passa pela consciencialização e pela estruturação de procedimentos de resposta a incidentes, contribuindo para uma melhor tomada de decisão em momentos de resposta a crises. Adicionalmente, a ENISA gere o programa de exercícios Pan-Europeus denominado *Cyber Europe*[174].

[170] "Risk management", Federal Financial Supervisory Authority, dezembro de 2017, https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Risikomanagement/risikomanagement_node_en.html

[171] "Gesetz iiber das Kreditwesen", Banking Act ofthe Federal Republic of Germany, setembro de 1998, https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf

[172] "The SNB's legal basis", Swiss National Bank, https://www.snb.ch/en/the-snb/organisation/legal-framework

[173] "Management of operational risk in supervised entities of the financial sector", FIN-FSA, agosto de 2014, https://www.finanssivalvonta.fi/globalassets/en/regulation/fin-fsa-regulations-and-guidelines/2014/08_2014/08_2014.m4_en.pdf

[174] ENISA, "Cyber Europe Programme", 2024, https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme

Para além da ENISA, as seguintes estruturas contribuem também para a gestão de crises de cibersegurança na UE[175]:

- *European Association for Secure Transactions (EAST)*: apoia na identificação de incidentes e na preparação de ações qualificadas de resposta nas várias localizações;
- *Nordic Financial CERT*: apoia os estados-membro na resposta a incidentes e na recuperação dos mesmos;
- *European Payments Council*: promove uma melhor colaboração entre fornecedores de serviços de pagamentos através do grupo de trabalho *Payment Scheme Fraud Prevention Working Group* (PSFPWG);
- *FS-ISAC*: fornece mecanismos de resposta e comunicação de crises, assim como recursos humanos de suporte, transversais às várias indústrias.

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

1.7. Desafios

De um modo geral, as grandes instituições bancárias a nível internacional demonstram uma boa capacidade de incorporar a gestão de risco na gestão da segurança dos seus sistemas de informação. Para isso, as entidades do setor seguem Sistemas de Gestão da Segurança da Informação (ISMS) e implementam controlos e *standards* como parte integrante do seu modelo de governo da segurança. Adicionalmente, muitos bancos são certificados em normas internacionais tais como a ISO 27001 e a ISO 22301, que garantem a implementação de boas práticas na área de *IT Governance* e que contribuem para uma melhor gestão de riscos, nomeadamente riscos de cibersegurança.

A gestão de riscos no setor bancário não se foca apenas em temas relacionados com a NIS. A gestão de riscos assenta em três pilares:

- Riscos financeiros: Qualquer tipo de risco associado ao financiamento de empresas, nomeadamente risco de crédito, risco de liquidez e risco operacional;
- Riscos operacionais: Qualquer tipo de risco associado às operações do dia-a-dia de uma determinada empresa;
- Riscos de segurança da informação: Qualquer risco associado à vulnerabilidade de certos ativos de uma empresa e que impacto no negócio caso estes sejam atingidos por um determinado incidente.

Apesar de os temas da NIS estarem em maior destaque nos riscos de segurança de informação, os restantes riscos, associados a contextos financeiro e operacional, direta ou indiretamente, podem ter impacto também nos próprios riscos de segurança de redes e informação. Isto faz com que a temática da NIS seja considerada transversal aos três pilares de gestão de riscos pelos atores do setor bancário. Uma das maiores vulnerabilidades e desafios neste setor, segundo o FMI, é a confiança colocada em infraestruturas críticas e a dependência do setor de redes altamente interligadas. As infraestruturas críticas do setor bancário abrangem vários sistemas, como sistemas de pagamento e sistemas de liquidação, e várias instituições/plataformas essenciais à infraestrutura como plataformas de *trading* e contrapartes centrais. Esta dependência, juntamente com a centralização de várias atividades numa única infraestrutura, constituem um risco muito elevado, que pode atingir os 3 pilares descritos anteriormente[176].

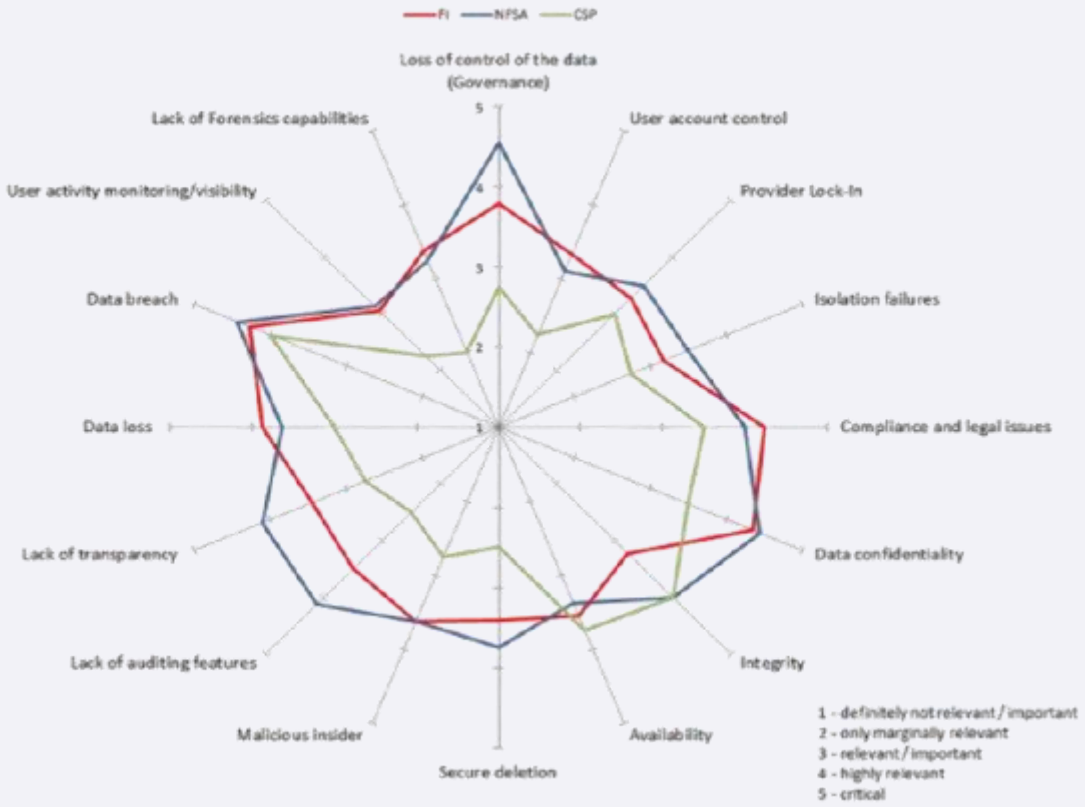
No que diz respeito a serviços *cloud*, segundo ENISA, é possível identificar as diferentes preocupações demonstradas pelas instituições financeiras, pelas autoridades nacionais de supervisão financeira (ANSF) e pelos prestadores de serviços de *cloud*. Essas preocupações são as seguintes:

- As instituições financeiras consideram que os principais desafios a que estão sujeitos estão ao nível da confidencialidade dos dados, *data breach*, questões legais e de conformidade.
- No caso das ANSF, consideram a falta de transparência e falta de recursos de auditoria como os principais desafios a superar.
- Considerando os prestadores de serviços *cloud*, os principais desafios a superar estão relacionados com a integridade e disponibilidade dos dados e *data breach*[177].

[176] Bouveret, "*Cyber Risk for the Financial sector",* 11, junho de 2018.

[177] ENISA, "*Secure Use of Cloud Computing in the Finance sector*", 7 de dezembro de 2015, 26.

Figura 2 - Perda de controlo de informação no setor Bancário



(Fonte: ENISA, "Secure Use of Cloud Computing in the Finance Sector", 7 de dezembro de 2015, 26, https://www.enisa.europa.eu/publications/cloud-in-finance)

De acordo com o documento "Desafios da transformação digital para o Setor Bancário", um dos grandes desafios é a criação de uma *API* denominada por *Open Banking* e, esta, tem como grande objetivo evoluir o setor para plataformas mais ágeis, distribuídas e escaláveis. Com o *Open Banking*, as contas passam a ser possíveis de serem acedidas por outras entidades, sendo assim possível, por exemplo, levantar montantes em qualquer país da UE apenas utilizando uma aplicação. O maior desafio será as *Big Tech*, visto estas fornecerem soluções de pagamento *end-to-end* em concorrência com o banco, alavancando os pagamentos tradicionais. É importante assim adaptar a regulação às *Big Tech* e bancos digitais, garantindo assim um tratamento justo e equilibrado entre os incumbentes e os novos operadores. Outro ponto crucial é remover barreiras à inovação, adaptando os *standards* às novas tecnologias[178].

[178] Hélder Rosalino, "Desafios da transformação digital para o Setor Bancário", Fintech House Lisboa, janeiro de 2020, 8-18, https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20200123.pdf.

1.8. Recomendações

O relatório mencionado ("*Network and Information Security in the Finance Sector*", ENISA) resulta na análise ao panorama da cibersegurança no setor financeiro com a formulação das seguintes recomendações:

- **Criação do *European Security Guidebook***: definição de um conjunto de linhas orientadoras comuns que apresentem uma solução possível para a implementação de medidas uniformizadas de segurança operacional ao invés de regular os níveis de serviço. No contexto dos operadores do setor financeiro, a utilização de *standards* é a medida utilizada com maior frequência para garantir a prevenção, deteção e resposta a incidentes de segurança. Adicionalmente, é crucial definir linhas orientadoras transversais que facilitem a avaliação custo-benefício de investimentos em cibersegurança e o envolvimento da gestão de topo na tomada de decisão relacionada com cibersegurança;
- **Segurança da Cadeia de Abastecimento:** As entidades beneficiaram da implementação de mecanismos de transparência para partilha de riscos identificados.
- ***Security Intelligence:*** Cooperação internacional entre entidades bancárias é uma das formas mais eficazes para definir um conjunto de indicadores comuns. Esta medida permitiria garantir a consistência técnica dos mesmos e elaborar linhas orientadoras mais intuitivas para aplicação por parte das entidades bancárias. As instâncias de colaboração podiam ainda permitir a realização de *stress-tests* regulares no setor bancário[179].

No relatório da ENISA mencionado anteriormente, foi também realizada uma avaliação das práticas de segurança em implementação no setor. Das respostas obtidas, foi possível verificar que as práticas implementadas nas entidades do setor estão em linha com os *standards* mencionados. Alguns exemplos de práticas implementadas conforme apresentadas pelas entidades inquiridas são:

- O responsável pela segurança da informação (*Chief Information Security Officer*) define as políticas, estruturas e técnicas a utilizar;
- As avaliações de riscos e respetivo impacto no negócio são feitos com periodicidade no mínimo anual;
- Todos os incidentes de segurança são registados, classificados, analisados e discutidos com equipas de auditoria interna em reuniões periódicas[180].

[179] ENISA, "*Network and Information Security in the Finance Sector: Regulatory landscape and Industry priorities*", 2014, 31.

[180] ENISA, "*Network and Information Security in the Finance Sector: Regulatory landscape and Industry priorities* ", 2014, 26-27.

Também num relatório elaborado pela ENISA denominado "*EU Cybersecurity Initiatives in the Finance Sector*", publicado em março de 2021, é reunido um conjunto de ações no âmbito do setor bancário e financeiro que permitem uma maior resiliência em matéria de cibersegurança. Estas iniciativas estão divididas em 6 áreas principais, onde se listam algumas das atividades:

1. **Desenvolvimento e implementação de políticas:**
   - Estas iniciativas são da responsabilidade da Comissão Europeia (CE). A CE emitiu em 2018 o Plano de Ação "*Fintech"* que se propõe a alcançar uma mais forte ciberresiliência, através da partilha de informação entre operadores do mercado, promover a convergência de supervisão de gestão de riscos de IT, aumentar a coordenação da UE em processos *threat intel* entre EM (como TIBER-EU[181]);
   - Em 2020, a *Digital Finance Strategy* definiu linhas gerais sobre como a Europa pode apoiar a transformação digital do setor bancário e financeiro nos próximos anos, regulando os seus riscos;
   - O principal papel da EBA é o de contribuir para a criação do *European Single Rulebook*, com o objetivo de fornecer um conjunto único de regras de harmonização para as IF em toda a UE;
   - Desenvolvimento e aplicação de Diretrizes da EBA sobre a comunicação de fraude em pagamentos *online* considerando a PSD2. As Diretrizes pretendem contribuir para o aumento da segurança dos pagamentos na UE, exigindo que as instituições de crédito, as instituições de pagamento e instituições de *e-money* coletem e relatem dados sobre as transações de pagamento e transações de pagamento fraudulentas.
   - Implementação do "TIBER-PT", quadro de referência para testes de cibersegurança avançados pelas instituições de crédito em Portugal[182].
2. **Partilha de informação e capacitação:**
   - O ECRB lançou a *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU) em 27 de fevereiro de 2020. O CIISI-EU reúne uma comunidade de entidades públicas e privadas com o objetivo de compartilhar informações e trocar boas práticas. Os principais objetivos do CIISI-EU são: proteger o sistema financeiro prevenindo, detetando e respondendo a ciberataques; facilitar a partilha de informação, inteligência e boas práticas entre infraestruturas financeiras; aumentar a consciencialização sobre as ameaças à cibersegurança.
   - Plataforma e fórum da "CIISI-PT", o centro para partilha e análise de informação sobre ameaças de cibersegurança do setor bancário. Em atividade desde setembro de 2023, o centro apresenta sinais positivos de crescimento e interação[183].

[181] TIBER-EU: estrutura europeia para *red-teaming* ético, baseado em *threat intelligence*. É o primeiro guia da UE sobre como autoridades, entidades e *threat intelligence* e provedores de *red-team* devem trabalhar juntos para testar e melhorar a resiliência em matéria de cibersegurança de entidades, através da realização de ciberataques controlados.

[182] "Banco de Portugal avança na cooperação para a cibersegurança", Banco de Portugal, maio de 2024, https://www.bportugal.pt/comunicado/banco-de-portugal-avanca-na-cooperacao-para-ciberseguranca.

[183] "Banco de Portugal avança na cooperação para a cibersegurança", Banco de Portugal, maio de 2024.

3. **Gestão de crises de cibersegurança:**
   - A EBA promove ações de sensibilização em matéria de ciberresiliência através do seu trabalho político e atividades de convergência de supervisão. Isso envolve workshops e formação para entidades supervisoras e reguladores em toda a UE e em algumas jurisdições externas à UE. Do lado da supervisão, a EBA aumenta a sensibilização também incorporando detalhes específicos sobre TIC. Como parte de seu mandato para avaliar riscos e vulnerabilidades no setor bancário da UE, a EBA publica regularmente relatórios de avaliação de riscos de TIC e cibersegurança.
4. **Formação e sensibilização**:
   - A Autoridade Bancária Europeia (EBA) promove a consciencialização sobre a ciberresiliência do seu trabalho político e atividades de convergência de supervisão. Isto inclui *workshops*, formações e a incorporação de questões de TIC e cibersegurança na supervisão dos supervisores e reguladores da União Europeia e de algumas jurisdições não pertencentes à UE. A EBA também publica relatórios de avaliação de riscos, que incluem riscos relacionados com a cibersegurança, para avaliar vulnerabilidades no setor bancário da UE.
   - A EBA colabora com partes interessadas externas para promover a partilha de conhecimento sobre cibersegurança. Através do FinTech Knowledge Hub, a EBA oferece formação às autoridades competentes sobre a supervisão de TIC e segurança, promovendo uma compreensão comum e a troca de conhecimentos.
   - A European Banking Federation (EBF) implementa campanhas e iniciativas para aumentar a consciencialização sobre questões de cibersegurança, tanto para colaboradores de entidades bancárias quanto para cidadãos da UE. Através da *Cybersecurity Working Group*, a EBF realiza ações como a campanha *Cyber Scams*, em colaboração com o Centro Europeu de Cibercrime da Europol, além de organizar anualmente a Conferência de Cibersegurança da EBF em Bruxelas, durante o Mês Europeu da Cibersegurança (ECSM).

5. **Certificação e padronização**[184]:
   - **i.** O BCE publicou a *Cyber Resilience Oversight Expectations* (*CROE*) para as infraestruturas do mercado financeiro. A *CROE* define as expectativas do regulador do Euro em relação à ciberresiliência com base nas orientações globais;
   - **ii.** Já o *Cyber Risk Institute* (*CRI*) promove a cibersegurança no setor financeiro através do *Financial Services Cybersecurity Profile*, que serve como referência para a cibersegurança;
   - **iii.** A *EBA* publicou dois padrões técnicos sob a *PSD2*, focada no registo central eletrónico e na estrutura das informações e o *FSB* criou o *Cyber Lexicon* com o objetivo de padronizar a terminologia relacionada à cibersegurança neste setor, de forma a facilitar a comunicação entre o setor público e o privado;
   - **iv.** O PCI desenvolve padrões para proteger os dados das contas de pagamentos e garantir a segurança de todos os ciclos de pagamento.
6. **Pesquisa e Inovação**[185]:

   - O CONCORDIA é uma rede de competência em cibersegurança que reúne lideranças em pesquisa, tecnologia, indústria e competências públicas. O objetivo é estabelecer um ecossistema de cibersegurança integrado na União Europeia e voltado ao utilizador, promovendo soluções inovadoras para vários setores, incluindo o setor financeiro. Além disso, o CONCORDIA oferece laboratórios virtuais, cursos de formação e exercícios de cibersegurança (*cyber ranges*), e fornece experiência aos responsáveis políticos e à indústria europeia.
   - O projeto Cybersecurity for Europe visa harmonizar o desenvolvimento de componentes de *software* para enfrentar desafios de cibersegurança em setores críticos, como infraestruturas digitais, finanças, governo, cidades inteligentes, saúde e transportes. Este projeto foca-se na pesquisa, desenvolvimento e inovação em tecnologias de cibersegurança de próxima geração, com especial atenção à cibersegurança em setores essenciais como o financeiro.

[184] ENISA, "*EU Cybersecurity Initiatives in the Finance Sector*", março de 2021, 12-13.
[185] ENISA, "*EU Cybersecurity Initiatives in the Finance Sector*", março de 2021, 4-17.

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 8 - Cenários de risco (Bancário)

Cenários de risco
Instalação de SOFTWARE MALICIOSO em dispositivo da entidade com o objetivo de aceder a dados sensíveis. Pode também ocorrer no âmbito da cadeia de fornecimento ou afetar os sistemas de controlo industrial.
Comprometimento de serviços *WEB*, através de um *URL* malicioso ou script malicioso que direciona um colaborador da entidade para um website falso e instala software malicioso (ataques *Watering Hole*, ataques *Drive-By*), permitindo o furto de dados.
Campanha de *PHISHING* dirigida a colaboradores ou clientes da entidade com o fim de furtar dados sensíveis, como credenciais de login ou dados de cartões de crédito. Por vezes, assume a forma de Compromisso de Email de Negócio/CEO, o que promove a realização de transferências bancárias ilícitas por parte de um colaborador.
Negação de serviço distribuído (DDoS) a um serviço digital da organização, tornando-o indisponível, com o objetivo de exibir uma capacidade por parte do atacante, retaliar alguma ação prévia da entidade ou pedir um resgate.
FURTO DE IDENTIDADE a um colaborador ou à imagem da entidade, através do furto de credenciais ou de outros dados sensíveis, permitindo o acesso não autorizado à infraestrutura ou a serviços externos, como bancários, ou o uso ilegítimo da imagem da entidade.
VIOLAÇÃO DE DADOS da entidade (dados de clientes, dados financeiros, propriedade intelectual), através de ação negligente por parte de um colaborador ou mediante a exploração de vulnerabilidade e intrusão.
RANSOMWARE que cifra informação essencial ao funcionamento da entidade, sendo pedido um resgate em *bitcoins*, sob a ameaça da sua destruição ou exposição ao público.

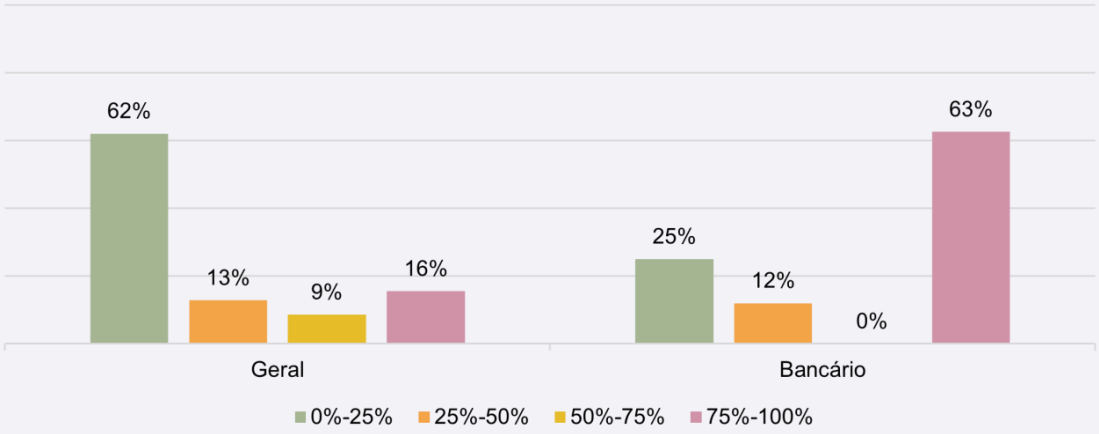
(Fonte: CNCS, “Riscos & Conflitos 2021”, obtido em 19 de setembro de 2024, https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriocibersegurancа-cncs.pdf)

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

Formação

As ameaças mais prevalentes neste setor são o *ransomware* e as ameaças relativas a dados pessoais dos clientes, sendo estas ameaças concretizadas, normalmente, através de ataques bem-sucedidos de *phishing*. A sensibilização para este tipo de riscos e a formação para identificar estes riscos são essenciais para impedir que estas se concretizem, já que a formação leva a que medidas de prevenção, como realização de *backups*, sejam implementadas. A formação nestas matérias é também importante para que se evitem divulgações de informação de forma indevida. Este setor está à frente da média geral, dado que nos OSE, cerca de 63% dos 75%-100% trabalhadores têm formação básica em cibersegurança quando, no âmbito geral, apenas 16% dos setores estão nesse patamar **(Gráfico 33)**.

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



Os resultados do questionário evidenciam que a totalidade dos OSE do setor disponibiliza formação em cibersegurança aos seus colaboradores (**Gráfico 38**), sendo que 88% são de carácter obrigatório (**Gráfico 39**). No âmbito geral podemos observar que a média da disponibilização de formação em cibersegurança aos colaborados está nos 65% e apenas 42% tem caráter obrigatório.

Gráfico 38 - Disponibilização de formação em cibersegurança aos colaboradores

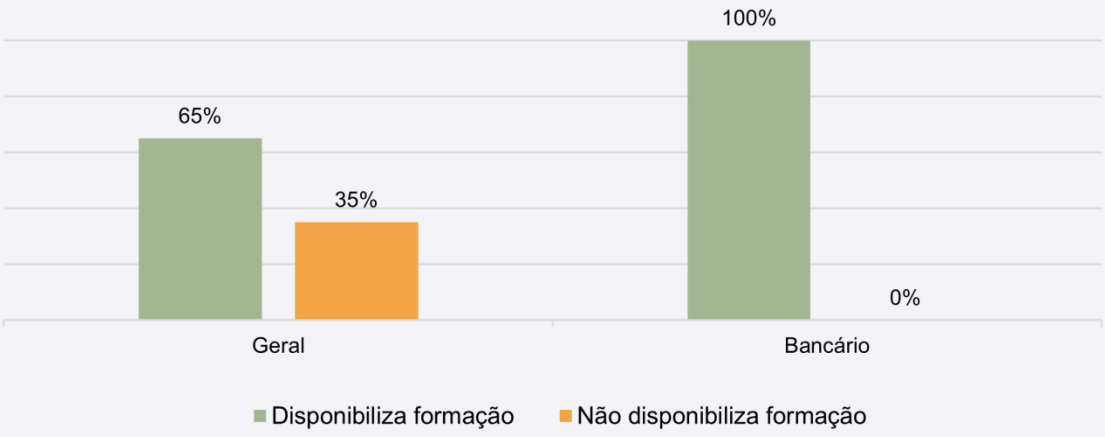
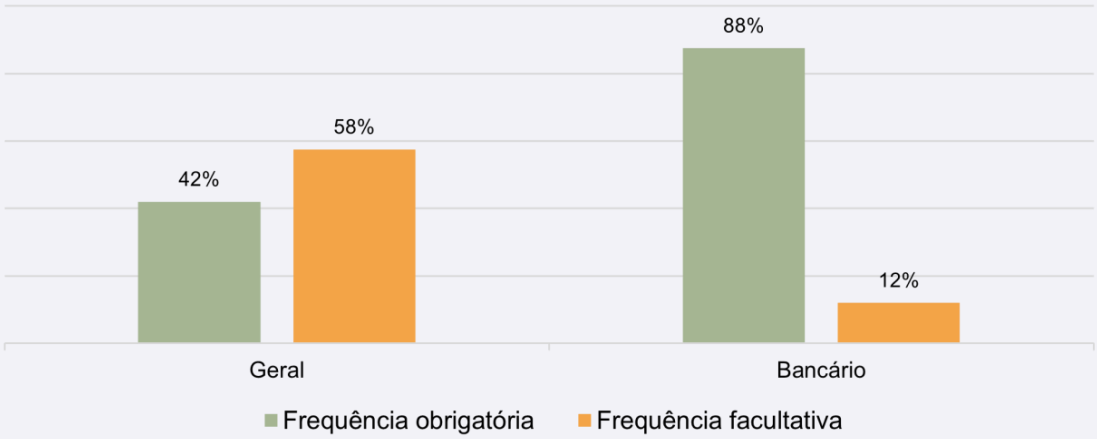
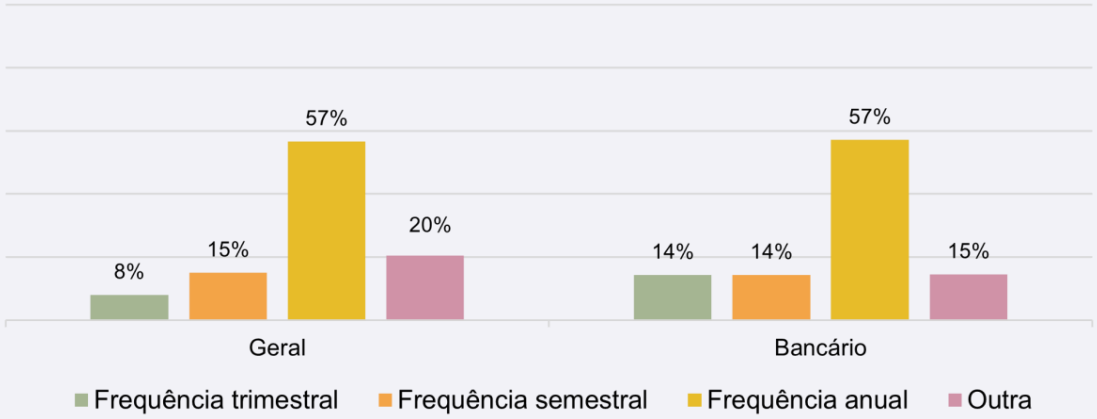


Gráfico 39 - Caráter das formações disponibilizadas - frequência obrigatória ou facultativa



Além disso, a maior parte dos momentos de formação têm frequência anual (**Gráfico 41**), o que no contexto do setor assegura a sensibilização necessária para boas práticas de cibersegurança por parte dos colaboradores e está na média geral.

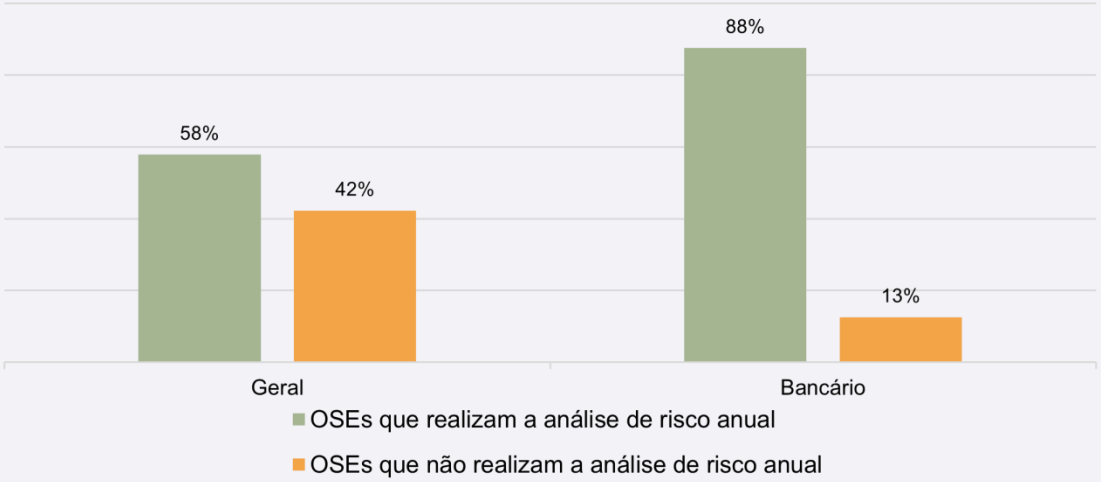
Gráfico 41 - Frequência média dos momentos de formação



Medidas de proteção contra ameaças de cibersegurança

Ao nível das medidas de proteção contra ameaças de cibersegurança, o questionário realizado evidencia que este setor, comparativamente com os restantes, está acima da média, com exceção na *Firewall*/*WAF*/*Webfilter*. Este setor está acima da média na realização de avaliações de segurança anuais no âmbito de cibersegurança (**Gráfico 99**).

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



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

- Realizem avaliações de segurança, em todas as entidades, pelo menos anualmente;
- Realizem análises de risco pelo menos anualmente;
- Implementem, onde possível, *Firewall*/*WAF*/*Webfilter*.

Políticas, procedimentos e planos de cibersegurança

Com base nos dados reunidos no questionário, todos os OSE do setor possuíam políticas e procedimentos de cibersegurança documentados e implementados. Este valor é superior à média geral (100% vs 50%).

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

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

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

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

No setor bancário, os controlos fundacionais, que dizem respeito à segurança da rede, assumem um papel especialmente crítico. Infraestruturas bancárias, como sistemas de pagamento e transferência de fundos, dependem da configuração correta e da segurança de *firewalls*, *routers* e *switches* para garantir a integridade, disponibilidade e continuidade dos serviços financeiros. Qualquer falha ou configuração inadequada pode ser explorada para interromper transações, desviar fundos, ou comprometer a privacidade e segurança dos dados financeiros dos clientes, colocando em risco a estabilidade das operações bancárias.

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

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

Tabela 9 - Controlos de Segurança da CIS (Bancário)

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)

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

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

- Alves, Maria. “Bancos privados com 3,3 mil milhões de lucros em 2023 a subirem 74,2% face ao ano anterior”. Jornal Económico, 5 de março de 2024. https://leitor.jornaleconomico.pt/noticia/bancos-privados-com-3-3-mil-milhoes-de-lucros-em-2023-a-subirem-74-2-face-ao-ano-anterior.
- American National Standards Institute. “X9: Accredited Standards Committee X9, Inc.”. ANSI Webstore. https://webstore.ansi.org/sdo/x9?source=blog&_gl=1*v6wen5*_gcl_au*NzI0ODc2NzI1LjE3MjU1NTU5ODc.
- ANACOM, “Utilização da Internet das Coisas (IoT - Internet of Things)”, 2022. https://www.anacom.pt/streaming/relatorioInternet_dasCoisas_IoT2022.pdf?contentId=1737940&field=ATTACHED_FILE.
- Banco Central Europeu. “Card fraud in Europe declined notably in 2021 amid the implementation of regulatory measures”, maio de 2023. https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html
- Banco Central Europeu. “ECB and EBA publish joint report on payment fraud”, agosto de 2024. https://www.ecb.europa.eu/press/pr/date/2024/html/ecb.pr240801~f21cc4a009.en.html
- Banco Central Europeu. “TIBER-EU Guidance for Target Threat Intelligence Report”, julho de 2020. https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/shared/pdf/Final_TIBER-EU_Guidance_for_Target_Threat_Intelligence_July_2020.pdf.
- Banco de Portugal. “Análise das empresas do setor dos transportes”, BPStat, 2022. https://bpstat.bportugal.pt/conteudos/publicacoes/1343.
- Banco de Portugal. “Banco de Portugal atualiza séries longas do setor bancário português”. BPStat, 26 de julho de 2023. https://bpstat.bportugal.pt/conteudos/noticias/1955.
- Banco de Portugal. “Banco de Portugal avança na cooperação para a cibersegurança”, maio de 2024. https://www.bportugal.pt/comunicado/banco-de-portugal-avanca-na-cooperacao-para-ciberseguranca.
- Banco de Portugal. “Campanha #ficaadica. Banco de Portugal divulga brochura com conselhos sobre o acesso a produtos e serviços bancários digitais”, 7 de fevereiro de 2023. https://www.bportugal.pt/comunicado/campanha-ficaadica-banco-de-portugal-divulga-brochura-com-conselhos-sobre-o-acesso.
- Banco de Portugal. “Economia numa imagem”, março de 2022. https://www.bportugal.pt/page/economia-numa-imagem-148-0.
- Banco de Portugal. “História do Banco de Portugal”. Sobre o Banco. https://www.bportugal.pt/page/historia-do-banco-de-portugal
- Banco de Portugal. “Instituições autorizadas”, última atualização em 23 de setembro de 2024. https://www.bportugal.pt/page/listagem-entidades-autorizadas

- Banco de Portugal. "Lista de agências", agosto de 2024. https://www.bportugal.pt/sites/default/files/listaagencias.xls
- Banco de Portugal. "Outros sistemas de liquidação". Infraestruturas de mercado. https://www.bportugal.pt/page/outros-sistemas-de-liquidacao.
- Banco de Portugal. "Recomendações sobre Gestão da Continuidade de Negócio", Carta Circular n.º CC/2021/00000047, 2021. https://www.bportugal.pt/sites/default/files/anexos/cartas-circulares//463107899_6.docx.pdf.
- Banco de Portugal. "Relatório de Estabilidade Financeira", novembro de 2023. https://www.bportugal.pt/sites/default/files/documents/2024-02/ref_11_2023_pt.pdf.
- Banco Montepio. "Relatório e Contas 2023", 15 de abril de 2024. https://www.bancomontepio.pt/content/dam/montepio/pdf/institucional/investor-relations/relatorios-comunicados-e-informacao-financeira/2023/informacao-anual/relatorio-contas-anual-banco-montepio-2023.pdf.
- Banco Português de Investimento. "Relatório e Contas 2023". https://www.bancobpi.pt/contentservice/getContent?documentName=PR_UCMS02106736.
- Banco Santander Totta. "Annual Report 2023: Proposal", 17 de maio de 2024. https://www.santander.pt/pdfs/investor-relations/santander-totta-sa/relatorio-e-contas/2023/BST_Annual_Report_2023_non_official_non_audited.pdf.
- Bank for International Settlements e International Organization of Securities Commissions. "Guidance on cyber resilience for financial market infrastructures", junho de 2016. https://www.bis.org/cpmi/publ/d146.pdf.
- Bank for International Settlements. "Basel II: Revised international capital framework", Basel Committee on Banking Supervision. https://www.bis.org/publ/bcbsca.htm.
- Bank of England. "CHAPS". https://www.bankofengland.co.uk/payment-and-settlement/chaps.
- Banking Act of the Federal Republic of Germany, "Gesetz iiber das Kreditwesen",setembro de 1998. https://www.cftc.gov/sites/default/files/idc/groups/public/@otherif/documents/ifdocs/eurexmcobankingact.pdf
- Bouveret, Antoine. "Cyber Risk for the Financial sector: A framework for Quantitative Assessment". Working Paper do Fundo Monetário Internacional, junho de 2018. https://www.imf.org/en/Publications/WP/Issues/2018/06/22/Cyber-Risk-for-the-Financial-Sector-A-Framework-for-Quantitative-Assessment-45924.
- Business IT. "A Tecnologia e a Banca. As Inovações que Estão a Permitir Digitalizar o setor", 21 de outubro de 2022. https://business-it.pt/2022/10/21/a-tecnologia-e-a-banca-as-inovacoes-que-estao-a-permitir-digitalizar-o-sector/.
- Caixa Geral de Depósitos. "Fintech: o que são e o que fazem". Saldo Positivo, 4 de abril de 2023. https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/o-que-sao-fintech.aspx
- Caixa Geral de Depósitos. "Relatório de Gestão e Contas 2023". https://www.cgd.pt/Investor-Relations/Informacao-Financeira/CGD/Relatorios-Contas/Pages/Relatorios-Contas-CGD.aspx.
- Center for Internet Security. "The 18 CIS Critical Security Controls", CIS Critical Security Controls. https://www.cisecurity.org/controls/cis-controls-list.
- Cheney, Julia. "Heartland Payment Systems: Lessons Learned from a Data Breach", janeiro de 2010. https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/d-2010-january-heartland-payment-systems.pdf?la=en&hash=EEAF5C96513D6E176D6C5312E4007061.
- CNCS, "Compromisso C-Academy". https://www.cncs.gov.pt/pt/c-academy-compromisso/.
- CNCS, "Estratégia Nacional de Segurança do Ciberespaço 2019-2023". https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf.
- CNCS, "Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança", dezembro de 2022. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf.
- CNCS, ISAC. https://www.cncs.gov.pt/pt/isac/.

- CNCS. “Incidentes e Setores”. Conhecimento Situacional: Estatísticas. https://www.cncs.gov.pt/pt/estatistica/#cert.pt.
- CNCS. “ISAC Portos”, Comunidades de Cibersegurança, última atualização em abril de 2024. https://www.cncs.gov.pt/pt/comunidades-ciberseguranca/isacs/portos/.
- CNCS. “Relatório Cibersegurança em Portugal: Riscos & Conflitos 2021”. https://www.cncs.gov.pt/docs/relatorio-riscosconflitos2021-observatoriociberseguranca-cncs.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.
- Comissão Europeia. “Ficha temática sobre o semestre europeu: Setor Bancário e estabilidade financeira”, 16 de outubro de 2017. https://commission.europa.eu/system/files/2021-01/european-semester_thematic-factsheet_banking-sector-financial-stability_pt.pdf.
- Conselho Europeu, “Horizonte Europa”. https://www.consilium.europa.eu/pt/policies/horizon-europe/.
- Decreto-Lei n.º 298/92, de 31 de dezembro, “Regime Geral das Instituições de Crédito e Sociedades Financeiras - RGICSF”, Diário da República. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1992-70072322.
- Decreto-Lei n.º 65/2021, de 30 de julho. Diário da República. https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.
- Department for Science, Innovation & Technology, “Cyber security breaches survey 2023”, 19 de abril de 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023
- Dias, Mariana. “Cinco maiores bancos pagaram 17% do IRC total arrecadado em 2023”. Diário de Notícias, 25 de março de 2023. https://www.dn.pt/3384889811/cinco-maiores-bancos-pagaram-17-do-irc-total-arrecadado-em-2023/.
- Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32015L2366.
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.
- Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148.
- Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2), Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022L2555&qid=1730847643285
- Diretiva 2007/64/CE do Parlamento Europeu e do Conselho de 13 de novembro de 2007 relativa aos serviços de pagamento no mercado interno. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32007L0064.
- EBA. “Orientações definitivas sobre a segurança dos pagamentos efetuados através da internet”. https://www.eba.europa.eu/sites/default/files/documents/10180/1004450/558993c7-c253-472c-bae3-f897f6c6038a/EBA-GL-2014-12_PT_rev1%20GL%20on%20Internet%20Payments.pdf.
- EBA. “Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366 (PSD2)”, 12 de janeiro de 2018. https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-

cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf.

- Empowering EU ISACs, "European ISACs". https://www.isacs.eu/european-isacs.
- ENISA, "Cybersecurity Skills Conference: Strengthening human capital in the EU". https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu.
- ENISA, "NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist", 11 de dezembro de 2020, https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist.
- ENISA. "Cyber Europe Programme", 2024. https://www.enisa.europa.eu/topics/training-and-exercises/cyber-exercises/cyber-europe-programme.
- ENISA. "ENISA Threat Landscape 2023", 19 de outubro de 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023/@@download/fullReport.
- ENISA. "EU Cybersecurity Initiatives in the Finance Sector", março de 2021. https://www.enisa.europa.eu/publications/EU_Cybersecurity_Initiatives_in_the_Finance_Sector/@@download/fullReport.
- ENISA. "Mapping of OES Security Requirements to Specific Sectors", 18 de janeiro de 2018. https://www.enisa.europa.eu/publications/mapping-of-oes-security-requirements-to-specific-sectors.
- ENISA. "NIS 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.
- European Energy Information Sharing & Analysis Centre (EE-ISAC), "Impact". https://www.ee-isac.eu/impact/#.
- Federal Financial Supervisory Authority. "Risk management", dezembro de 2017. https://www.bafin.de/EN/Aufsicht/BankenFinanzdienstleister/Risikomanagement/risikomanagement_node_en.html
- Federal Trade Commission. Equifax Data Breach Settlement", fevereiro de 2024. https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement.
- FIN-FSA. Management of operational risk in supervised entities of the financial sector", agosto de 2014. https://www.finanssivalvonta.fi/globalassets/en/regulation/fin-fsa-regulations-and-guidelines/2014/08_2014/08_2014.m4_en.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.
- Gulyas, Oliver e Gabor Kiss. "Cybersecurity threats in the banking sector". 2022 8th International Conference on Control, Decision and Information Technologies (CoDIT), junho de 2022. https://ieeexplore.ieee.org/abstract/document/9804140.
- Hassanzadeh, Amin, Amin Rasekhb, Stefano Galellic, Mohsen Aghashahid, Riccardo Taorminae, Avi Ostfeldf e Katherine Banksg. "A Review of Cybersecurity Incidents in the Water Sector". Journal of Environmental Engineering 146: 25 de julho de 2020. https://arxiv.org/pdf/2001.11144.
- IEFP, Cheque-Formação + Digital. https://www.iefp.pt/cheque-formacao-digital.
- INE, "Inquérito à Utilização das TIC nas Empresas", 2022. https://www.ine.pt/ngt_server/attachfileu.jsp?look_parentBoui=585250024&att_display=n&att_download=y.
- International Monetary Fund. "Cyber Risk: A Growing Concern for Macrofinancial Stability", abril de 2024, 7. https://www.imf.org/-/media/Files/Publications/GFSR/2024/April/English/ch3onlineannex.ashx

- ISO, “ISO/IEC 27001:2022”. https://www.iso.org/standard/27001.
- ISO. “ISO/TR 13569:2005”, novembro de 2005. https://www.iso.org/standard/37245.html
- ISO. “ISO/TR 27015:2012”, dezembro de 2012. https://www.iso.org/standard/43755.html
- Khan, Shaharyar, Ilya Kabanov, Yunke Hua e Stuart Madnick. “A Systematic Analysis of the Capital One Data Breach: Critical Lessons Learned”, novembro de 2022. https://dl.acm.org/doi/10.1145/3546068
- Lei n.º 46/2018, de 13 de agosto, Diário da República. https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.
- Magalhães, Flávia. “IA e o setor financeiro: A revolução da tecnologia”. Consumidor Moderno, 29 de fevereiro de 2024. https://consumidormoderno.com.br/ia-e-o-setor-financeiro-a-revolucao-da-tecnologia/.
- Maurer, Tim e Arthur Nelson. “The Global Cyber Threat to Financial Systems”, FINANCE & DEVELOPMENT, março de 2021. https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm.
- Microsoft, “Estado da Cibersegurança em Portugal”, 2023-2024. https://pulse.microsoft.com/wp-content/uploads/2024/02/Microsoft_Security_Report_final.pdf.
- Observador. “Inovação e setor financeiro: simplificar é a regra”, 29 de novembro de 2023. https://observador.pt/2023/11/29/inovacao-e-setor-financeiro-simplificar-e-a-regra/.
- PORDATA, “Empresas: total e por dimensão”, dados de 2022. https://www.pordata.pt/portugal/empresas+total+e+por+dimensao-2857.
- Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativo à resiliência operacional digital do setor financeiro. Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554.
- Reuters. “Bangladesh Bank hackers compromised SWIFT software, warning issued”, 25 de abril de 2016. https://www.reuters.com/article/world/exclusive-bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DW/
- Rosalino, Hélder. “Desafios da transformação digital para o Setor Bancário”. Fintech House Lisboa, janeiro de 2020. https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20200123.pdf.
- Sarbanes Oxley Act. “The Sarbanes-Oxley Act”, https://sarbanes-oxley-act.com/.
- Security Standards Council. “PCI Data Security Standard (PCI DSS)”. Standards. https://www.pcisecuritystandards.org/standards/pci-dss/.
- Silver-Greenberg, Jessica Matthew Goldstein e Nicole Perlroth. “JPMorgan Chase Hacking Affects 76 Million Households”. The New York Times, outubro de 2014. https://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/
- Sulaiman Asif, “Cyber Threat Analysis: Types, Benefits, Tools, Approaches”, Knowledge Hut, September 5, 2023. https://www.knowledgehut.com/blog/security/threat-analysis.
- Swiss National Bank. “The SNB’s legal basis”. https://www.snb.ch/en/the-snb/organisation/legal-framework
- Teixeira, Alberto. “Banca com lucros recorde em 5 gráficos”. Eco, 15 de março de 2024. https://eco.sapo.pt/2024/03/15/banca-com-lucros-recorde-em-5-graficos/.
- U.S. Securities and Exchange Commission. “OCIE Cybersecurity and Resiliency Observations”. https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf .
- United States Federal Trade Commission. “Gramm-Leach-Bliley Act”. Business Guidance: Privacy and Security. https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act.
- Wood, Johnny. “Global financial stability at risk due to cyber threats, IMF warns. Here's what to know”. World Economic Forum, 15 de maio de 2024. https://www.weforum.org/agenda/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/.
- World Bank. “Strategic Cybersecurity Talent Framework - White Paper”, abril de 2024. https://www3.weforum.org/docs/WEF_Strategic_Cybersecurity_Talent_Framework_2024.pdf.

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