Aliança para
a Cibersegurança

PME
e Cibersegurança
em Portugal
destaques

JULHO DE 2023

Índice

Documento desenvolvido pelo Centro Nacional de Cibersegurança no âmbito da Aliança para a Cibersegurança
Julho de 2023, Lisboa

Sumário Executivo

O presente documento, realizado pelo Centro Nacional de Cibersegurança (CNCS) no âmbito da Aliança para a Cibersegurança, faz uma análise aos principais dados disponíveis sobre a cibersegurança nas micro, pequenas e médias empresas (PME) em Portugal, de modo a disponibilizar uma melhor compreensão sobre as capacidades instaladas e as necessidades mais prioritárias neste domínio. O documento utiliza como fontes principais o Eurostat (2023a e 2023b), o Eurobarómetro (2022), o Pordata (2023) e um estudo sobre economia da cibersegurança realizado pelo Observatório de Cibersegurança do CNCS (CNCS, 2022), tendo em conta os dados mais recentes, nomeadamente de 2020, 2021 e 2022. Considerando a informação disponível, destacam-se os seguintes aspetos relativos às PME em Portugal:

- Sofrem menos incidentes com consequências na segurança da informação do que a média da União Europeia (UE) e do que as grandes empresas, sendo a consequência mais frequente a indisponibilidade de serviços digitais, algo que afeta o trabalho dos empregados;
- Têm menos recursos internos do que as grandes empresas;
- Têm uma elevada preocupação com as ameaças a contas bancárias, os programas maliciosos e o *phishing*;
- Tendem a reportar os incidentes graves, sobretudo à polícia;
- Menos de metade tem política de segurança das tecnologias de informação e comunicação (TIC) definida, mas mais do que a média da UE, tendo aumentado este valor nos últimos anos;
- Cerca de um terço tem um orçamento anual dedicado à cibersegurança de menos de três mil euros;
- Afirmam aplicar maioritariamente (mais de 50%) as seguintes boas práticas de cibersegurança, por ordem decrescente: palavras-passe fortes, *backups* para armazenamento externo, controlo do acesso à rede e registo de *logs*;
- Afirmam aplicar minoritariamente (menos de 50%) as seguintes boas práticas, por ordem crescente: múltiplo fator de autenticação, análises de risco, testes de segurança, mecanismos de monitorização e uso de VPN;
- Apenas um terço refere não ter dificuldade em contratar profissionais de cibersegurança;
- Quanto maior a empresa, mais relevante é o papel do departamento de informática nas tarefas de cibersegurança; quanto menor, mais relevante o da administração;

- Tendem a ter apenas um trabalhador alocado a tarefas de cibersegurança caso estas sejam realizadas internamente;
- Tendem a ter mais atividades efetuadas por fornecedores externos em lugar de pessoal interno, sobretudo em organizações mais pequenas;
- Mais de metade disponibiliza documentação sobre cibersegurança aos empregados, quase o dobro de em anos passados;
- Mais de metade sensibiliza os seus empregados para a cibersegurança (um valor que tem aumentado nos últimos anos), mas sobretudo através de ações voluntárias.

1. Introdução

As PME em Portugal não têm aparecido de uma forma central no quadro legal e político no que à cibersegurança diz respeito. Tal situação dever-se-á não tanto à sua pouca importância na economia nacional, mas à sua menor presença no âmbito da operação de serviços essenciais ou de infraestruturas críticas, comparando com as grandes empresas.

Por exemplo, a única referência a PME no Regime Jurídico de Segurança do Ciberespaço ocorre para excluir as microempresas e as pequenas empresas das entidades para que remetem as obrigações dos prestadores de serviços digitais. No texto da Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC) surge apenas uma referência direta às PME, nomeadamente no Eixo 3 – Proteção do Ciberespaço, onde se refere a linha de ação "promover estruturas de cooperação nacional e setorial de proteção do ciberespaço, inclusive do setor público ao nível central, regional e local, e também do setor privado, incluindo as pequenas e médias empresas, para a partilha de informação e de promoção da colaboração mútua na proteção de interesses comuns". Todavia, a referência a empresas e ao setor privado aparece noutras linhas de ação ao longo da ENSC.

Esta menor presença das PME no quadro legal e estratégico da cibersegurança não obsta a que se reconheça a sua importância para a cibersegurança nacional, como a linha de ação da ENSC descrita tão bem demonstra. Além disso, a relevância económica das PME exige cuidados de cibersegurança. Para o efeito, o presente documento, realizado pelo CNCS no âmbito da Aliança para a Cibersegurança, pretende dar resposta à necessidade de conhecer o estado da cibersegurança nas PME em Portugal, tendo em conta os dados disponíveis e os estudos já realizados.

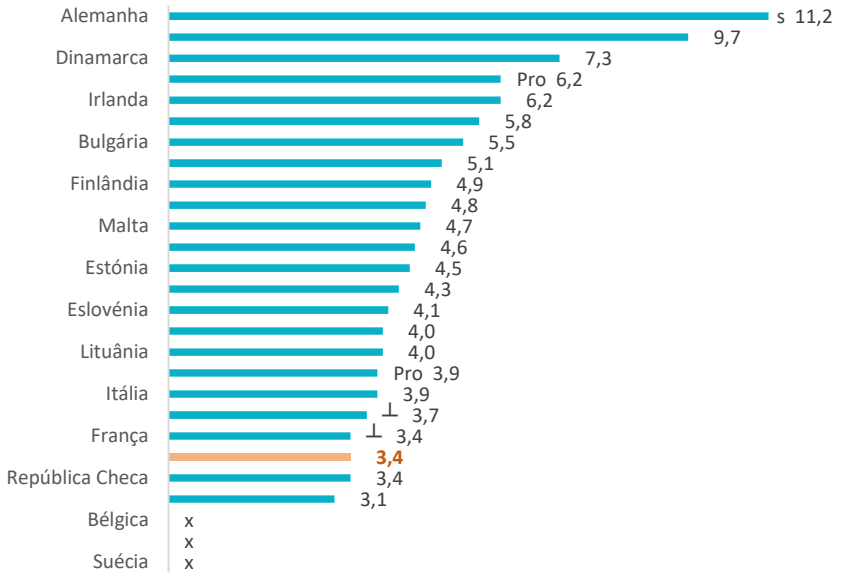
De seguida apresentam-se alguns valores e tendências que mostram a situação das PME no país no que à cibersegurança diz respeito, com particular atenção aos aspetos ligados à capacitação. Por fim, deixam-se algumas recomendações.

2. PME em Portugal

- Em Portugal, no ano 2021, existiam 1 357 657 PME. O setor com mais PME era o comércio por grosso e retalho (15,9%), seguido da agricultura, produção animal, caça, silvicultura e pesca (9,3%), do alojamento, restauração e similares (8,2%) e das atividades de saúde humana e apoio social (8,1%).
- Portugal é dos países da UE com uma média de empregados por empresa mais reduzida, em 2020, com 3,4 empregados por empresa, contra 11,2 da Alemanha – ver figura 1.

(Pordata, 2023)

Fig. 1. Dimensão média das empresas na UE em 2020 por nº de empregados



Simbologia

⊥ Quebra de série
... Confidencial
// Não aplicável ou zero ou zero por defeito
- Ausência de valor
N Valor negligenciável
fr Dado de fiabilidade reduzida

Pro Valor provisório
x Valor não disponível
f Valor previsto
Rv Valor revisto
s Valor estimado

Pre Valor preliminar
e Dado inferior a metade do módulo da unidade utiliza
§ Dado com coeficiente de variação elevado
(R) Dados rectificados pela entidade responsável
u Valor incerto ou não confiável

(Pordata, 2023)

- Relativamente ao total de empresas no país, em 2021, 96% são microempresas, 3,3% são pequenas empresas, 0,6% são médias empresas e 0,1% são grandes empresas – ver figura 2.

Fig. 2. Empresas por dimensão em Portugal, 2021 (%)

(Pordata, 2023)

3. Incidentes e Cibercrime

- Dados do Eurostat relativos a incidentes de segurança nas TIC sofridos pelas empresas e consequências dos mesmos em 2021, mostram que apenas 11,3% das PME[1] em Portugal reconhecem ter sofrido algum incidente deste tipo com consequências na disponibilidade, integridade ou confidencialidade da informação, contra 21,6% da média da UE (grandes empresas: 20,2% em Portugal e 41,1% na média da UE). O tipo de consequência nefasta mais frequente é a indisponibilidade de serviços digitais.[2]

> 11,3% das PME em Portugal, em 2021, admitem ter tido consequências de incidente de segurança nas TIC

(Eurostat, 2023a)

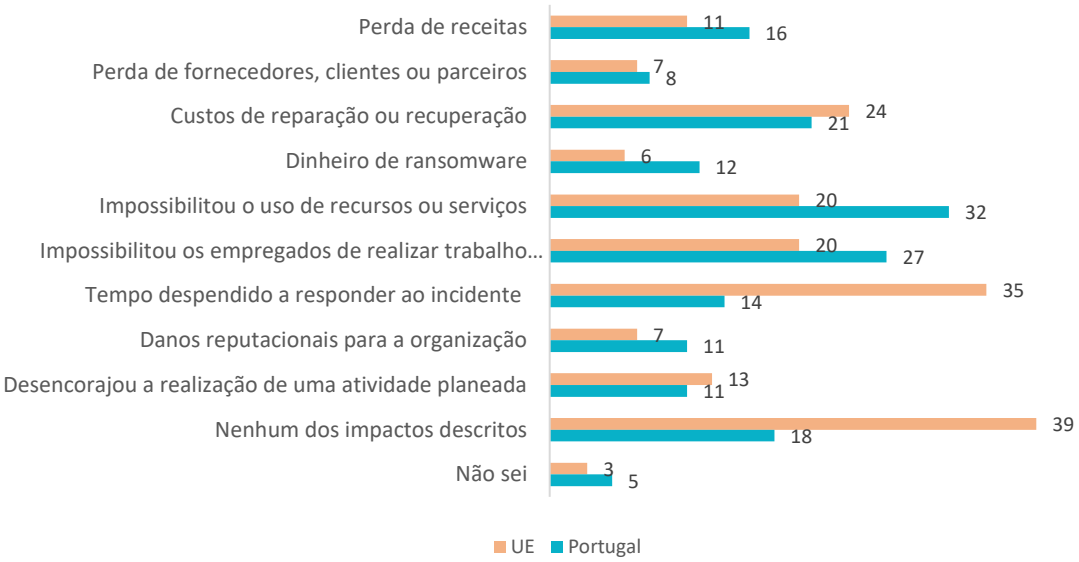
- Com base em inquérito do Eurobarómetro sobre cibercrime e PME, constata-se que em Portugal a maior preocupação das PME em 2021 em relação aos riscos no ciberespaço era com o *hacking* a contas bancárias (55% em Portugal e 32% na média da UE), seguida de vírus, *spyware* ou *malware* (47% em Portugal e 29% na média da UE) e do *phishing* (43% em Portugal e 31% na média da UE).
- O impacto do incidente mais grave relatado pelas PME em Portugal foi a impossibilidade de uso de recursos ou serviços e dos empregados realizarem o seu trabalho (reforçando as conclusões dos dados do Eurostat referidos). Na média da UE destaca-se o tempo despendido para responder ao incidente e os custos associados – ver figura 3.

(Eurobarómetro, 2022)

[1] Relativamente aos dados do Eurostat: PME considerando apenas empresas pequenas (entre 10 e 49 empregados) e empresas médias (entre 50 e 249 empregados), não tendo em conta, portanto, microempresas (entre 1 e 9 empregados), por indisponibilidade de dados. Não se consideraram empresas sem empregados. Esta situação aplica-se a ambos os inquéritos do Eurostat utilizados neste documento (Eurostat, 2023a 2023b).

[2] Os dados do Eurobarómetro (2022), apresentados de seguida, sobre PME e cibercrime, indicam que 48% das PME em Portugal admitem ter sido vítimas de algum tipo de cibercrime em 2021, contra 28% da média da UE, divergindo significativamente, portanto, destes dados do Eurostat (2023a) relativamente a incidentes e suas consequências. Esta divergência dever-se-á à natureza diferente das questões colocadas (sofrer consequências nefastas de um incidente tem características diferentes de identificar um cibercrime). Não obstante, esta disparidade é problemática. Neste contexto, atribui-se mais peso aos dados do Eurostat dada a sua maior robustez metodológica e à natureza deste documento, orientado mais à capacitação e não tanto à identificação de ameaças.

Fig. 3. Pensando no incidente sofrido mais grave, que impacto sofreu o seu negócio (2021)? *PME* (%)



(Eurobarómetro, 2022)

- Quanto ao reporte dos incidentes sofridos nos 12 meses anteriores, as PME em Portugal no ano de 2021 afirmaram reportar muito mais (81%) do que a média da UE (54%). Quando o fazem é sobretudo à polícia (24% em Portugal e 18% na UE) e ao vendedor ou prestador do serviço (18% em Portugal e 17% na média da UE).

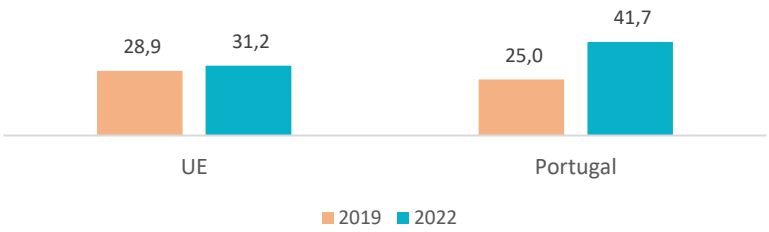
(Eurobarómetro, 2022)

4. Política de Segurança das TIC

- Voltando a dados do Eurostat, em Portugal, no ano 2022, 41,7% das PME tinha uma política de segurança para as TIC definida ou revista nos últimos dois anos, contra 31,2% na média da UE (grandes empresas: 83,4% em Portugal e 73,1% na média da UE).
- A percentagem de PME em Portugal com uma Política de Segurança das TIC definida aumentou bastante entre 2019[3] e 2022, em 16,7 pp (pontos percentuais) – ver figura 4.

(Eurostat, 2023b)

Fig. 4. Políticas de Segurança TIC definidas ou renovadas nos últimos 2 anos nas PME (%)



(Eurostat, 2023b)

[3] Último inquérito antes de 2022.

5. Orçamento de Cibersegurança

- De acordo com o estudo sobre economia da cibersegurança realizado pelo Observatório de Cibersegurança, em 2021, 36,8% das PME em Portugal tinha um orçamento anual dedicado à cibersegurança de menos de três mil euros e 17,2% entre três mil e oito mil euros. O valor máximo identificado foi de mais de 50 mil euros, para 3,4% dos inquiridos. Sem orçamento encontravam-se 8,4% das PME.

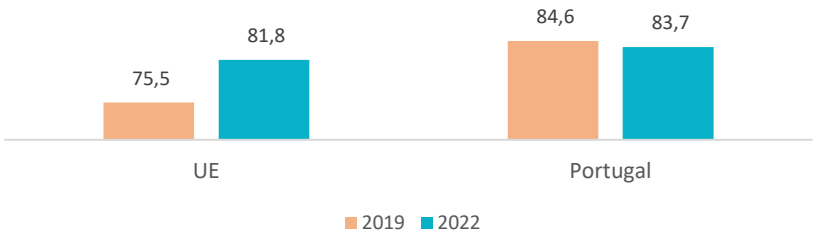
(CNCS, 2022)

6. Boas Práticas de Cibersegurança

- De acordo com o Eurostat, em 2022, 83,7% das PME em Portugal aplicavam palavras-passe fortes, contra 81,8% da média da UE (grandes empresas: 97,8% em Portugal e 96,3% na UE);
- Verificou-se uma descida no uso de palavras-passe fortes nas PME em Portugal em 2022, em 0,9 pp, mas ficando acima da média da UE – ver figura 5.

(Eurostat 2023b)

Fig. 5. Uso de palavras-passe fortes nas PME (%)

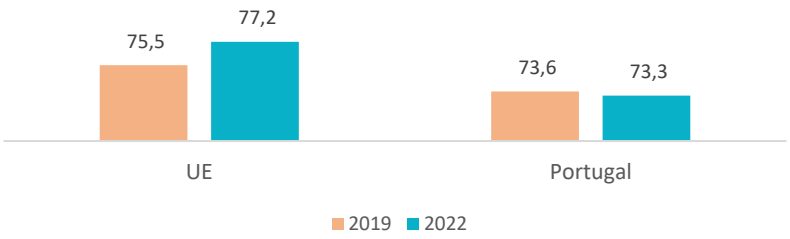


(Eurostat 2023)

- No mesmo ano, 73,3% das PME em Portugal fazia *backups* para armazenamento externo (incluindo na nuvem), contra 77,2% na média da UE (grandes empresas: 95,5% em Portugal e 93,2% na média da UE).
- Verificou-se um ligeiro decrescimento na realização de *backups* nas PME em Portugal no ano 2022, comparando com 2019, em 0,3 pp – ver figura 6.

(Eurostat 2023b)

Fig. 6. Backups para armazenamento externo (incluindo na nuvem) nas PME (%)

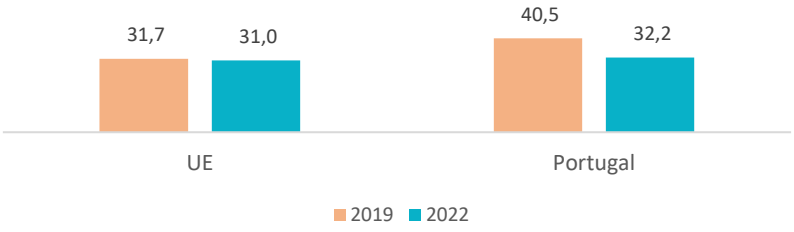


(Eurostat 2023b)

- Ainda no mesmo inquérito, 61,8% das PME afirmaram controlar o acesso à rede da empresa, contra 64,1% na média da UE (grandes empresas: 96,4% em Portugal e 91,5% na média da UE).
- Acresce que 43,1% das PME no país usavam VPN, contra 47,3% na média da UE (grandes empresas: 93,6% em Portugal e 91,3% na média da UE).
- No que diz respeito ao registo de *logs* para futura análise em caso de incidentes, 53,1% das PME em Portugal afirmaram realizar este registo, contra 43,7% na média da UE (grandes empresas: 88,2% em Portugal e 82,2% na média da UE).
- A análise de risco em relação a incidentes de cibersegurança é realizada, segundo afirmam, por 32,2% das PME em Portugal e 31% na média da UE (grandes empresas: 77,8% em Portugal e 72,4% na média da UE).
- Entre 2019 e 2022 houve uma diminuição acentuada no número de PME que realizaram análises de risco de cibersegurança em Portugal, na ordem dos 8,3 pp – ver figura 7.

(Eurostat 2023b)

Fig. 7. Análises de risco de cibersegurança nas PME (%)



(Eurostat 2023b)

- Quanto a testes de segurança às TIC, 34% das PME em Portugal admitiram que os fazem, contra 33,3% na média da UE (grandes empresas: 78% em Portugal e 75,7% na média da UE).
- Apenas 26,8% das PME em Portugal aplicaram pelo menos dois fatores de autenticação em 2022, enquanto a média da UE atinge os 30% (grandes empresas: 63,7% em Portugal e 63,6% na média da UE).
- No que diz respeito a mecanismos de monitorização de atividade suspeita nos sistemas de TIC, 39,9% das PME em Portugal afirmam ter aplicado os mesmos, contra 39,7% na média da UE (grandes empresas: 83,1% em Portugal e 76,6% na média da UE).

- Entre as várias medidas identificadas neste inquérito do Eurostat, 51,3% das PME em Portugal aplicaram pelo menos cinco, contra 53,5% da média da UE (grandes empresas: 95,4% em Portugal e 92,4% na média da UE).

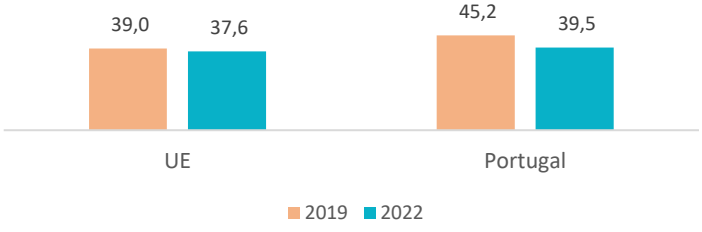
7. Capacitação Humana para a Cibersegurança

- Em 2021, segundo o estudo do Observatório de Cibersegurança sobre a economia da cibersegurança, quase um quinto das PME em Portugal manifestou ter dificuldade em contratar/reter trabalhadores dedicados a tarefas de cibersegurança (17,5%). Contudo, apenas 31,3% declarou não ter esta dificuldade e metade (51,2%) não se manifestou a propósito desta questão. Quanto mais pequenas as empresas, mais esta dificuldade se agudiza.
- Entre as PME que manifestaram esta dificuldade, 78,4% afirmaram que esta se deveu à escassez de profissionais a nível local e 56,8% aos custos elevados em termos salariais.
- Quando é realizada internamente, a gestão da cibersegurança nas PME em Portugal, em 2021, foi feita pelo departamento de informática (40,3% dos casos), a administração (29,5%) ou um responsável de segurança informática (26,5%). Quanto maior a empresa, mais peso tem o departamento de informática; quanto menor, mais peso tem a administração.
- Entre as PME com trabalhadores dedicados internamente à função de cibersegurança a tempo integral, 70% têm um colaborador alocado, 15% têm dois, 7% têm três, 2% têm quatro e 6% têm cinco ou mais.

(CNCS, 2022)

- De acordo com o inquérito do Eurostat, em 2022, quanto às atividades relacionadas com a segurança das TIC, em 39,5% das PME algumas destas atividades são realizadas internamente (37,6% na média da UE) (grandes empresas: 87,5% em Portugal e 83,8% na média da UE). Por outro lado, 71,8% têm atividades deste tipo realizadas por fornecedores externos (67,9% na média da UE) (grandes empresas: 66,6% em Portugal e 73,3% na média da UE) – ver figura 7.

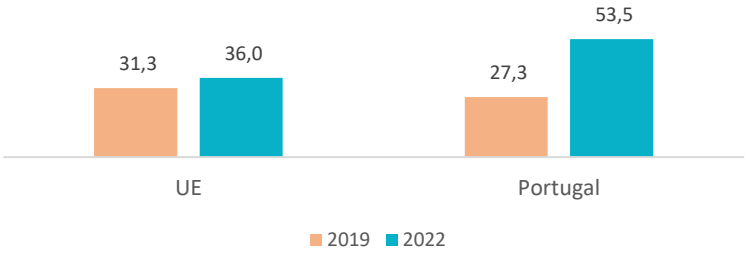
Fig. 7. PME com atividades de segurança das TIC realizadas pelos empregados internos (%)



(Eurostat, 2023b)

- Em 2022, 53,5% das PME em Portugal disponibilizaram internamente documentos com medidas, práticas e procedimentos sobre segurança nas TIC aos seus empregados, contra apenas 36% na média da UE (grandes empresas: 94,1% em Portugal e 79,6% na média da UE).
- A percentagem de PME no país, em 2022, com documentos com medidas, práticas e procedimentos sobre segurança nas TIC disponibilizados aumentou acentuadamente, em 26,2 pp – ver figura 5.

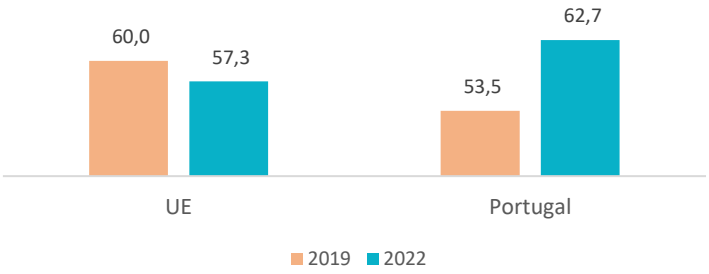
Fig. 5. Documentos com medidas, práticas e procedimentos sobre segurança nas TIC disponibilizados pelas PME (%)



(Eurostat, 2023b)

- No âmbito deste mesmo inquérito, 62,7% das PME em Portugal, em 2022, sensibilizaram os seus empregados para as obrigações de segurança nas TIC (55,6% com atividades voluntárias e 18,5% com atividades obrigatórias), contra 57,3% na média da EU (grandes empresas: 88,8% em Portugal e 91% na média da UE).
- Há mais PME a sensibilizar os seus empregados em Portugal para a segurança das TIC em 2022 do que em 2019, mais 9,2 pp – ver figura 6.

Fig. 6. Sensibilização dos seus empregados para as obrigações de segurança nas TIC, nas PME (%)



(Eurostat, 2023b)

8. Recomendações

Considerando os dados apresentados, deixam-se algumas recomendações para consideração:

- Capacitar as PME para a recuperação de serviços digitais após incidentes de cibersegurança que afetem a disponibilidade;
- Divulgar a Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) junto das PME para o reporte de incidentes graves;
- Continuar a investir no desenvolvimento de Políticas de Segurança das TIC nas PME;
- Promover um maior financiamento das PME para a cibersegurança;
- Apostar na sensibilização das PME em geral, mas com particular incidência no múltiplo fator de autenticação (ter em consideração as contas bancárias), análises de risco, testes de segurança, mecanismos de monitorização e uso de VPN;
- Promover a formação ou requalificação de especialistas a nível local;
- Sensibilizar a administração e os empregados das PME para as práticas mais essenciais de cibersegurança, garantindo que todos os empregados são sujeitos às mesmas, numa lógica contínua e orientada à criação de uma cultura.

9. Notas Conclusivas

As PME portuguesas, em diversos aspetos, comparam relativamente bem com as suas congéneres europeias, como, por exemplo, quanto ao número de incidentes e suas consequências, à existência de políticas de segurança das TIC, ao uso de palavras-passe fortes ou à existência de documentação sobre boas práticas de cibersegurança disponibilizada na organização. Todavia, noutros domínios, existe um trabalho de capacitação a intensificar, como, por exemplo, na recuperação de serviços digitais depois de sofrer incidentes, na disponibilidade orçamental para a cibersegurança, no uso do múltiplo-fator de autenticação ou no que se refere a recursos humanos especializados.

Julga-se que o quadro apresentado poderá ajudar na definição de estratégias que considerem a importância económica e social das PME. A ubiquidade das PME exige uma maior atenção a este tipo de organização, cuja transformação para a cibersegurança tende a trazer impactos sociais alargados e geograficamente distribuídos. O tipo de apoio a prestar terá, contudo, de se ater ao nível de maturidade em apreço, de modo que se desenvolvam instrumentos de capacitação acessíveis e com abordagens passo-a-passo (tutoriais).

10. Nota Metodológica

Os dados utilizados neste documento foram recolhidos no âmbito dos inquéritos referenciados e com base na validade metodológica garantida pelas entidades que os disponibilizaram. Sugere-se a consulta das referências para verificação das metodologias de recolha da informação. Os dados nacionais do Pordata e do Eurostat foram produzidos sobretudo pelo Instituto Nacional de Estatística. Os dados do *Relatório Cibersegurança em Portugal – Economia* foram desenvolvidos pelo Observatório de Cibersegurança do CNCS em parceria com o IAPMEI, I.P. - Agência para a Competitividade e Inovação. O inquérito do Eurobarómetro utilizado não é regular, mas sim de aplicação ocasional.

11. Siglas

CERT.PT: Equipa de Resposta a Incidentes de Segurança Informática Nacional [CERT - Computer Emergency Response Team]

CNCS – Centro Nacional de Cibersegurança

ENSC – Estratégia Nacional de Segurança do Ciberespaço

PME - Micro, Pequenas e Médias Empresas

TIC – Tecnologias de Informação e Comunicação

UE – União Europeia

VPN – Rede Virtual Privada [Virtual Private Network]

12. Referências

CNCS (2022) *Relatório Cibersegurança em Portugal – Economia*. Observatório de Cibersegurança. Centro nacional de Cibersegurança. Disponível em https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf [consultado a 30/06/2023]

EUROBARÓMETRO (2022) *Flash Eurobarómetro 496 PMEs e crime cibernético*. Eurobarómetro. Disponível em: https://europa.eu/eurobarometer/surveys/detail/2280 [consultado a 30/06/2023]

EUROSTAT (2023a) *Security incidents and consequences by size class of enterprise* [ISOC_CISCE_IC__custom_6640477], disponível em https://ec.europa.eu/eurostat/databrowser/product/page/isoc_cisce_ic [consultado a 30/06/2023]

EUROSTAT (2023b) *Security policy: measures, risks and staff awareness by size class of enterprise* [ISOC_CISCE_RA__custom_6600321], disponível em https://ec.europa.eu/eurostat/databrowser/product/page/isoc_cisce_ra [consultado a 30/06/2023]

PORDATA (2023) *Empresas e Pessoal*. Disponível em https://www.pordata.pt/home [consultado a 30/06/2023

Aliança para
a Cibersegurança