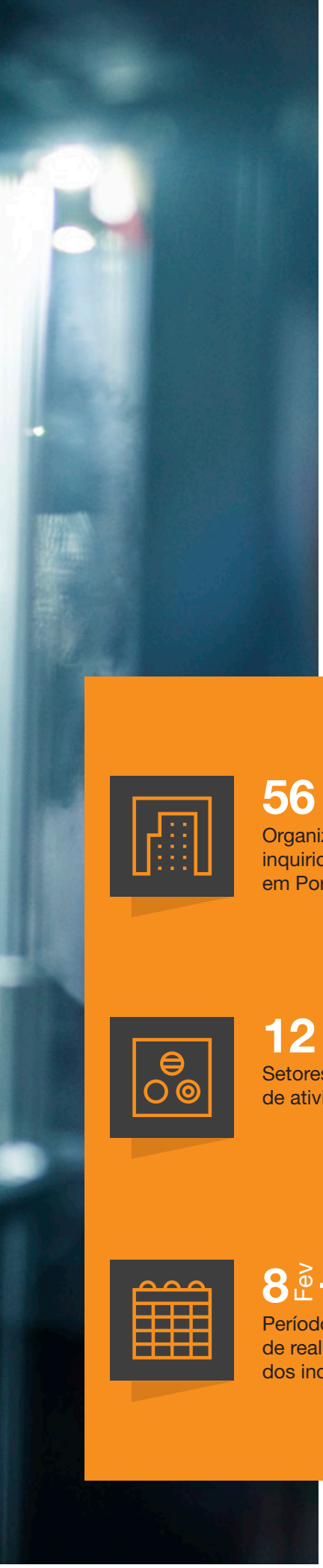
# Cyber Survey Portugal 2021

## Compreender a cibersegurança num novo panorama social

Dezembro 2021

pwc

pwc.pt/**cybersurvey**



# Introdução

Em 2020 verificámos uma rápida aceleração do processo de transformação digital das Organizações, em grande medida potenciado pelo contexto pandémico da COVID-19, que promoveu forçadamente a flexibilização da forma de trabalhar, principalmente através do trabalho remoto.

Este novo panorama obrigou à consideração de novos riscos e desafios para as Organizações na dimensão da cibersegurança, levando a que muitas tivessem de repensar a sua estratégia face a um período de "pandemia cibernética", por forma a dinamizar a aceleração rápida e segura, bem como proteger o valor dos seus ativos nesta fase de transição digital, em que o número de ciberameaças e outros incidentes têm aumentado.

A PwC tem vindo a acompanhar o atual impacto destas alterações para avaliar a maturidade, os principais desafios e as prioridades das Organizações em cibersegurança, contando com o apoio à divulgação do Gabinete Nacional de Segurança, bem como do Centro Nacional da Cibersegurança.

Foi neste sentido que desenvolvemos o **Cyber Survey Portugal 2021** – um inquérito em que procurámos aferir o nível em que se encontram as várias Organizações em Portugal em matérias de cibersegurança no ano de 2020 e compreender como estas se estão a preparar para adversidades no futuro.

Para a preparação deste relatório, foram inquiridas 56 Organizações a nível nacional, no período compreendido entre 8 de fevereiro a 5 de março de 2021, com representação nos diversos setores de atuação como a Indústria e Serviços, o Setor Público, Telecomunicações, Média e Tecnologia, Serviços Financeiros, entre outros.

Entre as questões levantadas neste inquérito, foram também endereçados vários tópicos de análise relacionados com a própria Estratégia Nacional de Segurança do Ciberespaço de 2019-2023.

**56**
Organizações inquiridas em Portugal

**12**
Setores de atividade

**8 Fev – 5 Mar**
Período de realização dos inquéritos

# A solidez cibernética em tempos adversos

**Miguel Dias Fernandes**
Consulting Partner da PwC
em Portugal, Cabo Verde e Angola

Se é certo que as novas tecnologias têm transformado Organizações inteiras, em todos os setores de atividade, ao longo dos últimos anos, nunca tal progresso foi tão importante e tão intenso como em 2020. Como o CEO da Microsoft, Satya Nadella, afirmou: "Em apenas 2 meses, assistimos a uma transformação digital equivalente a 2 anos".

2020 foi um ano atípico, devido à crise pandémica causada pela COVID-19, o digital superou todas as barreiras e mudou formas de estar e de trabalhar, tornando-as mais práticas, eficientes e, sobretudo, mais seguras para as pessoas poderem operar no novo normal.

Contudo, a cada vez maior sofisticação tecnológica tem, também, o seu lado potencialmente negativo. Ao deslocarem toda a sua estrutura e atividades para este meio, as empresas ficaram inevitavelmente mais expostas a riscos externos, nomeadamente ataques cibernéticos. Segundo a equipa CERT.PT, serviço integrante do Centro Nacional de Cibersegurança (CNCS) verifica-se um registo de 394 incidentes no 2º trimestre de 2020, o que se traduz num crescimento de 124% face aos 176 incidentes registados no mesmo trimestre do ano anterior.

Os incidentes desta natureza têm o potencial de afetar criticamente não só as operações das empresas, mas também de causar sérios danos financeiros e reputacionais.

O trabalho remoto veio garantir segurança ao nível da exposição individual, mas também tornou, inversamente, a segurança das empresas mais vulnerável.

Chegados aqui, importa olhar para dentro e começar a dar os primeiros passos sobre um tema que muito tem sido abordado, mas ainda pouco aprofundado internamente – a cibersegurança.

Uma das conclusões do nosso **Cyber Survey Portugal 2021** a de que a maioria das Organizações em Portugal estão dispostas a investir mais em cibersegurança por forma a mitigar e prevenir eventuais ameaças, tais como por exemplo o *phishing*, ataques de *malware* e *ransomware*, mas carecem de uma estratégia desenvolvida para esta área, bem como de equipas especializadas.

Torna-se, por isso, premente dotar as Organizações de competências de cibersegurança, envolvendo as pessoas, processos e tecnologia.

Das 56 Organizações inquiridas pela PwC, apenas 2 em cada 10 realizam testes e simulações de segurança com regularidade e cerca de um terço não têm equipa ou área de Cibersegurança, a nível interno.

Muitos têm sido os casos de incidentes com prejuízos na ordem dos milhões de euros, existem até exemplos a nível nacional, podendo ter um impacto negativo na reputação construída ao longos dos anos. Falamos da identidade da própria Organização, da sua marca lá fora.

Não é por acaso que as três principais preocupações entre os inquiridos foram os danos reputacionais, a indisponibilidade de sistemas por longos períodos e os incidentes que causam perdas financeiras.

A ameaça é real e torna-se essencial mobilizar meios (internos e externos) para tornar as Organizações mais resilientes a nível cibernético. O orçamento para a Cibersegurança deve corresponder ao nível esperado de potenciais ameaças. E envolver os trabalhadores transversalmente, criar um modelo de governação, investir em novas tecnologias e desenvolver a automação serão abordagens-chave para agilizar esse processo.


01

# Principais resultados

## Preocupações...

Neste período pandémico, as preocupações das Organizações também se têm focado nos riscos cibernéticos. Aliás, o nível de preocupação aumentou em cerca de 50% face ao reportado anteriormente. Refere-se também que estas preocupações devem ser alinhadas com a estratégia das Organizações para assim garantir uma aceleração rápida e segura através dos meios necessários, começando pela reestruturação do modelo de governo para delinear a atribuição de responsabilidades para a cibersegurança (e.g. CISO).

**15%**

das Organizações estão preocupadas com **danos reputacionais** e com a indisponibilidade sistemas críticos, por um período prolongado.

**13%**

das Organizações inquiridas temem incidentes que causem **perdas financeiras** ou o roubo de informações confidenciais.

**1 em cada 10**

preocupa-se com a **perda de dados pessoais**, e, em grande medida, essa preocupação parte da exfiltração de dados.

## … e ameaças das Organizações

De acordo com o inquérito da PwC, o panorama de segurança português alterou drasticamente em 2020 e cerca de 40% dos inquiridos admitiram que experienciaram pelo menos um incidente de segurança no último ano.

Deve-se notar que estes incidentes são somente aqueles detetados pela Organização, não devendo ser descurados os não detetados.

**#1 Phishing**

Conjuntamente com o *smishing*, são as **principais ameaças a enfrentar no próximo ano** para 64% das Organizações. Mais de metade (59%) temem ainda situações de *malware*.

**27%**

das Organizações experienciaram **entre um a cinco incidentes** nos últimos 12 meses que antecederam ao inquérito.

**59%**

dos incidentes registados envolveram **dados pessoais**.

# Da estratégia nacional

Os objetivos estratégicos da Estratégia Nacional de Segurança no Ciberespaço (ENSC) de Portugal devem ser alinhados com a aquela que é a estratégia das Organizações para a cibersegurança.

74% dos inquiridos – na sua maioria grandes empresas do setor da indústria e serviços – referiu ter conhecimento da ENSC. No entanto, apenas 14% admitiu conhecer totalmente o seu conteúdo.

# …à visão das Organizações

Para uma resposta eficaz às ameaças cibernéticas, é necessário construir uma visão estratégica para a cibersegurança que inclua também o respetivo orçamento de forma a garantir a afetação eficiente de recursos nas iniciativas prioritárias face às necessidades do negócio.

Em grande medida, as Organizações reconhecem a necessidade em investir na cibersegurança, mas 63% dos inquiridos, sobretudo as grandes empresas, referem que o seu investimento não corresponde totalmente ao que consideram ser necessário face às potenciais ameaças.

**14%**

Afirmou que a ENSC afetou a sua Organização, sendo que a maioria admitiu que a sua existência as tornou mais conscientes acerca das potenciais ameaças.

**68%**

das Organizações admitiu nunca ter notificado o CNCS.

Porém, dos 18% que já o fizeram, a grande maioria referiu ter notificado o CNCS para reportar incidentes e ataques de *phishing*.

**> 50 mil €**

Este é o valor aproximado que a maioria das Organizações inquiridas indica ter disponível para cibersegurança.

No entanto, um terço considera que o seu investimento não é adequado face às ameaças existentes e potenciais, e 43% admite que o seu investimento é pouco, ou só em parte, equilibrado.

**15%**

têm como prioridade elevada o desenvolvimento de iniciativas que promovam a consciencialização em cibersegurança nos próximos 12 meses.

Cerca de um quarto referiu ainda levar a cabo iniciativas de gestão de identificação e acessos e de segurança de dispositivos móveis.

# Cinco ações…

1. Redefinir a sua estratégia de Cibersegurança
2. Repensar o orçamento de Cibersegurança
3. Nivelar o "campo de jogo" com os atacantes
4. Construir resiliência para cada cenário
5. Tornar a sua equipa de segurança "à prova do futuro"

# …com alguns fatores críticos

Como tal, qualquer abordagem à cibersegurança deve compreender os fatores críticos que devem ser considerados para garantir o sucesso da estratégia. Neste sentido, deve envolver as pessoas, a tecnologias, as capacidades e processos e, por fim, a automação.

**Pessoas**

**Capacidades e processos**

**Tecnologia**

**Automação**

02

# Enquadramento

## Vivemos uma pandemia cibernética

No atual contexto da pandemia, a transformação digital tem sido acelerada com a adaptação da atividade das Organizações. O investimento em tecnologias, sobretudo em ferramentas colaborativas, e o reconhecimento da necessidade de um maior investimento em infraestruturas digitais - principalmente no caso dos fornecedores dos serviços de internet -, são um reflexo de tentativa de dar resposta ao aumento exponencial do tráfego de dados verificado desde 2020. (Fonte: ITU, 2021; OECD, 2020) Esta aceleração teve impacto na forma como as Organizações oferecem os seus produtos ou serviços (mais digitalizados), na implementação de formas de trabalho mais flexíveis, adotando um regime remoto parcial ou integral. Simultaneamente, esta intensificação da digitalização trouxe, também, novos riscos e potenciou o aumento dos ciberataques.

De facto, este é um dos maiores riscos apontados no relatório do *The Global Risks Report 2021* do Fórum Económico Mundial. No top 10 de riscos por probabilidade de ocorrência, as falhas de cibersegurança ocupam a 9ª posição. Outros riscos tecnológicos, como a concentração de poder digital e a desigualdade digital estão presentes entre os principais riscos deste ano.

É neste sentido que a PwC designa a atual conjuntura no seu relatório *Cyber Threats 2020* como uma "pandemia cibernética", devido à maior exposição a estes riscos. Esta exposição, além de associada em parte às novas formas de trabalho, está bastante influenciada pela instrumentalização da pandemia nas campanhas maliciosas.

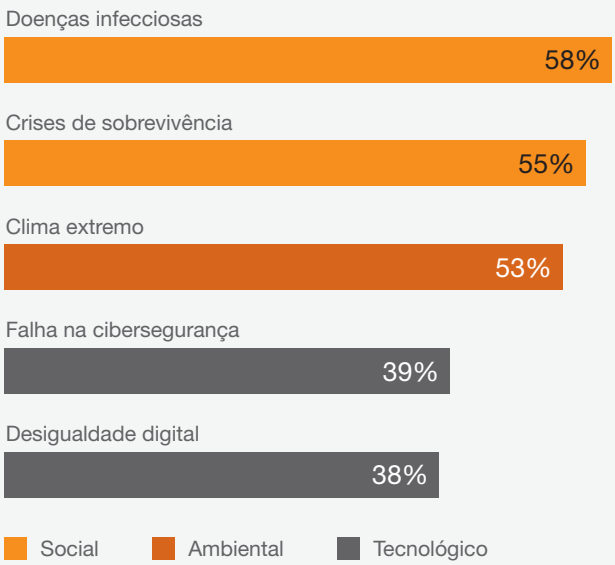
Uma parte substancial dessas campanhas, como a *Trickbot*, a *Emotet*, a *AppleSeed*, entre outras, instrumentalizam os temas dedicados à Covid-19 – como a testagem e as campanhas de compensação aos trabalhadores em regime de *lay-off* –, manipulando o utilizador através de técnicas de engenharia social, tipicamente via correio eletrónico (*phishing*) e via mensagem de texto (*smishing*), visando a infeção do computador do utilizador para fins ilícitos.

As repercussões para as Organizações são cada vez maiores, bem como proveito económico para o agente cibecriminoso, reconhecendo que uma parte substancial do valor das Organizações reside no digital. Estes ativos podem ser a propriedade intelectual, dados sensíveis (e.g. dados bancários, pessoais), entre outros, podendo recorrer às diversas técnicas e táticas para enriquecimento ilícito. Por vezes, o intuito poderá ser somente o de causar interrupção dos serviços para finalidades intrínsecas do cibercriminoso.

De acordo com ITU, os **custos** poderão **ascender os $2 biliões.**

### Top 5 perigos a nível global

Riscos a curto prazo (0-2 anos)




**Fonte:** WEF. *Global Risks Report 2021*

# Incluir a cibersegurança na estratégia de negócio

Face a estes factos verificámos, à escala global, uma maior necessidade de repensar o negócio por parte das Organizações face aos riscos de cibersegurança com tendência crescente. De acordo com o inquérito *PwC Digital Trust 2021*, 96% dos respondentes apontaram existir uma necessidade de realinhar a estratégia do negócio com a cibersegurança.

No processo de transformação digital, as Organizações devem considerar medidas que mitiguem os riscos inerentes a esta transformação e envolver, cada vez mais, a cibersegurança e os temas da privacidade na sua estratégia de negócio – essa necessidade é identificada por uma em cada duas entidades.

Este alinhamento também deve ser considerado em Portugal, pois os assuntos referidos previamente também têm efeitos negativos nas Organizações portuguesas, devendo estes riscos de cibersegurança ser acautelados na estratégia do negócio.

As campanhas maliciosas que mencionámos previamente registaram, também, um aumento considerável nas em Portugal, em particular via *phishing*.

De acordo com o Relatório Riscos e Conflitos 2021, do CNCS, verificou-se um aumento substancial do volume de incidentes de cibersegurança em 2020, em particular de campanhas de *phishing/smishing* – 43% dos incidentes registados –, a infeção por *malware* (12%), o *ransomware* e algumas formas de intrusão, potenciadas pelo contexto atual de trabalho remoto, por exemplo, e uma maior vulnerabilidade técnica. Ameaças como várias formas de fraude/burla e desinformação digital foram também registadas. No total, o número de incidentes com vulnerabilidades registados pelo CERT.PT aumentou em 88% no ano de 2020, face a 2019.

Segundo dados da *Kaspersky*, Portugal foi o segundo país do mundo a sofrer mais ataques de phishing em 2020, atrás do Brasil.

03

# Preocupações e ameaças

## As ciberameaças estão no topo das preocupações da gestão

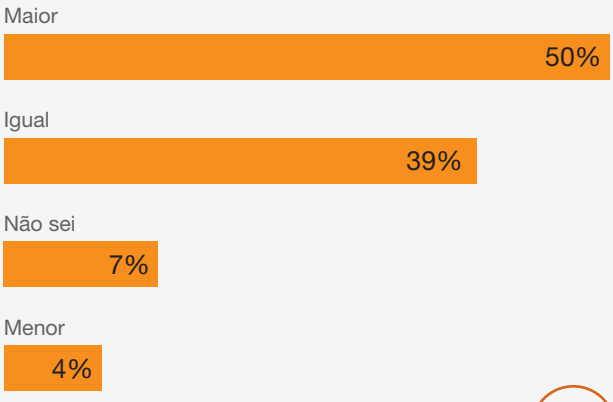
Este é um assunto que preocupa a gestão de topo das Organizações, como podemos notar na 24ª edição do *CEO Survey* global da PwC, em que a principal preocupação indicada pelos CEO na Europa Ocidental é a das ciberameaças.

Em linha com o global, o nível de preocupação dos CEO portugueses com este tema também tem vindo a crescer, com 50% a indicar que aumentou face ao ano anterior. Este é, de facto, um tema que, cada vez mais, deve ser enquadrado ao nível estratégico nas Organizações, devendo integrar pessoas, processos e as tecnologias para contemplar a cibersegurança e a privacidade.

É compreensível o aumento desta preocupação, face ao crescente aumento de determinadas tipologias de incidentes de cibersegurança ao CERT.PT, como tivemos oportunidade de mencionar previamente.

A preocupação das Organizações com as ciberameaças é **cada vez maior.**

**Q:** Relativamente há 12 meses atrás, como compara o atual nível de preocupação da Organização relativamente às ameaças enfrentadas?



**Q:** Quais as maiores preocupações da sua Organização em relação às consequências de segurança da informação ou cibersegurança?


# Principais consequências com a falta de segurança da informação

15% das Organizações em Portugal **temem danos ao nível da sua marca e reputação** e 14% receiam a indisponibilidade de sistemas críticos por longos períodos.

Mais do que danos estritamente financeiros, as Organizações portuguesas compreendem que este tipo de danos pode acarretar repercussões mais abrangentes como a perda da confiança.

As Organizações estão, também, preocupadas com a indisponibilidade dos sistemas críticos por um período prolongado. Ao ter as atividades mais digitalizadas, é necessário que os sistemas estejam operacionais para garantir a continuidade do negócio.

Outra preocupação foca-se na exfiltração de dados sensíveis, como os dados pessoais, à qual estão associadas pesadas coimas ao incumprimento do RGPD.

As 4 principais preocupações são os **danos reputacionais, a indisponibilidade de sistemas por longos períodos e os incidentes que causam perdas financeiras.**

# Ações de formação e consciencialização sobre cibersegurança

Para uma transição digital que proteja o valor dos ativos e garanta uma aceleração rápida e segura, cabe às Organizações desenvolverem controlos de cibersegurança que permitam mitigar os riscos associados ao negócio. É por esse fundamento que procuramos compreender as ações tomadas.

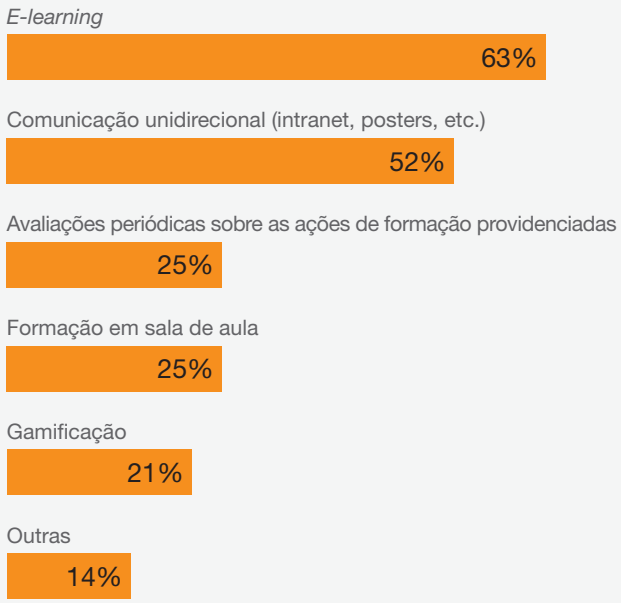
Relativamente às ações de consciencialização, é relevante compreender a necessidade de existir uma **comunicação unidirecional através de materiais de *awareness*** como posters, publicações internas, entre outras, conjuntamente com **ações de formação em *e-learning***.

As Organizações têm previsto aumentar as suas comunicações unidirecionais nos próximos 12 meses. No entanto, este aumento não é tão expressivo como aquele verificado para as ações de formação em *e-learning*. Já as iniciativas de formação em sala de aula verificou-se uma quebra, potenciada pelo contexto pandémico e pela aceleração digital que dela resultou.

É relevante compreendermos que estas formações, para assumirem o efeito pretendido de sensibilização, precisam de ser posteriormente avaliadas para verificar se houve uma compreensão efetiva dos temas abordados. Neste sentido, apenas 10% das Organizações avaliam periodicamente as ações de formação que proporcionam aos seus colaboradores. Esta é uma situação onde as Organizações identificam falhas e estão a procurar soluções de melhoria.

Devemos ainda compreender que das ações de sensibilização, a maioria não têm um caráter obrigatório, pese embora o número de respondentes seja limitado.

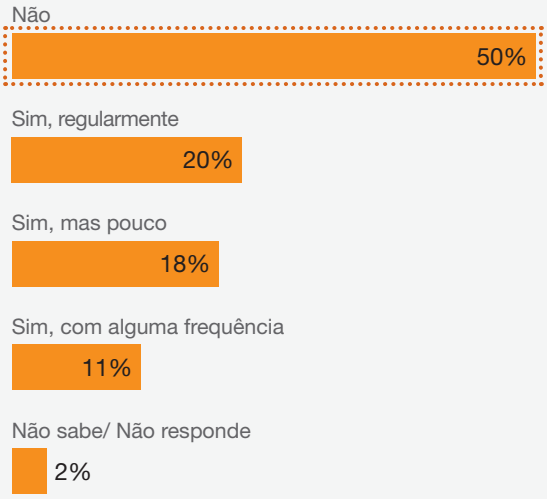
**Ações de formação previstas, relativamente a cibersegurança**




**32%** das Organizações **não prevê ações de consciencializaço.**

# 49% realizam testes de cibersegurança, mas não regularmente

**Q:** A sua Organização realiza testes de cibersegurança (e.g. simulação de ataques de *phishing*, simulação de roubo de informação, etc.)?




Observando os resultados, verificamos que apenas **20% das Organizações** inquiridas em Portugal **realizam testes regularmente**, enquanto que as restantes fazem-no de forma dispersa no tempo e **50% não realizam testes** de todo.

Esta situação poderá incorrer em riscos que não estão a ser acautelados no momento indicado para empregar sessões direcionadas de sensibilização aos colaboradores com desempenho abaixo do expectável, mitigando os riscos tipicamente conexos com a engenharia social.

**50% dos inquiridos indica não realizar qualquer teste de cibersegurança.**

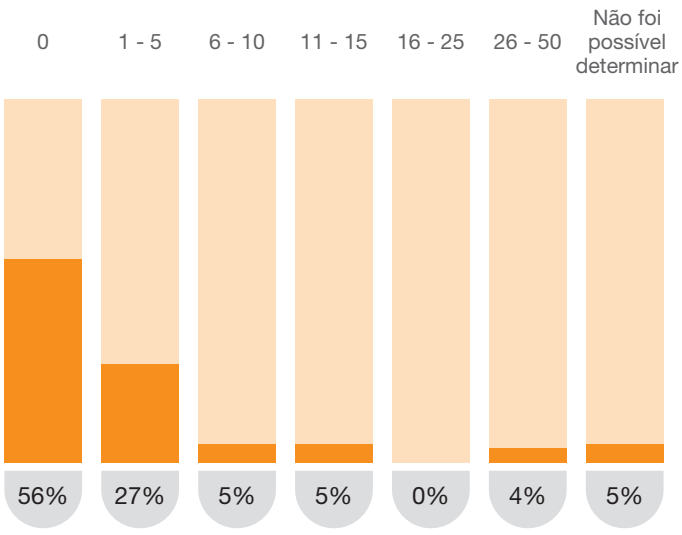
# O *spam* e o *phishing* são a maior causa de incidentes

De acordo com os dados prestados pela equipa coordenadora CERT.PT, Portugal tem sido alvo de um aumento considerável do número de incidentes de cibersegurança. Das Organizações inquiridas, 47% refere que foi alvo de um incidente de cibersegurança nos últimos 12 meses, e 27% referiu ter sofrido entre 1 a 5 incidentes.

Destas 47% incluímos aquelas que não conseguiram determinar o incidente pela circunstância de potencialmente não terem capacidades de monitorização para identificar que tenha decorrido algum incidente.

**47% das Organizações experienciou incidentes de cibersegurança nos últimos 12 meses.**

**Nº de incidentes nos últimos 12 meses**



## 27% sofreram perdas monetárias com os incidentes e mais de metade destes envolve dados pessoais.

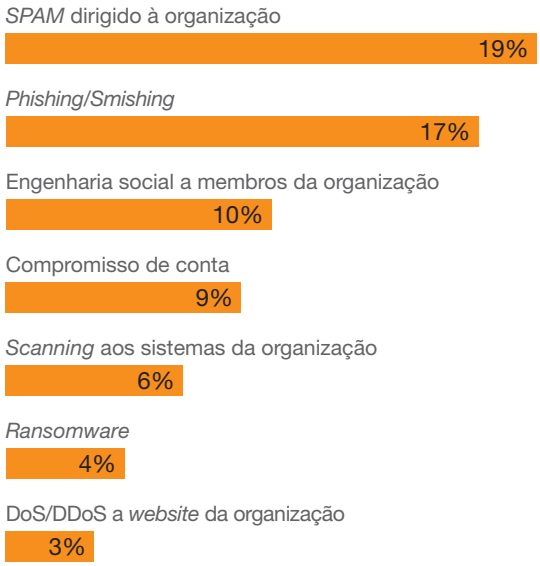
Em Portugal, as maiores causa de incidentes com cibersegurança identificados pelas Organizações são o *spam* e o *phishing*, e 27% das empresas revelaram ter sofrido perdas monetárias com estes ataques.

As iniciativas mais importantes para evitar este tipo de ataques passam por campanhas de sensibilização que permitam identificar este tipo de engenharia social.

Da mesma forma, também reforçando os seus investimentos nesta área as Organizações podem minimizar os riscos de perdas, nomeadamente através de métodos de análise preditiva que permitam quantificar e priorizar as ameaças permitindo canalizar recursos humanos e monetários de forma eficaz.

Adicionalmente, 35% destes incidentes envolveram dados pessoais, pelo que se deve também considerar avaliar as medidas de gestão de *compliance* com o enquadramento legal da privacidade a nível da União (e.g. RGPD, *E-Privacy*), e posicioná-las como um motor de geração de confiança nas pessoas ao proteger os seus dados.

### Tipo de incidentes




# O *phishing/smishing* e o *malware* são as maiores ameaças

Das ameaças identificadas, as que mais preocupação causam são principalmente o *phishing* e o *malware*. Dentro do *malware*, o *ransomware*, representa a 3.ª maior ameaça para as Organizações.

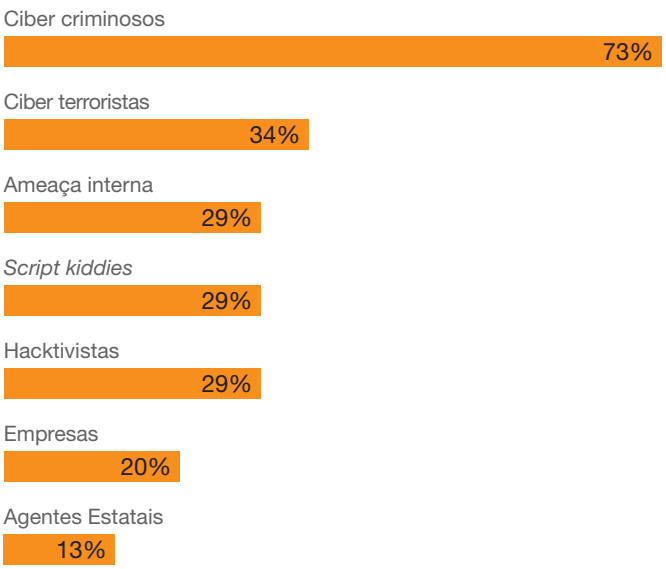
Os cibercriminosos são considerados **os maiores agentes de ameaça**, seguidos dos **ciberterroristas** não só pela crescente adoção do ciberespaço e dos sistemas *cloud* pelas Organizações como suporte para o seu negócio, mas também pela facilidade de acesso a ferramentas tecnológicas sofisticadas com que executam os ataques.

Verifica-se, também, algum receio com as ameaças internas. Ou seja, os próprios colaboradores por motivos diversos (financeiros, maliciosos ou negligência) poderem provocar danos à Organização. Assim, e considerando que **o 3º maior agente identificado são as ameaças internas**, as Organizações devem implementar iniciativas de mitigação destes riscos com um especial foco de atuação na força de trabalho.

É, também, relevante constatar que o grupo de agentes de ameaça enunciados anteriormente convivem com os *Script Kiddies* - indivíduos geralmente pouco qualificados, mas com fácil acesso a tecnologias e meios para recorrer a fontes abertas (habitualmente a um custo reduzido). Este contexto, possibilita o aumento dos ataques por estes agentes.

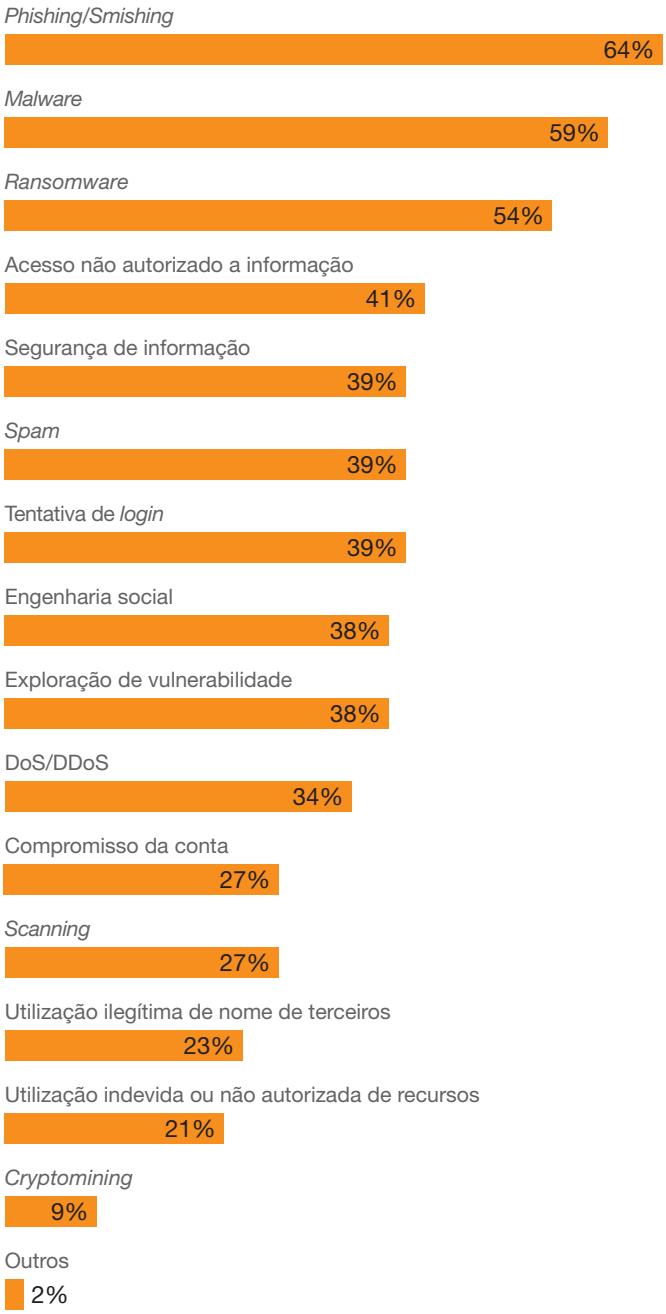
**A preocupação com as ameaças deverá aumentar nos próximos 12 meses.**

## Agentes de ameaças




**Os cibercriminosos e os ciberterroristas são os dois principais agentes de ameaça.**

## Maiores ameaças



04

# Da estratégia nacional à visão das Organizações

## Conhecimento da ENSC

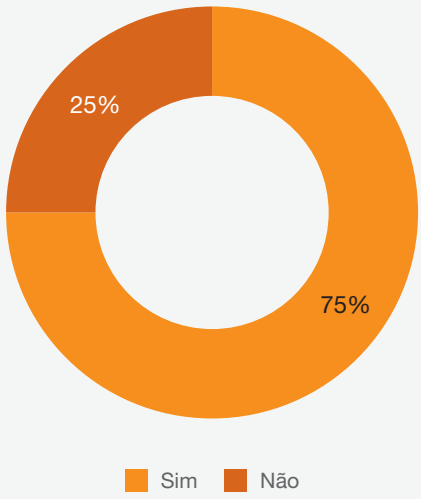
No âmbito da estratégia das Organizações, estas devem ter como prioridade procurar obter um alinhamento da cibersegurança com os objetivos estratégicos do negócio. Contudo, devem também permitir ser influenciados pelos desafios estratégicos identificados pela Estratégia Nacional de Segurança do Ciberespaço (2019-2023).

É relevante o conhecimento do conteúdo desta estratégia para compreender as sinergias que o Estado procura estabelecer com as Organizações, entre as quais as ações nvestigação, sensibilização, partilha de informação, colaboração para a resposta aos desafios da cibersegurança.

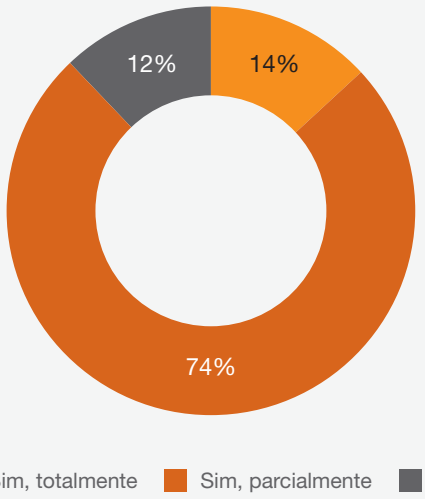
Em Portugal 74% das Organizações indica ter conhecimento da existência da ENSC. No entanto, apenas 14% referiram conhecer o seu conteúdo na totalidade.

**74% conhece a ENSC, mas somente 14% conhece totalmente os conteúdos.**

**Q:** Tem conhecimento da existência de uma Estratégia Nacional de Segurança no Ciberespaço (ENSC)?




**Q:** Se sim, tem conhecimento do seu conteúdo?



# Impacto da ENSC

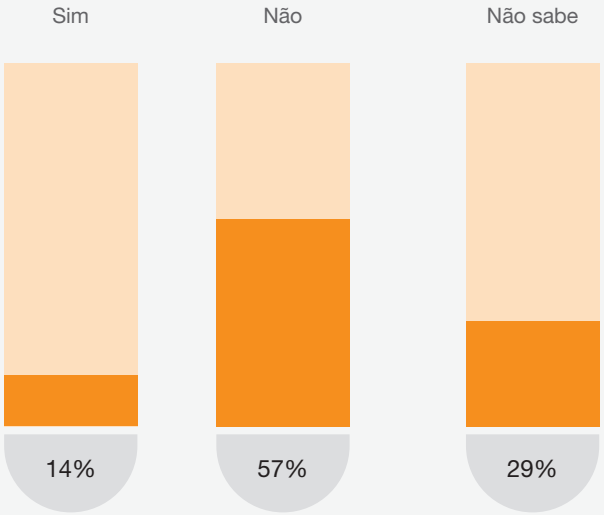
O conhecimento da estratégia é relevante para compreender as principais ameaças identificadas pelo Estado português e, subsequentemente, alinhar a estratégia do negócio, bem como as iniciativas de cibersegurança ao perfil de ameaças e desafios mencionados na ENSC.

De entre as Organizações inquiridas, 14% referiram ter sofrido um impacto devido à ENSC, sendo que desses, 38% refere ter-se tornado mais consciente quanto às potenciais ameaças de cibersegurança a que está exposto.

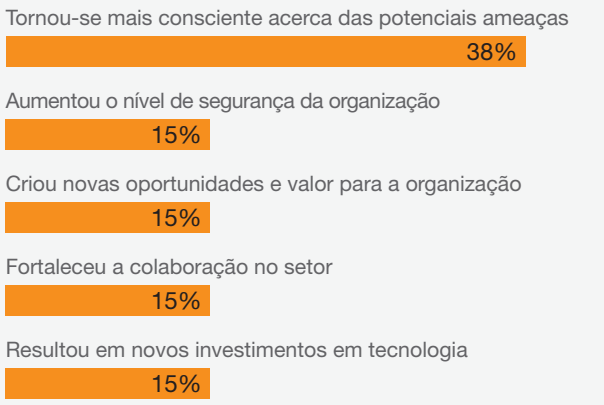
Estes apontam, ainda, que a ENSC permitiu aumentar os seus níveis de segurança, potenciou a criação de novas oportunidades e valor para a Organização, fortaleceu a colaboração com o setor e resultou em novos investimentos em tecnologia.

**Verificamos que apenas 14% das Organizações apontam que a ENSC teve impacto na estratégia do negócio.**

**Q:** A ENSC afetou a sua Organização?




**Q:** Se sim, de que modo?



# Notificação ao CNCS

De acordo com o Eurobarómetro de 2020, a maioria dos respondentes em Portugal sentem estar desinformados quanto aos riscos do cibercrime: 80% desconhece os canais de reporte disponíveis para o efeito.

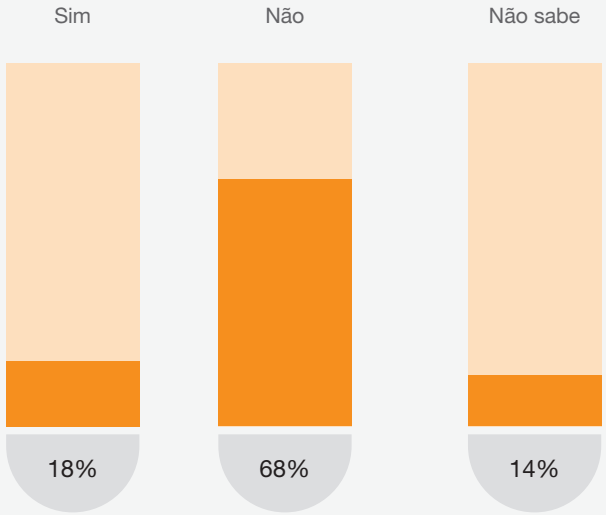
Não é por acaso que Portugal é o país que, de acordo com o mesmo estudo, menos reporta cibercrimes ou outras condutas ilícitas *online*.

Este reporte é relevante pois representa passo para se obter apoio operacional do CNCS na resolução de incidentes. Este poderá permitir ao CNCS compreender se está em curso alguma campanha maliciosa que necessite de uma resposta à escala nacional, ou até mesmo a nível comunitário.

Neste sentido, questionámos as Organizações relativamente ao reporte de incidentes de cibersegurança ao CNCS. Os resultados mostram que apenas 18% das reportam estes incidentes, sendo que os que reportam fazem-no, maioritariamente, para casos de *phishing*.

**82% das Organizações inquiridas indica nunca ter notificado o CNCD de qualquer incidente.**

**Q:** empresa que representa já notificou o CNCS?




# A consciencialização é a iniciativa mais prioritária

Relativamente ao investimento em matéria de cibersegurança, os resultados mostram que a **principal iniciativa** a ser considerada são as **ações de consciencialização** e a gestão de identidades e acessos. É, também, relevante **a segurança dos dispositivos móveis**, reconhecendo cada vez mais os riscos associados à utilização destes equipamentos.

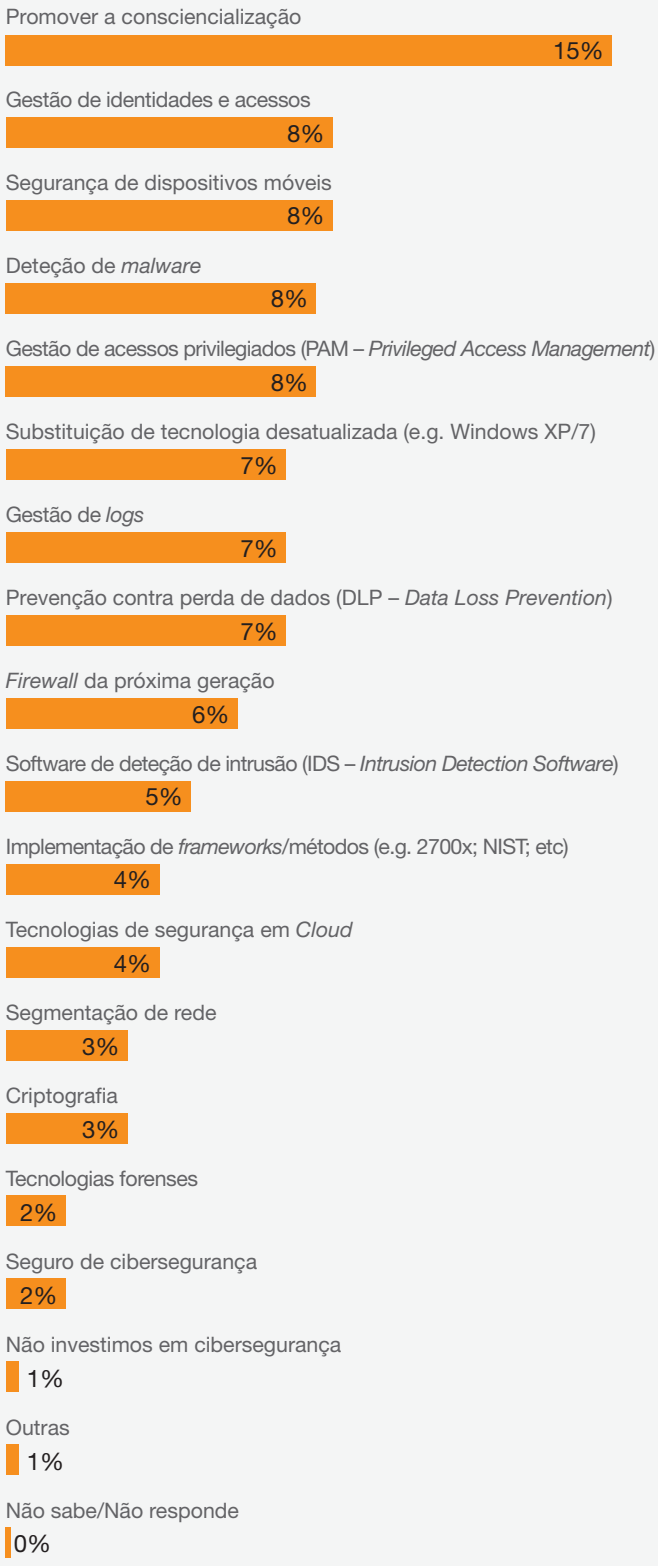
Numa visão por grupos, 18% das Organizações referem que as principais iniciativas a implementar deverão estar relacionadas com a **segurança da infraestrutura de redes** (*firewall*, tecnologias de segurança na *Cloud*, IDS, segmentação de rede) e 16% privilegiam a **gestão de acessos e identidades** (gestão de identidades e acessos e gestão de acessos privilegiados).

Este dado deve ser lido tendo em consideração os seguintes aspetos:

- O conjunto finito de possíveis iniciativas no âmbito deste *survey*;
- A existência de entidades que não responderam;
- A existência de Organizações que consideram não investir em cibersegurança.

**A iniciativa considerada como prioritária é a ação de consciencialização, mas numa visão segmentada, a segurança da infraestrutura de redes surge em primeiro lugar.**

**Q:** Identifique as iniciativas consideradas como "alta prioridade" para cibersegurança considerando os próximos 12 meses?



# Orçamento para cibersegurança

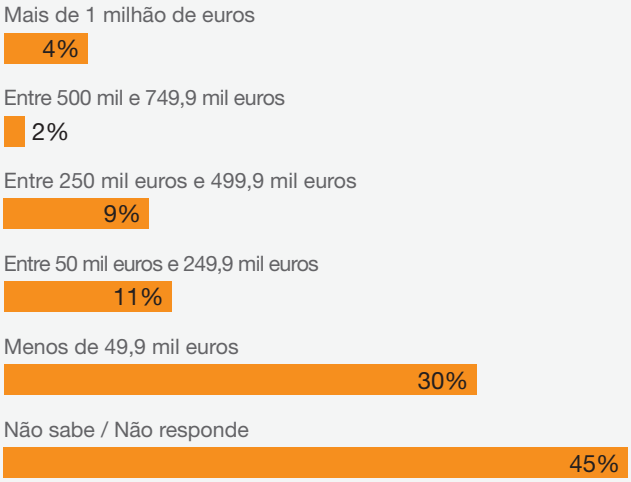
Como já referido, a visão estratégica das Organizações para a cibersegurança é crítica, uma vez que permite proteger os seus ativos, bem como estimular a confiança dos mercados em que opera, pelo facto de ter implementados mecanismos de gestão de risco.

Reconhecendo a necessidade de dimensionar e priorizar estas iniciativas, as Organizações deverão ter um orçamento dedicado à cibersegurança.

Este investimento pode permitir alavancar as iniciativas previstas com base numa análise de risco e quantificar os prejuízos associados à materialização de ameaças aos ativos.

**Um terço das Organizações disponibiliza menos de 50 mil euros para a cibersegurança.** Não obstante, é necessário olhar para estes valores tendo em conta a dimensão das Organizações inquiridas, e o facto de o tecido empresarial português ser maioritariamente composto por pequenas e médias empresas.

**Q:** Qual o orçamento destinado à Cibersegurança na sua Organização? Por favor, responda à questão tendo por base a situação atual e a previsão para os próximos 18 meses?




## Cerca de um terço das Organizações prevê gastar menos de 50 mil euros em cibersegurança no próximo ano e meio.

# Adequação do investimento em cibersegurança

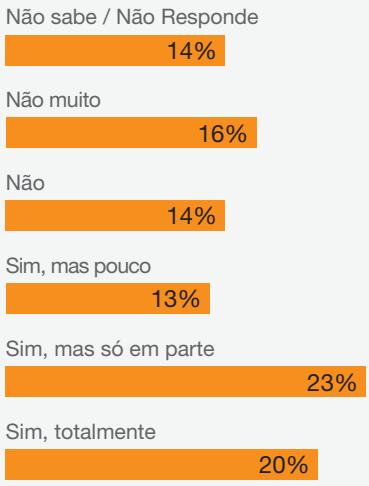
No já referido *Digital Trust 2021* da PwC, verificámos que a maioria das Organizações têm consciência dos riscos a que estão expostas e pretende aumentar o investimento em cibersegurança para os prevenir e mitigar.

Nesse sentido, questionámos as Organizações sobre o investimento realizado em cibersegurança, e constatou-se que 77% (excluindo não sabe/não responde) referem que o investimento realizado não é totalmente equilibrado face às ameaças existentes e potenciais.

No entanto, e para esta mesma amostra, caso analisemos os investimentos que cumprem parcialmente (resposta "Sim, mas pouco" e "Sim, mas só em parte") o equilíbrio necessário para endereçar os riscos cibernéticos, verifica-se que cerca de 36% das Organizações apontam que o investimento corresponde parcialmente às necessidades verificadas de cibersegurança.

É importante mencionar que 14% das Organizações preferiu não responder ou referiu não saber responder a esta questão.

**Q:** Considera que o investimento realizado em cibersegurança é equilibrado face às ameaças existentes e potenciais?




**77% refere que o investimento realizado não é totalmente equilibrado face às ameaças existentes e potenciais questionadas.**

# As competências em Cibersegurança são externalizadas

Atualmente, as Organizações lutam pelos melhores talentos e pelas competências técnicas de cibersegurança, sendo que as Organizações devem estar dotadas de recursos humanos especializados nesta área.

Estes recursos são escassos, sendo que uma das possibilidades passa por recorrer à externalização destas atividades de cibersegurança através de *managed service*. (*PwC Digital Trust 2021*)

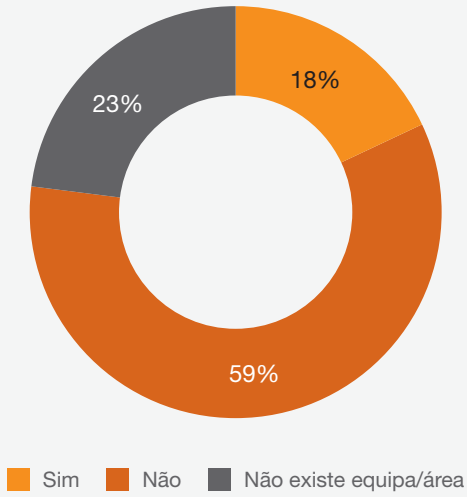
**Portugal é o 2º país que mais externaliza a atividade de cibersegurança.**

De acordo com dados do Eurostat, Portugal é o **2º país que mais externaliza a atividade de cibersegurança**. Nesse sentido, procurámos verificar se as Organizações pretendem intensificar o recrutamento de trabalhadores para esta área, mas 59% indica não estar a considerar novas contratações.

Esta tendência pode convergir com a externalização dos serviços de cibersegurança para fornecedores terceiros.

Adicionalmente, os resultados mostram que 23% das Organizações não têm uma equipa especializada ou um departamento de cibersegurança. Nestes casos, a primeira solução indicada é a de recorrer às áreas de tecnologias de informação para para colmatar esta lacuna.

**Q:** Consideram contratar mais pessoas para esta área?




# 61% das Organizações inquiridas não tem um CISO nomeado

Dentro das ações a serem consideradas pelas Organizações, procurámos compreender a sua dimensão, facto que consideramos relevante para se verificar, ou não, uma maior adesão à cibersegurança pela gestão de topo e, em certa medida, integrar a cibersegurança com a estratégia de negócio.

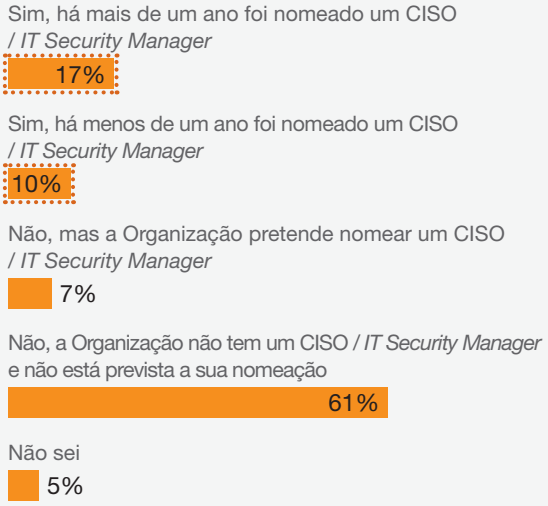
Um maneira habitualmente utilizada para capacitar a maturidade da Organização e diferenciar a mesma no mercado passa pela obtenção de certificações (e.g. ISO 27K). Cerca de 62% dos inquiridos indica que a sua Organização não possui certificações no âmbito da cibersegurança e privacidade de dados, e apenas 13% está a planear ou em processo de obtenção dessas mesmas certificações.

**Em termos do modelo de governo, cerca de 61% das Organizações não têm a função de CISO ou semelhante, como também 62% das Organizações não têm certificações.**

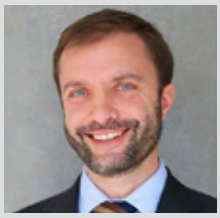
Cerca de 61% das Organizações inquiridas não tem designado um CISO (*Chief Information Security Officer*), ou equivalente, para gerir as questões relacionadas com cibersegurança.

Quanto aos colaboradores que as Organizações têm atualmente alocados a esta área, a maioria não ultrapassa as cinco pessoas.

**Q:** A sua Organização tem um CISO ou função equivalente?



# A Cibersegurança como ferramenta de proteção do valor da Organização



**Jorge Sacadura Costa**
Consulting Senior Manager da PwC em Portugal, Cabo Verde e Angola

Todos concordamos que, atualmente, vivemos num contexto de profundas e abrangentes transformações organizacionais. As empresas apostam, cada vez mais, em novas soluções tecnológicas e modelos de negócio mais diferenciados. Adicionalmente, a frequência destas transformações é cada vez mais superior.

Da nossa experiência, as organizações (e os seus clientes) têm também outro tipo de preocupações. Sem nunca abdicarem da qualidade dos produtos ou serviços, dão também relevância a temas como a confiança, privacidade, ambiente, entre outras.

Uma das principais questões que se coloca aos líderes, prende-se essencialmente com o desconhecimento de como prosperar num cenário com estas características (novos riscos/ preocupações e maior incerteza).

Atuando nas vertentes da (geração de) Confiança e (garantia da) Privacidade, deve-se passar a encarar a Cibersegurança como o veículo que possibilita e incentiva que se integrem estas preocupações, nas atividades do dia-a-dia de uma Organização: desenvolvimento de produtos, processos, gestão de dados (incluindo os pessoais), entre outros.

**Como construir uma função de Cibersegurança com estas características?**

Idealmente, deve-se implementar uma estratégia de Cibersegurança que garanta o seu alinhamento com os objetivos e riscos da organização como um todo e não apenas com a vertente tecnológica. É esta estratégia que permite o desenho de uma estrutura funcional clara, onde a definição e o conhecimento das responsabilidades de cada elemento é transparente, traduzindo-se assim numa menor ambiguidade em momentos de tomada de decisão.

Este objetivo é cumprido através do desenho de políticas e procedimentos robustos ao mesmo tempo que se investe  numa arquitetura de segurança (devidamente integrada na de Sistemas de Informação) que atue como catalisador destas características.

De acordo o estudo "2022 Global Digital Trust Insights" da PwC, 69%das organizações prevêem um aumento dos gastos cibernéticos em 2022, em comparação com 55% do ano passado. Cerca de 26% prevêem aumentos de 10% dos gastos cibernéticos (apenas 8% no ano passado). Importa referir que, mais de 50% das organizações esperam um aumento nos número de incidentes reportados no próximo ano, acima dos níveis de 2021.

Em conclusão, e apesar da crescente complexidade dos cenários que descrevemos, as organizações identificaram que a chave para uma maior eficácia na concretização do potencial deste investimento, reside na simplificação da operacionalização dos modelos de governo. Esta simplificação, tem em consideração os 4 Ps da Cibersegurança:

**Princípios:** O CEO deve definir um princípio inequívoco para o estabelecimento da segurança e privacidade como um imperativo para a criação de negócio.

**Pessoas:** Contratar o líder certo e permitir que o CISO, as equipas de segurança e as de negócio estejam articuladas/ entrosadas. É através desta junção que se cumpre com a simplificação mesmo estando na presença de um determinado grau de (boa) complexidade.

**Priorização:** Os riscos mudam continuamente à medida que as ambições digitais aumentam pelo que se deve usar os dados e informação para uma monitorização contínua.

**Perceção:** Não se pode proteger o que não se vê, pelo que se devem eliminar os ângulos cegos nos relacionamentos internos e externos da organização.

05

# O caminho a seguir

## Cinco ações para evoluir na maturidade de cibersegurança

| | | |
|---|---|---|
| 1 | Redefinir a sua estratégia de Cibersegurança | Permitir que as organizações definam a estratégia para a cibersegurança tendo por base um alinhamento estreito com o negócio. |
| 2 | Repensar o orçamento de Cibersegurança | Elaborar o orçamento de Cibersegurança com base na quantificação da diminuição do risco demonstrando assim o valor dos investimentos nesta área. |
| 3 | Nivelar o "campo de jogo" com os atacantes | Priorizar as iniciativas com base na implementação de novas tecnologias/ modelos de segurança (e.g. *Cloud, Zero Trust*). |
| 4 | Construir resiliência para cada cenário | Preparar medidas de gestão e respetiva orquestração pelas áreas envolvidas na continuidade de negócio, *disaster recovery* e gestão de crises. |
| 5 | Construir uma equipa à prova do futuro | Aumentar as competências em cibersegurança através de formação (*upskilling*), atração de talento ou contratação de *Managed Services*. |

# Fatores críticos de sucesso

## Qualquer estratégia deverá incluir os seguintes pilares

### Pessoas

- Melhorar o conjunto de competências de segurança (internas ou externas);
- Uma equipa de cibersegurança a colaborar mais com o negócio na obtenção de resultados comerciais;
- Maior alinhamento e influência do CISO sobre a estratégia através de interações com outros quadros executivos.

### Capacidades e processos

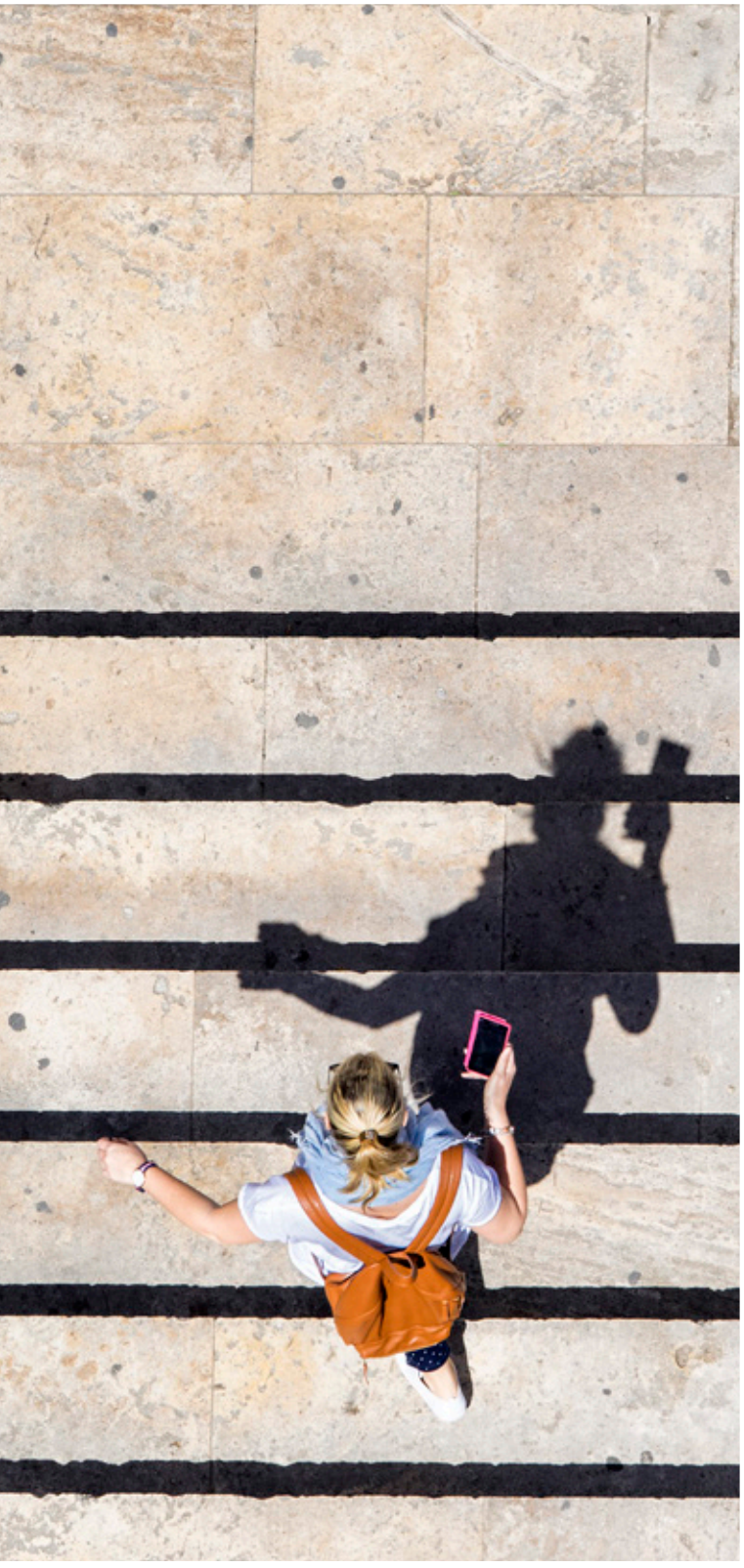
- Incorporar iniciativas empresariais de segurança e privacidade;
- Modelo de governação da informação para toda a empresa;
- Quantificar melhor os riscos cibernéticos;
- Unificar os relatórios em toda a Organização sobre riscos cibernéticos;
- Ligar investimentos e despesas de cibersegurança a métricas ou resultados empresariais tangíveis;
- Passar do planeamento
- da continuidade do negócio para a resiliência cibernética.

### Tecnologia

- Investir em tecnologias avançadas para as capacidades de defesa cibernética e de identificação de segurança da minha Organização;
- Reduzir o custo das operações cibernéticas através da automatização, racionalização e/ou outras soluções.

### Automação

- Investir em tecnologias
- de Monitorização em tempo real da eficácia dos controlos
- de segurança;
- Descoberta, gestão e governação de dados mais modernos;
- Acelerar a adoção de soluções
- *Cloud*;
- Aplicar inteligência artificial na defesa cibernética.



# Contactos


**Miguel Dias Fernandes**
Consulting Partner da PwC em Portugal, Cabo Verde e Angola
+351 965 354 475
miguel.dias.fernandes@pwc.com

**Jorge Sacadura Costa**
Consulting Senior Manager da PwC em Portugal, Cabo Verde e Angola
+351 914 142 752
jorge.sacadura.costa@pwc.com

**João Rui Baptista**
Knowledge Management Senior Manager da PwC em Portugal, Cabo Verde e Angola
+351 912 292 385
joao.rui.baptista@pwc.com

**Pedro Palha**
Clients & Markets Senior Manager da PwC em Portugal, Cabo Verde e Angola
+351 915 189 486
pedro.santos.palha@pwc.com

**Lisboa**
Palácio Sottomayor
Avenida Fontes Pereira de Melo, n.º 16
1050-121 Lisboa

Tel. (+351) 213 599 000
Fax. (+351) 231 599 999

**Porto**
Porto Office Park
Avenida de Sidónio Pais, 153
4100-467 Porto

Tel. (+351) 225 433 000
Fax. (+351) 225 433 499

**Cidade da Praia**
Edifício BAI Center, Piso 2 Direito
Avenida Cidade de Lisboa
C.P. 303 Cidade da Praia
República de Cabo Verde

Tel. (+238) 261 5934
Fax. (+238) 261 6028

**Luanda**
Edifício Presidente
Largo 17 de Setembro n.º 3
1º andar – Sala 137
Luanda – República de Angola

Tel. (+244) 227 286 109
Fax. (+244) 222 311 213

pwc

Siga-nos