CNCS
Centro Nacional de Cibersegurança PORTUGAL

RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

RISCOS & CONFLITOS

3ª EDIÇÃO

JUNHO DE 2022

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

Observatório de Cibersegurança

ÍNDICE

03 **A. Sumário Executivo**
04 1. Análise Global
10 2. Destaques
15 **B. Introdução**
17 **C. Incidentes e Cibercrime**
18 Incidentes
18 Atividade do CERT.PT
32 Incidentes registados pelos membros da RNCSIRT
35 Notificações à CNPD sobre violações de dados pessoais
39 Cibercrime
39 Registos da cibercriminalidade em Portugal (DGPJ)
47 Denúncias ao Gabinete Cibercrime da PGR
51 Linha Internet Segura
55 Síntese do capítulo Incidentes e Cibercrime, em 2021
57 **D. Ameaças e Tendências**
58 Ameaças
58 Perceção de risco - resultados de inquérito a comunidade CNCS
63 Agentes de ameaça relevantes para o ciberespaço de interesse nacional
69 Tendências
69 Ameaças internacionais com potencial de impacto em Portugal
74 Prospetivas para o ciberespaço de interesse nacional em 2022/2023
76 Síntese do capítulo Ameaças e Tendências, em 2021
77 **E. Briefing da Estratégia Nacional de Segurança do Ciberespaço**
79 **F. Recomendações e Recursos**
81 **G. Notas Conclusivas**
83 **H. Notas Metodológicas**
84 **I. Entidades Parceiras**
85 **J. Observatório de Cibersegurança do CNCS**
86 **K. Termos, Abreviaturas e Siglas**
93 **L. Referências Principais**
98 **Anexo – Linhas de Ação da ENSC – Riscos e Conflitos 2022**

A. SUMÁRIO EXECUTIVO

A edição de 2022 do *Relatório Cibersegurança em Portugal - Riscos e Conflitos* analisa os principais incidentes de cibersegurança e indicadores de cibercrime, bem como os agentes de ameaça, no ciberespaço de interesse nacional e as grandes tendências nacionais e internacionais. Esta análise reporta sobretudo ao ano anterior, mas tem em consideração os acontecimentos mais importantes do ano presente e as tendências para o futuro.

O documento divide-se em dois grandes capítulos: no primeiro, apresentam-se os dados sobre os incidentes de cibersegurança e os indicadores de cibercrimes ocorridos em 2021 no ciberespaço de interesse nacional; e, no segundo, conjetura-se acerca dos principais agentes de ameaça e tendências que se destacam a partir dos dados apresentados e dos contributos dos vários parceiros. Pretende-se deste modo construir uma visão integrada que caracterize da forma mais rigorosa possível as principais ameaças ao ciberespaço de interesse nacional.

As conclusões que resultam deste estudo apontam para a persistência de algumas ameaças próprias do contexto de pandemia, como as ligadas à instrumentalização das fragilidades do fator humano, mas também o reforço de outras que têm grande capacidade de impacto, como o *ransomware* ou a exploração de vulnerabilidades. O número de incidentes e de cibercrimes continua a aumentar, não se vislumbrando o regresso a níveis pré-pandemia em grande parte dos casos. Perspetiva-se ainda o emergir da influência do contexto geopolítico e estratégico internacional nas dinâmicas do ciberespaço em manifestações de natureza híbrida, bem como a mitigação progressiva da pandemia enquanto tema dominante nesta matéria.

1. ANÁLISE GLOBAL

Uma análise global dos resultados do presente documento permite uma leitura integrada, sintética e mais concisa da informação disponibilizada. Com esta perspetiva, de seguida destacam-se, no âmbito do ciberespaço de interesse nacional, as ameaças, a perceção de risco, as grandes tendências, o contexto internacional e a relação dos indicadores apresentados com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC).

AMEAÇAS

Mantém-se a tendência de aumento do volume de incidentes de cibersegurança e de cibercrimes no ciberespaço de interesse nacional em 2021 e 2022.

Em 2021, a tendência de crescimento no volume de incidentes e de cibercrimes manteve-se. Confirma-se, portanto, o não retorno aos níveis verificados antes da pandemia da Covid-19, ainda que a variação em relação ao ano anterior em alguns casos seja menor do que em 2020. No âmbito da cibercriminalidade, esta tendência não se verifica sempre no crime estritamente informático (do âmbito da Lei do Cibercrime), uma vez que ocorre um decréscimo no registo deste tipo de crime pelas autoridades policiais, ao contrário de crimes que utilizam a esfera digital de modo instrumental, como a burla informática, a qual continua a ser cada vez mais frequente.

As ciberameaças dominantes em Portugal durante o ano de 2021 foram o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla *online*, o comprometimento de contas ou tentativa e a exploração de vulnerabilidades.

Durante o ano de 2021, destacaram-se como ciberameaças particularmente relevantes as ações que utilizam a engenharia social para a captura de informação, como o *phishing* (através de *email*), o *smishing* (SMS) e o *vishing* (telefone). A fraude e a burla *online* também tiveram relevância no âmbito das técnicas de manipulação do fator humano. Em menor volume, mas com bastante impacto, verifica-se o aumento dos casos, e da sua relevância, de *ransomware*, de comprometimento de contas e de exploração de vulnerabilidades (esta última com grande presença a nível internacional).

Os agentes de ameaça mais relevantes no ciberespaço de interesse nacional em 2021 com tendência de persistência em 2022 foram os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas.

O ano de 2021 foi marcado pela atividade de cibercriminosos razoavelmente organizados que procuraram ganhos financeiros através do *phishing/smishing/vishing*, de *ransomware* e de fraudes/burlas *online*. Os atores estatais (e algumas ameaças persistentes avançadas) também tiveram uma atividade relevante no ciberespaço de interesse nacional, visando objetivos geopolíticos e estratégicos, através de ataques de *phishing* e *spear phishing*, do comprometimento de contas, bem como da exploração de vulnerabilidades para a realização de intrusões.

Com menos relevância, mas a merecer menção, persiste a ameaça interna negligente, que diz respeito aos colaboradores que inadvertidamente comprometem a sua organização, clicando num *link* malicioso de um *phishing*, por exemplo. É de referir ainda os *cyber-offenders*, os quais se caracterizam por realizar ações que visam apenas perturbar as suas vítimas ou criar disrupções, mediante, por exemplo, assédio ou destruição de informação. Por fim, também se registaram algumas ações de hacktivistas, os quais procuraram realizar afirmações ideológicas no ciberespaço, através, por exemplo, de *defacements*. A intensidade da atividade dos hacktivistas é muito variável e sujeita ao ciclo de vida de cada novo grupo.

O quadro que se segue apresenta uma panorâmica sobre as principais ameaças a afetar o ciberespaço de interesse nacional em 2021, com alguma persistência em 2022, considerando a articulação entre ciberameaças e agentes de ameaça, bem como os diferentes níveis de importância de cada um.[1]

Quadro de Ameaças: Ciberameaças/Agentes de ameaças em Portugal, 2021/2022

	Cibercriminosos	Atores estatais	Ameaça interna negligente	Cyber-offenders	Hacktivistas
Phishing/Smishing/Vishing					
Ransomware					
Fraude/Burla *online*					
Comprometimento de contas ou tentativa					
Vulnerabilidades e sua exploração					
Engenharia social (vários)					
Distribuição de *malware*					
Furto de identidade					
Sextortion					

Agentes de ameaça e ciberameaças com relevância alta em Portugal durante 2021/2022.

Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2021/2022.

Ciberameaça com frequência alta como prática dos agentes de ameaça em causa em Portugal.

Ciberameaça com frequência média como prática dos agentes de ameaça em causa em Portugal.

Ciberameaça com frequência baixa ou inexistente como prática dos agentes de ameaça em causa em Portugal.

Quadro 1 | CNCS (a partir de ENISA)

1 Este quadro resulta dos dados e dos contributos dos parceiros deste Relatório, com base na redundância entre fontes e no potencial impacto dos casos reportados (para mais detalhe, consultar Nota Metodológica).

A figura 1 apresenta uma cronologia de eventos com potencial de impacto elevado a nível internacional e nacional, tendo em conta o volume de sistemas e pessoas afetados, bem como a projeção mediática, a qual implica um certo alarme social. Nesta matéria, o ano de 2021 foi marcado por casos ligados à identificação de vulnerabilidades em produtos e serviços de uso massificado, conduzindo à sua exploração por agentes maliciosos - numa primeira fase, enquanto essas vulnerabilidades não são descobertas (*zero-day*) e, numa segunda fase, após o conhecimento dessas vulnerabilidades, direcionando a exploração para todos os sistemas que não realizaram ainda as devidas atualizações com correções de segurança (casos Microsoft Exchange, Proxyshell, Apache Log4j). No início de 2021, a violação de dados relacionada com o *software* NitroPDF também se revelou de alguma importância.

No primeiro trimestre de 2022, vários casos com potencial de impacto elevado afetaram o ciberespaço de interesse nacional do ponto de vista mediático e em termos de efeitos em serviços e pessoas. Destacaram-se os ataques ao grupo de *media* Impresa, pelo efeito mediático e pela importância dos dados comprometidos, bem como à Vodafone, sobretudo pelos serviços afetados. Em ambos os casos, assistiu-se a uma destruição de dados que comprometeu a disponibilidade da informação e de serviços.

Cronologia de eventos com potencial de impacto elevado em Portugal, 2021 e 1º tri. de 2022

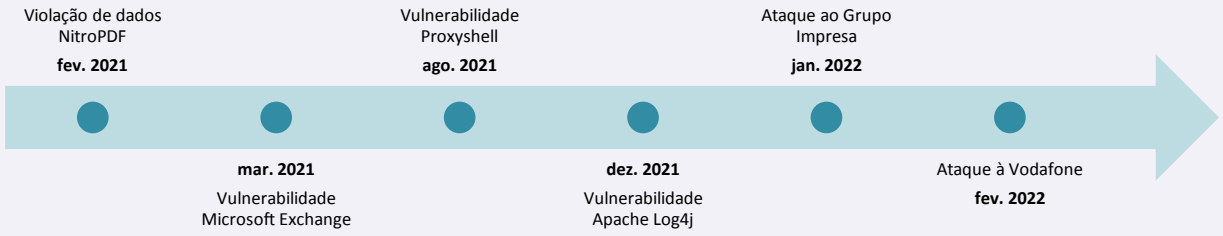


Figura 1 | CNCS

PERCEÇÃO DE RISCO E TENDÊNCIAS

A perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança aumentou em 2021.

De acordo com o inquérito realizado pelo Observatório de Cibersegurança à comunidade de entidades com protocolo de colaboração com o CNCS, a perceção de risco relativamente à segurança do ciberespaço de interesse nacional agravou-se entre os pontos de contacto destas entidades. Comparando com o ano

anterior, a pandemia teve menos influência neste resultado. Não obstante, uma parte importante dos inquiridos pensa que o ciberespaço está mais capacitado do que no ano anterior.

Em 2021, verificaram-se como tendências internacionais com potencial de impacto no ciberespaço de interesse nacional o incremento de ameaças híbridas, os ataques a cadeias de fornecimento, a exploração de vulnerabilidades e a proliferação de *ransomware*.

O ciberespaço de interesse nacional encontra-se bastante exposto às tendências internacionais, nomeadamente devido às características do país, mas também à estrutura do ciberespaço, naturalmente um domínio sem fronteiras claras. A nível internacional, verificou-se um conjunto de ameaças que direta ou indiretamente têm consequências no país: as ameaças híbridas indiciam a ação de atores estatais, os ataques a cadeias de fornecimento e a exploração de vulnerabilidades comprometem produtos e serviços usados em Portugal, e o *ransomware* é reconhecido por grande parte das fontes como estando cada vez mais presente no país.

Para 2022 e 2023 são identificadas como principais tendências em Portugal a propensão para uma maior intervenção de atores estatais, a persistência do uso das fragilidades do fator humano, ataques de *ransomware*, violações de dados relativas a credenciais de acesso, exploração de vulnerabilidades e as tecnologias móveis a serem cada vez mais utilizadas como superfícies de ataque.

As tendências nacionais para o futuro articulam-se com as tendências internacionais que têm continuidade em relação a 2021, mas também com as que emergem no início de 2022, como sejam as que resultam do conflito na Ucrânia ou da recorrência de ataques com impacto no país advindos de agentes de ameaça internacionais de caracterização ambígua. Se, por um lado, o contexto de guerra pode incentivar as ações de atores estatais, por outro, as fragilidades do fator humano no uso, por exemplo, de um *smartphone* podem ser portas de entrada para grupos que se confundem na motivação entre os ganhos financeiros, o niilismo político e o vandalismo informático.

CONTEXTO INTERNACIONAL ATUAL

O contexto internacional atual, muito marcado pelo conflito na Ucrânia, vem substituir a pandemia enquanto temática que cria dinâmicas de escala no ciberespaço de interesse nacional. Se a pandemia criou condições de contexto para ataques de cibercriminosos com vista à captura de dados sensíveis, realização de burlas e práticas de extorsão, o contexto de perturbação geopolítica e estratégica atual apresenta-se como particularmente propenso a ações

de atores estatais ou paraestatais com objetivos ligados à ciberespionagem ou à sabotagem, tendo como alvos a Administração Pública, os Órgãos de Soberania, as infraestruturas críticas e os operadores de serviços essenciais. Os ataques advindos de hacktivistas também podem emergir neste contexto, nomeadamente ataques de negação de serviço distribuída (DDoS) e *defacements*.

Cenários de ameaças próprias de contextos emergentes e/ou permanentes

Cenário 1 - Ameaças típicas do contexto pandémico	**Cenário 2 - Ameaças típicas do contexto geopolítico e estratégico atual**
Agentes de ameaça emergentes neste cenário: cibercriminosos com objetivos económicos.	Agentes de ameaça emergentes neste cenário: atores estatais e paraestatais com objetivos geopolíticos e estratégicos (e ameaças persistentes avançadas); hacktivistas com objetivos ideológicos.
Tipologias de ações hostis emergentes neste cenário*: _ burlas *online*; _ comprometimento de sistemas próprios do trabalho remoto; _ desinformação sobre saúde; _ *phishing* massificado; _ *ransomware.*	Tipologias de ações hostis emergentes neste cenário: _ ciberespionagem; _ comprometimento de cadeias de fornecimento; _ comprometimento de contas; _ comprometimento de sistemas próprios do trabalho remoto; _ DDoS; _ *defacements*; _ desinformação sobre o conflito na Ucrânia; _ exploração de vulnerabilidades; _ intrusões; _ *phishing* e *spear phishing;* _ *ransomware* e/ou sabotagem.
Temas e setores alvo: Banca, Saúde, Serviços de *streaming*, serviços postais e de transporte.	Temas e setores alvo: operadores de serviços essenciais, Administração Pública e Órgãos de Soberania.
Cenário 0 - Contexto permanente: a materialização dos cenários 1 e 2 não obsta a que exista uma dinâmica permanente própria das ameaças ao ciberespaço de interesse nacional para lá da pandemia ou do contexto internacional atual, âmbito no qual certos incidente e cibercrimes tendem a ocorrer.	

*Nem todas as ações hostis consideradas relevantes são consequência sempre e necessariamente dos agentes de ameaça emergentes no cenário em causa, embora tendencialmente sim.

Quadro 2 | CNCS

Embora o nível de incerteza relativamente a esta matéria seja elevado, é provável que os aspetos decorrentes do cenário 2 ainda convivam com os que são próprios do cenário 1, os quais, independentemente da persistência da pandemia, terão tendência para se manter, na medida em que muitos casos representam uma conversão da criminalidade a novos modos de operar. Além disso, existe a constância do cenário 0, o qual corresponde à habitual atividade maliciosa no ciberespaço de interesse nacional para lá dos acontecimentos excecionais da pandemia e do contexto geopolítico e estratégico atual. Eventualmente, a importância da descoberta e exploração de vulnerabilidades, tão relevante em 2021, enquadra-se num dos cenários traçados ou, simultaneamente, em todos eles.[2]

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Relativamente ao acompanhamento da ENSC, a linha de observação sobre Riscos e Conflitos do Observatório de Cibersegurança permite relevar duas dimensões: por um lado, este documento resulta de um tipo de dinâmica particularmente incentivado pela ENSC, isto é, da cooperação entre entidades na partilha de informação sobre ameaças; por outro, expõe os efetivos incidentes, cibercrimes e ameaças ao ciberespaço de interesse nacional, monitorizando, portanto, indicadores fundamentais de cibersegurança. Do ponto de vista da promoção da cooperação entre entidades na partilha de informação sobre ameaças, este Relatório é em si um indicador positivo. Quanto a um dos objetivos últimos da ENSC, em termos de efeitos, que será manter o ciberespaço seguro, não se pode ignorar o facto de o volume de incidentes e cibercrimes manter uma tendência crescente e isso representar um desafio para as linhas de ação da ENSC, nomeadamente para os eixos 3 (Proteção do ciberespaço e das infraestruturas) e 4 (Resposta às ameaças e combate ao cibercrime).

2 O CNCS elaborou um documento onde identificou um conjunto de potenciais ameaças no contexto atual e respetivas boas práticas para a sua mitigação. Este conteúdo mais detalhado pode ser visitado na página do CNCS, em “Conhecimento Situacional”, com o título “Contexto Atual”.

2. DESTAQUES

Incidentes e Cibercrime

O CERT.PT registou um aumento de 26% no número de incidentes de cibersegurança em 2021 comparando com 2020 (CERT.PT).

Os setores mais afetados pelos incidentes registados pelo CERT.PT em 2021 foram a Banca (13% dos incidentes), as Infraestruturas Digitais (8%) e os Prestadores de Serviços de Internet (6%) (CERT.PT).

O *phishing/smishing* (40% dos incidentes), a engenharia social (14%) e a distribuição de *malware* (13%) foram os tipos de incidentes mais registado pelo CERT.PT em 2021 (CERT.PT).

As marcas mais simuladas nos ataques de *phishing/smishing* em 2021 são do âmbito da Banca (48% dos casos), dos Transportes e Logística (21%) e das Plataformas de Emails (19%) (CERT.PT).

Os tipos de incidentes mais registado pelos membros da RNCSIRT em 2021 foram a tentativa de *login* (16% dos incidentes), a exploração de vulnerabilidades (9%) e o *scanning* (8%) (RNCSIRT).

Em 2021, verificou-se um aumento de 6% no número de notificações de violações de dados pessoais reportadas à CNPD face ao ano anterior (CNPD).

Incidentes e Cibercrime

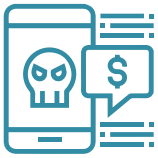
Os setores e atividades com mais notificações à CNPD em 2021 são o Comércio e Serviços (25% das notificações), a Banca (13%) e a Administração Local (8%) (CNPD).

Entre as notificações enviadas à CNPD em 2021, a origem mais frequente para os incidentes em causa é a falha humana (24% das notificações), o *ransomware* (22%) e as ações fraudulentas (13%). O princípio da informação mais comprometido é o da confidencialidade (62%) (CNPD).

O número de crimes relacionados com a informática registados pelas autoridades policiais cresceu 6% em 2021 face ao ano anterior, embora o número de crimes estritamente informáticos tenha decrescido 11% (DGPJ).

A percentagem de crimes relacionados com a informática em relação ao total de crimes registados em Portugal cresceu 0,4 pp, de 7,4% em 2020 para 7,8% em 2021 (DGPJ).

A burla informática/comunicações é o crime relacionado com a informática com mais registos em 2021 (91% do total), seguida do acesso/interceção ilegítimos (com 3%) - o crime estritamente informático com mais registos em 2021 (DGPJ).



A burla informática/comunicações é o tipo de crime relacionado com a informática com mais condenados em 2020 (75% dos casos), seguido da falsidade informática (13%) (DGPJ).

Incidentes e Cibercrime

Verifica-se um decréscimo no número de condenados em crimes relacionados com a informática (menos 44%) e de arguidos (menos 36%) em 2020 face a 2019 (DGPJ).

O número de denúncias ao Gabinete Cibercrime da PGR continua a aumentar com uma subida para mais do dobro em 2021 (113%) (PGR).

Em 2021, o *phishing* e variados tipos de burla *online* continuam a ser os tipos de criminalidade mais denunciados ao Gabinete Cibercrime da PGR (PGR).

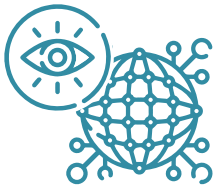
Verifica-se uma subida de 40% no número de processos de atendimento e apoio registados pela Linha Internet Segura em 2021 face ao ano anterior (APAV).

A *sextortion* (30% dos casos), a burla (12%) e o furto de identidade (8%) foram os crimes e outras formas de violência mais registados na dimensão Helpline da Linha Internet Segura em 2021 (APAV).

Ameaças e Tendências

A perceção de risco de alguma entidade sofrer um incidente de cibersegurança aumentou em 2021 para 98% dos inquiridos no inquérito anual à comunidade de entidades com protocolo com o CNCS - mais 4 pp do que em 2020 (CNCS).

Apesar do incremento da perceção de risco, uma grande parte dos inquiridos (48%) julga que o ciberespaço de interesse nacional está mais capacitado em 2021 (CNCS).



O *phishing*, o *ransomware* e a engenharia social são os tipos de ciberameaças percecionados como os mais relevantes em 2021 pelos inquiridos, com particular subida do *ransomware* (CNCS).

No âmbito deste mesmo inquérito, os agentes de ameaça percecionados como os mais relevantes em 2021 e 2022 são os cibercriminosos, os hacktivistas e os atores estatais (CNCS).

Considerando o conjunto de dados do presente Relatório, os tipos de ciberameaças efetivamente mais relevantes em Portugal em 2021 são o *phishing/smishing/vishing*, o *ransomware*, a fraude/burla online, o comprometimento de contas ou tentativa e a exploração de vulnerabilidades (CNCS).

Ameaças e Tendências

O tipo de agentes de ameaça efetivamente mais relevantes em Portugal em 2021, com base nas várias fontes deste Relatório, são sobretudo os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas (CNCS).

A nível internacional, durante 2021, destacam-se como tendências com potencial impacto em Portugal o incremento das ameaças híbridas, a persistência de ataques às cadeias de fornecimento, a descoberta de vulnerabilidades relevantes e posterior exploração, a proliferação de ataques de *ransomware* e a tentativa de resposta comum ao nível dos Estados (CNCS).

A tendência de aumento no volume de incidentes e de indicadores de cibercrime em 2021 não é apenas nacional, mas também internacional (ENISA, Europol e WEF).

Identificam-se as seguintes prospetivas para o ciberespaço de interesse nacional em 2022 e 2023: contexto internacional propenso à ação de atores estatais; persistência da exploração das fragilidades do fator humano; casos de *ransomware*; violações de dados para uso de credenciais de acesso; exploração de vulnerabilidades; e relevância das tecnologias móveis e da Internet das Coisas como potenciais superfícies de ataque (CNCS).

B. INTRODUÇÃO

A cibersegurança conquistou nos últimos anos uma presença no espaço mediático que resulta em parte de alguns incidentes de cibersegurança com impacto relevante no normal funcionamento da sociedade. O contexto de pandemia também mostrou a importância de a transição digital (acelerada neste contexto) ser acompanhada por garantias de segurança no ciberespaço. Por isso, uma análise às principais ameaças ao ciberespaço de interesse nacional é cada vez mais importante.

Os Relatórios do tema *Riscos e Conflitos* do Observatório de Cibersegurança do CNCS têm procurado estabelecer uma articulação entre os incidentes e cibercrimes verificados e os contextos nacional e internacional que ajudam a explicá-los. Esta terceira edição não é exceção. Se as duas primeiras edições deste documento procuraram estabelecer uma articulação com o contexto de pandemia, a edição atual surge num momento de desafios importantes à estabilidade geopolítica. Além disso, este documento é lançado imediatamente após a ocorrência de incidentes relevantes no ciberespaço de interesse nacional. Por isso, esta análise, apesar de reportar a 2021, acompanha os acontecimentos de 2022, sobretudo porque alguns aspetos são transversais aos dois anos, mas também porque se pretende identificar tendências que se projetam no futuro.

O presente Relatório divide-se em dois capítulos principais: o primeiro – Incidentes e Cibercrime – concentra-se na apresentação dos dados disponíveis relativos a incidentes de cibersegurança e indicadores de cibercrime no ciberespaço de interesse nacional; o segundo – Ameaças e Tendências – desenvolve uma análise sobre os possíveis agentes de ameaça e sobre as principais tendências do presente e do futuro em matéria da cibersegurança nacional.

Após o desenvolvimento destes capítulos, efetua-se uma análise relativamente à ENSC e a hipotéticos impactos da mesma

à luz do trabalho e dos resultados deste documento, seguindo-se um conjunto de recomendações e recursos do CNCS e a nota metodológica, entre outros tópicos. Em anexo é possível encontrar a identificação das linhas de ação da ENSC consideradas neste documento.

C. — INCIDENTES E CIBERCRIME

Os dados sobre os incidentes e cibercrimes são essenciais para se alcançar uma panorâmica sobre a evolução e as tendências relativamente à cibersegurança no ciberespaço de interesse nacional. Este capítulo é dedicado à apresentação e análise dos números disponíveis a este respeito, dividindo-se numa parte dedicada aos incidentes no ciberespaço de interesse nacional e outra respeitante aos indicadores de cibercrime registados por várias entidades.

INCIDENTES

No âmbito dos incidentes no ciberespaço de interesse nacional disponibilizam-se dados de três fontes: da Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), da Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática (RNCSIRTs) e da Comissão Nacional de Proteção de Dados (CNPD), permitindo-se assim uma visão consideravelmente abrangente do ciberespaço em Portugal no que ao registo de incidentes diz respeito.

ATIVIDADE DO CERT.PT

O CERT.PT, que funciona no CNCS, integra na sua missão a gestão da resposta a incidentes no ciberespaço de interesse nacional, com particular foco nas entidades designadas no âmbito da aplicação do Regime Jurídico da Segurança do Ciberespaço, estabelecido na Lei n.º 46/2018, de 13 de agosto, nomeadamente a Administração Pública, os operadores de infraestruturas críticas, os operadores de serviços essenciais e os prestadores de serviços digitais. De seguida, apresentam-se os incidentes e observáveis registados por esta entidade ao longo do ano e em comparação com anos anteriores. Pelas suas características de espectro nacional, estes dados, não abrangendo todos os incidentes que eventualmente ocorreram no país, são um indicador importante para identificar tendências e predomínios.

1. Incidentes de cibersegurança registados pelo CERT.PT

A tendência de subida do número de incidentes registados pelo CERT.PT desde 2015 mantém-se, verificando-se um crescimento de 26% em 2021 face ao ano anterior, a que corresponde o registo de 1418 incidentes em 2020 e 1781 em

2021. No entanto, esta variação percentual é similar à ocorrida em 2019, depois de em 2020 se ter verificado uma subida muito acentuada, coincidindo esta tendência com o início da pandemia da Covid-19. Este regresso a níveis de variação anteriores à pandemia ocorre cumulativamente em relação à variação entre 2019 e 2020, não significando, portanto, um regresso ao número de incidentes absolutos registados antes da pandemia. Verifica-se também que o último trimestre do ano e o segundo semestre continuam a ser os períodos, comparativamente, com mais incidentes registados, tal como no ano anterior. Novembro, por sua vez, foi o mês com mais incidentes registados.

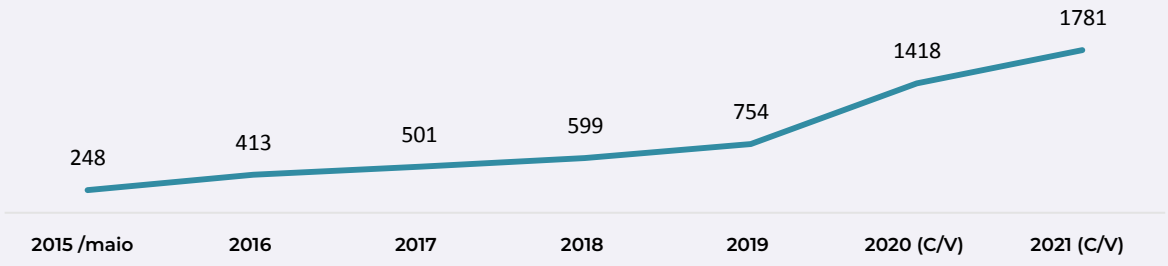
Incidentes registados pelo CERT.PT, entre 2015 e 2021, e mês, trimestre e semestre com mais registos

	Total	Tend. %	Mês c/mais	Trimestre c/mais	Semestre c/mais
2015 (desde maio)	248	N/A	out. (42)	N/A	N/A
2016	413	N/A	fev. (56)	1º (135)	1º (243)
2017	501	+21	mar. (57)	4º (143)	2º (255)
2018	599	+20	out. (68)	2º (169)	1º (301)
2019	754	+26	set. (79)	3º (213)	2º (412)
2020*	1347 (S/V) 1418 (C/V)	+79 (S/V) +88 (C/V)	abr. (150/145)	4º (418/407)	2º (729/697)
2021	1781 (C/V)	+26 (C/V)	nov. (222)	4º (497)	2º (934)

* Devido ao facto de a taxonomia utilizada pelo CERT.PT ter sofrido ligeiras alterações em 2020 (RNCSIRT, 2020), nomeadamente passando a integrar as vulnerabilidades como incidentes, para efeitos de comparação entre percentagens, optou-se por apresentar dois dados - C/V: com vulnerabilidades; e S/V: sem vulnerabilidades. Os dados anteriores a 2020 não incluem vulnerabilidades (S/V).

Tabela 1 | CERT.PT

Número de incidentes registados pelo CERT.PT, entre 2015 e 2021*



* C/V: contabilizando as vulnerabilidades como incidentes (a partir de 2020).

Figura 2 | CERT.PT

Na comparação entre os últimos 3 anos, de modo a incluir pelo menos um ano anterior à pandemia da Covid-19, verifica-se, na figura 3, que no ano de 2021 se acentua o maior número de incidentes verificados a partir de 2020, mas com diferenças relativamente aos meses com mais incidentes registados. Enquanto no ano de 2020 os meses com mais incidentes foram abril (150) e outubro (146), em 2021 foram fevereiro (190) e novembro (222). De referir que o mês de abril de 2020 e o mês de fevereiro de 2021 coincidem com os meses de maior confinamento social verificados em Portugal fruto da pandemia da Covid-19 (ver CNCS, 2021).

Número de incidentes registados pelo CERT.PT, 2019, 2020 e 2021 – por mês*

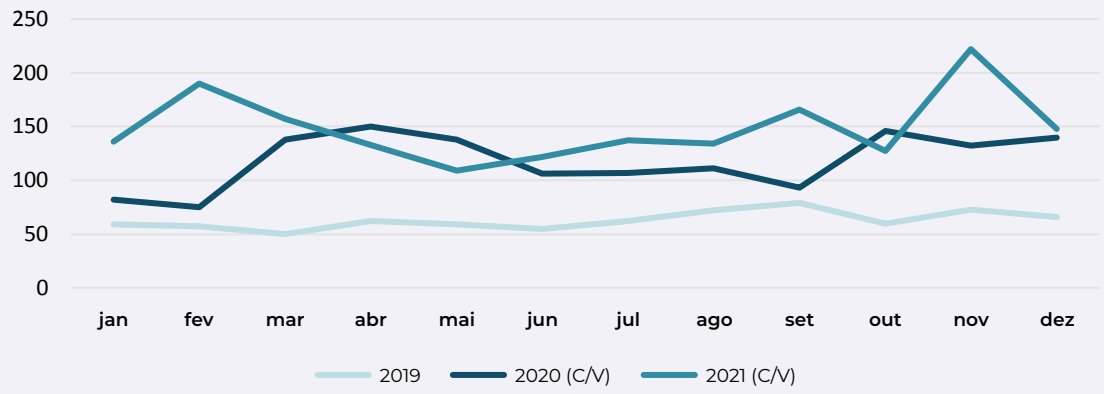


Figura 3 | CERT.PT

Enquanto em 2020 houve 5170 notificações externas por parte da comunidade ao CNCS para 1418 incidentes efetivamente registados, em 2021 houve 4988 notificações externas para 1781 incidentes. Portanto, em média, durante 2021 registaram-se mais incidentes por cada notificação externa do que em 2020, com 0,4 incidentes por cada notificação externa, quando no ano anterior foram 0,3. Apesar do número de incidentes ter aumentado, o número de notificações externas diminuiu 4%. Nem todos os incidentes registados resultam de notificações externas, mas quanto maior o número de incidentes por cada notificação externa, maior eficácia, em geral, revelam as denúncias da comunidade.

Incidentes e notificações externas registados pelo CERT.PT, 2020 e 2021

	Incidentes	Notificações externas	Tend. Not. Ext. %	Incidentes p/notificações
2020	1418	5170	N/A	0,3
2021	1781	4988	-4	0,4

Tabela 2 | CERT.PT

Durante 2021, em comparação com 2020, assistiu-se a uma variação menor entre meses quanto ao número de incidentes registados pelo CERT.PT por cada notificação externa, mantendo-se os valores entre os 0,3 e os 0,4 incidentes por cada notificação externa, quando no ano anterior a variação ocorreu no intervalo entre 0,1 e 0,5. Quanto menor for esta variação, maior correlação haverá entre o volume de reporte da comunidade e o número de incidentes registados. Saliente-se que os meses com menos incidentes por notificação externa em 2020, os do terceiro trimestre, não são os mesmos de 2021.

Número de incidentes por cada notificação externa registados pelo CERT.PT, 2020 e 2021 – por mês

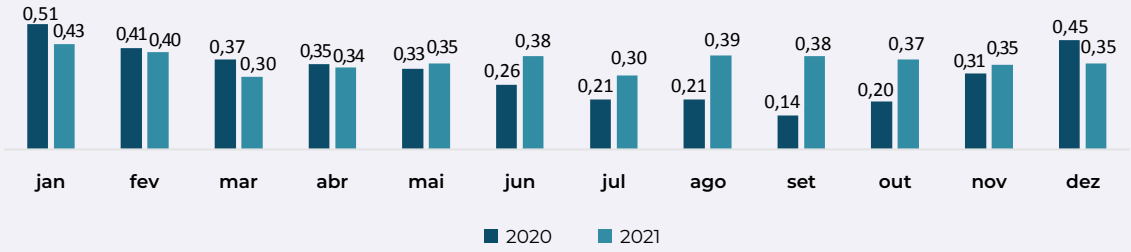


Figura 4 | CERT.PT

A tendência para, aproximadamente, dois terços dos incidentes afetarem entidades privadas e um terço entidades públicas mantém-se em 2021, com 67% dos incidentes registados nas primeiras e 33% nas segundas, verificando-se assim uma variação de 2 pontos percentuais (pp) relativamente ao ano anterior, em que 69% dos incidentes foram registados em entidades privadas e 31% em públicas, como é possível observar na tabela 3.

Incidentes por Entidades Privadas e Entidades Públicas registados pelo CERT.PT, 2020 e 2021

2020			2021		
RK	Comunidade	%	RK	Comunidade	%
1º	Entidades Privadas	69	1º	Entidades Privadas	67
2º	Entidades Públicas	31	2º	Entidades Públicas	33

Tabela 3 | CERT.PT

Ao longo do ano de 2021, a proporção de incidentes registados em entidades públicas e privadas manteve-se relativamente estável, com exceção dos meses de agosto, em que os incidentes em entidades públicas chegaram aos 40%, e novembro,

em que os incidentes em entidades privadas atingiram os 75%, em ambos os casos representando os máximos proporcionais mensais do ano para cada tipo de entidade.

Incidentes por Entidades Privadas e Entidades Públicas registados pelo CERT.PT, 2021 - por mês, percentagem do total

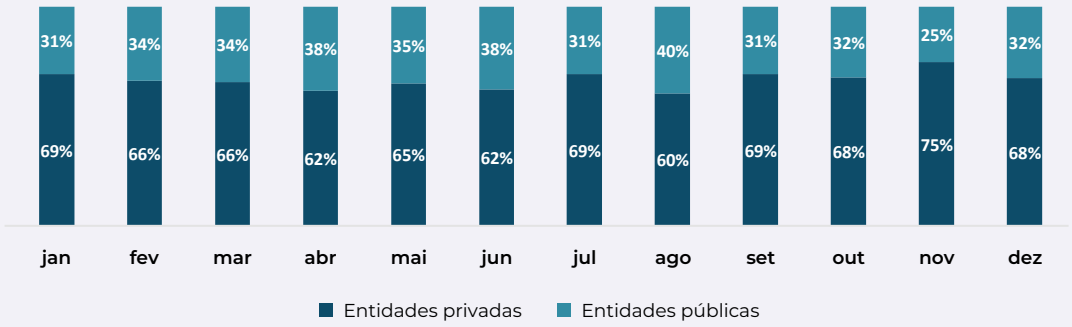


Figura 5 | CERT.PT

A distribuição dos incidentes de cibersegurança pelos setores e áreas governativas continua, tal como em anos anteriores, a colocar um peso maior na Banca, com 13% dos incidentes registados a dizerem respeito a este setor, com uma subida absoluta de 79% relativamente ao ano anterior. Verifica-se ainda um crescimento relevante da área governativa da Presidência do Conselhos de Ministros, que contabiliza todas as instituições sob o domínio desta área, que passou da oitava para a terceira posição, com mais 559% de incidentes. A área da Administração Interna também apresenta uma subida relativa acentuada no número de incidentes, atingindo a sexta posição. As Infraestruturas Digitais e os Prestadores de Serviços Digitais continuam a ter muita relevância, sobretudo por corresponderem à tipologia na qual se registam os utilizadores domésticos e organizacionais não incluídos nos restantes tipos. De referir que na área governativa Educação e Ciência, Tecnologia e Ensino Superior se verifica um decréscimo do número de incidentes (o único domínio em que isso ocorre) e do seu lugar no *ranking*, da quinta para a nona posição.

Incidentes por setor e área governativa registados pelo CERT.PT, 2020 e 2021 - Top 15*

2020				2021				Ordenação	
RK	Setor e Área Governativa[3]	Nº	%	RK	Setor e Área Governativa	Nº	%	Tendência absoluta %	Lugar RK
1º	Outros	626	36	1º	Outros	1220	39	+ 95	=
2º	Banca	229	13	2º	Banca	411	13	+ 79	=
3º	Infraestruturas Digitais	184	11	3º	Presidência do Conselho de Ministros	270	9	+ 559	+
4º	Prestadores de Serviços de Internet	161	9	4º	Infraestruturas Digitais	266	8	+ 45	-
5º	Educação e Ciência, Tecnologia e Ensino Superior	154	9	5º	Prestadores de Serviços de Internet	187	6	+ 16	-
6º	Transportes	79	5	6º	Administração Interna	181	6	+ 1408	+
7º	Administração Local	41	2	7º	Transportes	133	4	+ 68	-
8º	Presidência do Conselho de Ministros	41	2	8º	Administração Local	120	4	+ 193	-
9º	Energia	30	2	9º	Educação, Ciência, Tecnologia e Ensino Superior	109	3	- 29	-
10º	Saúde	29	2	10º	Saúde	63	2	+ 117	=
11º	Administração Regional	20	1	11º	Energia	31	1	+ 3	-
12º	Defesa Nacional	19	1	12º	Cultura e Turismo	26	1	+ 53	+
13º	Cultura e Turismo	17	1	13º	Finanças	20	1	+ 122	+
14º	Trabalho, Solidariedade e Segurança Social	17	1	14º	Defesa Nacional	19	1	=	-
15º	Negócios Estrangeiros	12	1	15º	Negócios Estrangeiros	18	1	+ 50	=

* O total de incidentes por setor e área governativa é ligeiramente superior ao nº total de incidentes devido ao facto de em alguns casos um incidente poder ser contabilizado simultaneamente em mais do que um setor e área governativa. Acresce que este ano o número de setores e áreas governativas considerados aumentou, de 25 em 2020 para 28 em 2021. As áreas governativas identificadas dizem respeito a todas as entidades sob o domínio administrativo das mesmas.

Tabela 4 | CERT.PT

2. Tipos de incidentes de cibersegurança registados pelo CERT.PT

Em 2021, o *phishing/smishing* continua a ser o tipo de incidente de cibersegurança mais registado pelo CERT.PT, tal como no ano anterior, representando 40% do total de incidentes e um aumento de 17% em termos absolutos. De destacar a subida muito acentuada da engenharia social para a segunda posição nos tipos de incidentes mais frequentes, dizendo respeito a 14% do total. A infeção de sistemas por *malware*

3 Esta tipologia obedeceu a uma análise por parte do CERT.PT considerando a pertinência e o uso generalizado, bem como os setores referidos na Lei n.º 46/2018. O Decreto-Lei n.º 65/2021, de 30 de julho, estabelece os requisitos de notificação de incidentes aplicáveis a todos os setores previstos na Lei n.º 46/2018, de 13 de agosto, sem prejuízo de regimes setoriais específicos a definir nos termos do n.º 1 do artigo 18.º do mesmo normativo. Contudo, e apesar desta previsão, os dados apresentados neste Relatório baseiam-se, maioritariamente, no estabelecido no artigo 20 da Lei n.º 46/2018, de 13 de agosto, onde se determina que quaisquer entidades podem notificar, a título voluntário, os incidentes com impacto na continuidade dos serviços por si prestados. Acresce que nem todos os incidentes integrados nos setores e áreas governativas indicados neste Relatório estão no âmbito da referida Lei (mesmo no caso dos setores previstos na Lei), nem se considera que todos os incidentes registados tiveram um impacto relevante nesse mesmo âmbito.

desceu da segunda para a sétima posição, o que corresponde a um decréscimo de 71% relativamente a 2020. A distribuição de *malware* e o comprometimento de conta não privilegiada mantêm os lugares do ano anterior, com a terceira e quarta posições, respetivamente.

Incidentes por tipo registados pelo CERT.PT, 2020 e 2021 – Top 10

2020				2021				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta %	Lugar RK
1º	*Phishing/smishing*	613	43	1º	*Phishing/smishing*	715	40	+ 17	=
2º	Sistema infetado (*malware*)	169	12	2º	Engenharia social	246	14	+ 2136	+
3º	Distribuição de *malware*	119	8	3º	Distribuição de *malware*	226	13	+ 90	=
4º	Comprometimento de conta não privilegiada	111	8	4º	Comprometimento de conta não privilegiada	114	6	+ 2,7	=
5º	Acesso não autorizado	58	4	5º	Utilização Ilegítima de nome de terceiros	80	4	+ 150	+
6º	Comprometimento de aplicação	55	4	6º	Indeterminado (outro)	50	3	+ 79	+
7º	Sistema vulnerável (vulnerabilidade)	41	3	7º	Sistema infetado (*malware*)	46	3	- 73	-
8º	Utilização Ilegítima de nome de terceiros	32	2	8º	Sistema vulnerável (vulnerabilidade)	44	2	+ 7	-
9º	Indeterminado (outro)	28	2	9º	Modificação não autorizada (35 *ransomware*) *	38	2	+ 111	+
10º	Tentativa de *login*	26	2	10º	Exploração de Vulnerabilidade (tent. Intrusão)	37	2	+ 61	+

* 35 incidentes de ransomware: mais 17 do que em 2020, durante o qual se verificou a ocorrência de 18.

Tabela 5 | CERT.PT

Destacando apenas os cinco tipos de incidentes mais frequentes ao longo do ano, verifica-se, de acordo com a figura 6, que os meses com mais incidentes registados, fevereiro e novembro, devem esse aumento em grande medida ao *phishing* e à engenharia social. Entre janeiro e fevereiro, o *phishing* aumentou de 61 para 73 incidentes e a engenharia social de 15 para 39; entre outubro e novembro, o *phishing* registou um aumento de 58 para 101 incidentes e a engenharia social de 18 para 43. Os números do mês de setembro, por sua vez, foram particularmente influenciados pelo aumento do comprometimento de conta não privilegiada, que viu os seus números subirem de 16 registos em agosto para 28 em setembro.

Número de incidentes por tipo registados pelo CERT.PT, 2021 – Top 5, por mês

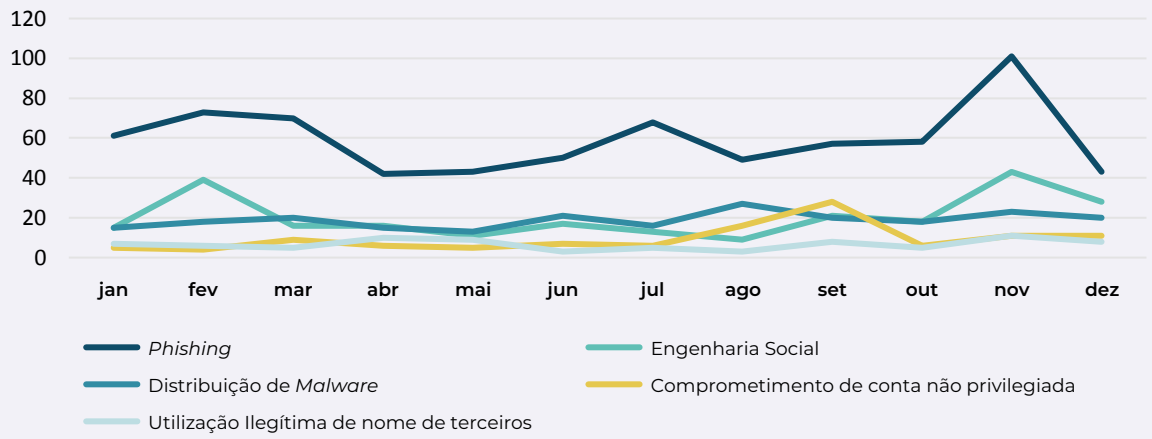


Figura 6 | CERT.PT

A importância dos tipos de incidentes *phishing/smishing* e engenharia social merece uma atenção específica às suas características, nem sempre visíveis numa análise agregada. O *phishing* e o *smishing*, independentemente das plataformas utilizadas para a sua realização, são incidentes através dos quais um agente malicioso simula uma determinada marca/organização, procurando afetar uma vítima com o estatuto de cliente, cidadão ou colaborador, capturando os seus dados e/ou conduzindo-o a instalar *malware*. Através de uma análise a estas simulações, foi possível identificar os tipos de marcas mais utilizadas para estes fins. Sobressaem claramente três tipos: as marcas da Banca, com 48% dos casos; dos Transportes e Logística, com 21%; e do âmbito da captura de credenciais de *email* e outras, com 19%.

Tipos de marca simuladas nos ataques de *phishing/smishing* registados pelo CERT.PT, 2021

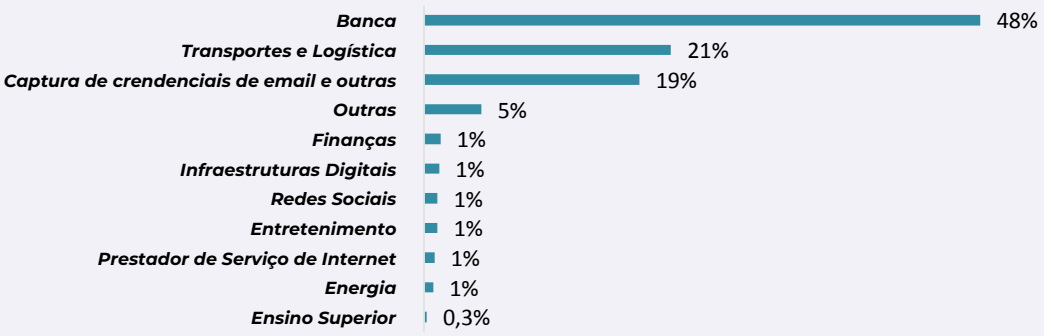


Figura 7 | CERT.PT

No que diz respeito à engenharia social, cabem dentro deste tipo de incidente atividades maliciosas particularmente orientadas às vulnerabilidades do fator humano. Os casos aqui agregados, tal como o *phishing* e o *smishing*, também procuram recolher informação de uma determinada vítima e conduzi-la a praticar ações contra os seus próprios interesses, mas através de técnicas de manipulação mais interativas e vetores de ataque diversificados.

Os incidentes registados em engenharia social são, em 43% dos casos, ataques de *vishing*, isto é, técnicas semelhantes ao *phishing* e *smishing*, mas através de telefonemas e uso de técnicas de persuasão dialógicas, grande parte das vezes, neste caso, simulando o contacto de um funcionário da empresa Microsoft que pretende resolver um problema de segurança no computador da vítima, mas conduzindo-a a instalar *malware* no seu dispositivo. A *sextortion* também continua a ser um tipo de ataque de engenharia social relevante, representando 26% dos casos, muitos dos quais consistindo em tentativas de extorsão através de *email* sob ameaça de divulgação de imagens íntimas de uma vítima, frequentemente sem que a posse dessas imagens pelo agente ameaçador seja verdadeira. Na terceira posição, surge a CEO Fraud, com 9%, referindo-se a um tipo de ataque com alguma sofisticação, através de *email* dirigido a um empregado de uma organização com responsabilidades financeiras, solicitando-se uma transferência bancária para uma conta indicada pelo agente criminoso, o qual se faz passar por uma chefia.

Nas posições seguintes surgem a tentativa de burla mediante caso fictício de herança (7%), em que alguém informa uma vítima de que ganhou uma grande quantia de dinheiro (frequentemente com a justificação de ser uma herança), pedindo uma determinada quantia para desbloquear essa oferta; a que se seguem os pedidos fraudulentos de pagamentos de faturas (7%); outros casos diversificados (5%); e a conhecida burla mediante a plataforma MBway (3%), que conduz vítimas com fraco conhecimento sobre o funcionamento desta aplicação a permitirem a transferência de dinheiro para um burlão.

Tipos ataques de engenharia social registados pelo CERT.PT, 2021

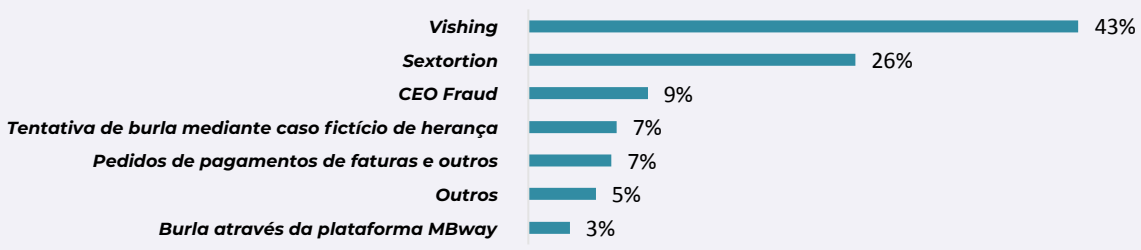


Figura 8 | CERT.PT

3. Observáveis registado pelo CERT.PT

Os chamados "observáveis" são eventos considerados relevantes, como *malware* ou vulnerabilidades nos sistemas técnicos, que são detetados de forma automatizada por várias fontes, em lugar de resultarem de métodos não automatizados de registo de incidentes. Alguns destes observáveis podem contribuir, contudo, para o registo de incidentes.

Observáveis registados pelo CERT.PT, entre 2015 e 2021, e mês, trimestre e semestre com mais registos

	Total	Tend. %	Mês c/mais	Trimestre c/mais	Semestre c/mais
2015 (desde maio)	4 117 875	N/A	Dez. (1 355 528)	N/A	N/A
2016	2 931 767	N/A	jun. (543 908)	2º (749 839)	1º (1 497 109)
2017	42 956 624	+1365	abr. (9 880 158)	2º (16 224 673)	2º (26 138 163)
2018	55 607 704	+29	mai. (5 711 090)	2º (14 891 405)	2º (28 177 553)
2019	54 925 366	-1	abr. (4 929 377)	3º (14 142 871)	2º (27 607 524)
2020	61 045 497	+11	fev. (8 838 632)	1º (18 631 817)	1º (34 386 651)
2021	47 699 049	-22	set. (5 607 771)	3º (12 803 828)	1º (24 370 391)

Tabela 6 | CERT.PT

Apesar do número de incidentes ter aumentado, o número de observáveis decresceu 22% em 2021, depois de ter ocorrido um aumento entre 2019 e 2020, em 11%, e desde 2016 apenas ter ocorrido um decréscimo de 1%, entre 2018 e 2019. Alguma variação no número e tipo de fontes utilizadas pode produzir efeitos nos dados apresentados. Neste caso, ocorreu uma falha numa das fontes de observáveis no mês de novembro que ajudou a produzir esta descida.

Durante 2021, o mês de setembro foi aquele que registou o maior volume de observáveis. Entre os vários trimestres, a este respeito, sobressai o terceiro. Entre os semestres, o primeiro teve mais registos do que o segundo. Comparando os vários anos, não parece haver um padrão quanto a meses, trimestres e semestres com mais observáveis, exceto quanto ao facto de o quarto trimestre nunca ter sido o que regista mais observáveis, embora frequentemente seja o que apresenta mais incidentes.

Número de observáveis registados pelo CERT.PT, entre 2015 (maio) e 2021

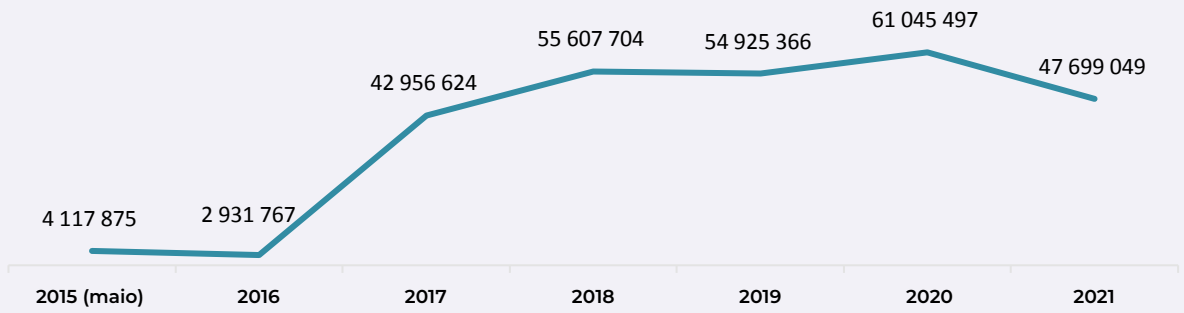
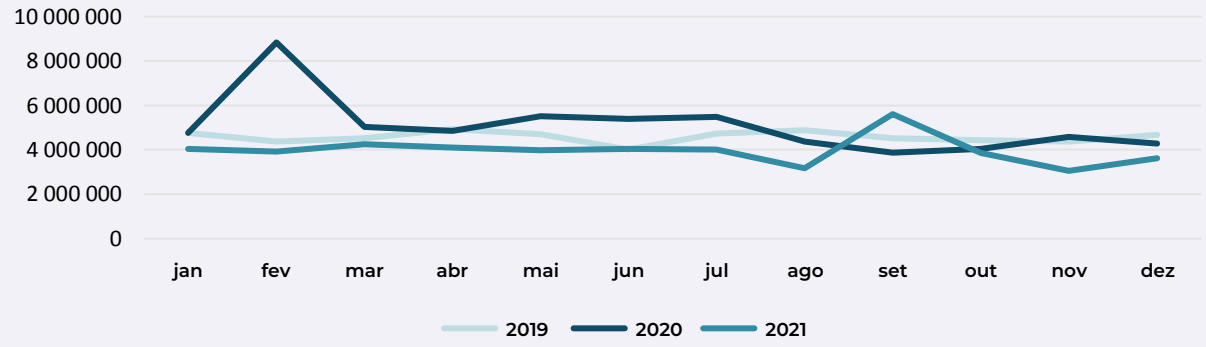


Figura 9 | CERT.PT

Pese embora a variação fruto de questões metodológicas, que interferem em particular com os meses de fevereiro de 2020 e de novembro de 2021, verifica-se que o ano de 2021 regista menos observáveis do que 2019 e 2020 em quase todos os meses, com exceção de junho, relativamente a 2019, e de setembro, com respeito a 2019 e 2020.

Número de observáveis registados pelo CERT.PT, 2019, 2020 e 2021 – por mês*



*Os valores de fevereiro de 2020 são inflacionados por fatores metodológicos que conduziram ao acumular de registos neste período. Os valores de 2021 foram influenciados por uma quebra de fornecimento numa das fontes, em particular no mês de novembro.

Figura 10 | CERT.PT

Quanto ao tipo de observáveis, o serviço vulnerável mantém-se como o mais frequente, representando 94% dos casos. Em geral, identifica-se um decréscimo no número de quase todos os tipos de observáveis, mas uma subida significativa do *botnet drone*, em 29%, para a segunda posição, e uma descida acentuada do *malware*, que passou da segunda posição para fora do quadro (na 13ª posição). Mantém-se a importância relativa da *blacklist* e da força-bruta, além da entrada para a sexta posição do DDoS (tipo de observável que não se incluía na taxonomia do ano anterior).

Observáveis por tipo registados pelo CERT.PT, 2020 e 2021 - Top 10

2020				2021				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta %	Lugar RK
1º	Serviço vulnerável	55 367 757	91	1º	Serviço vulnerável	44 843 932	94	- 19	=
2º	*Malware*	3 139 447	5	2º	*Botnet drone*	1 301 026	3	+ 29	+
3º	*Blacklist*	1 355 290	2	3º	Outro	783 690	2	N/A*	N/A
4º	*Botnet drone*	1 011 832	2	4º	*Blacklist*	612 251	1	- 55	-
5º	Força-bruta	118 234	0,2	5º	Força-bruta	92473	0,2	- 22	=
6º	C&C	20342	0,03	6º	DDoS	26951	0,1	N/A	N/A
7º	Distribuição de *malware*	14232	0,02	7º	C&C	15466	0,03	- 24	-
8º	Alerta IDS	8657	0,01	8º	*Scanner*	11859	0,02	+ 605	+
9º	*Phishing*	6146	0,01	9º	Alerta IDS	8946	0,02	+ 3	-
10º	Comprometimento	1866	0,003	10º	*Phishing*	1253	0,002	- 80	-

* *Os casos em que não se aplica (N/A) correspondem a novas entradas na série de tipos de observáveis.

Tabela 7 | CERT.PT

O setor com mais observáveis registados em 2021 voltou a ser o dos Prestadores de Serviços de Internet, em 84% dos casos, devido ao facto de representar grande parte dos consumidores domésticos e de organizações não incluídas noutras categorias. Com percentagens bastantes mais baixas, mas mantendo as posições de destaque do ano anterior, surgem a Educação e Ciência, Tecnologia e Ensino Superior e os Serviços de Computação em Nuvem.

Observáveis por setor e área governativa, registados pelo CERT.PT, 2020 e 2021 - Top 15*

2020				2021				Ordenação	
RK	Setor e Área Governativa	Nº	%	RK	Setor e Área Governativa	Nº	%	Tendência absoluta %	Lugar RK
1º	Prestadores de Serviços de Internet	49 416 994	81	1º	Prestadores de Serviços de Internet	40 109 351	84	- 19	=
2º	Nulos	3 378 523	6	2º	Infraestruturas Digitais	3 507 901	7	+ 14	+
3º	Infraestruturas Digitais	3 085 590	5	3º	Educação e Ciência, Tecnologia e Ensino Superior	2 604 015	5	- 4	+
4º	Educação e Ciência, Tecnologia e Ensino Superior	2 721 137	5	4º	Nulos	956 713	2	- 72	-
5º	Serviços de Computação em Nuvem	1 621 847	3	5º	Outros	310 643	1	- 56	+
6º	Outros	702 879	1	6º	Serviços de Computação em Nuvem	100 695	0,2	- 94	-
7º	Administração Central	57104	0,1	7º	Cultura e Turismo	11844	0,02	+ 274	+
8º	Energia	10979	0,02	8º	Saúde	11809	0,02	+ 108	+
9º	Transportes	9293	0,02	9º	Banca	11455	0,02	+ 39	+
10º	Banca	8266	0,01	10º	Administração Local	10566	0,02	+ 308	+
11º	Saúde	5674	0,01	11º	Energia	9321	0,02	- 15	-
12º	Órgãos de Soberania	4420	0,01	12º	Agricultura	8904	0,02	+ 3174	+
13º	Ambiente	3992	0,01	13º	Transportes	8211	0,02	- 12	-
14º	Cultura e Turismo	3166	0,01	14º	Administração Central	6019	0,01	- 89	-
15º	Administração Interna	2902	0,005	15º	Órgãos de Soberania	5754	0,01	+ 30	-

* Este ano o número de setores e áreas governativas relativamente aos observáveis considerados aumentou, passando de 28 em 2020 para 30 em 2021.

Tabela 8 | CERT.PT

DESTAQUES

O CERT.PT registou um aumento de 26% no número de incidentes de cibersegurança em 2021 face ao ano anterior, passando de 1418 incidentes registados em 2020 para 1781 em 2021.

Este aumento, embora cumulativo no que diz respeito à subida acentuada de 2020 em relação a 2019, apresenta a mesma percentagem de aumento registada antes da pandemia, entre 2018 e 2019.

O segundo semestre, com particular relevância para o último trimestre e para o mês de novembro, é o período do ano com mais incidentes de cibersegurança registados pelo CERT.PT.

Durante 2021, por cada notificação externa, houve, em média, o registo de 0,4 incidentes, quando em 2020 o valor médio foi de 0,3. Também houve uma menor variação mensal a este respeito do que no ano anterior. Por isso, em 2021, verifica-se uma tendência para uma maior eficácia do reporte da comunidade relativamente à existência de incidentes de cibersegurança do que no ano anterior.

Mantém-se, tal como em anos anteriores, a proporção na distribuição da percentagem de incidentes entre entidades públicas e privadas, com cerca de um terço a afetar as primeiras e dois terços as segundas.

O setor com mais incidentes registados pelo CERT.PT é a Banca (primeira posição entre todos os setores e áreas governativas). A área governativa com mais incidentes registados é a Presidência do Conselho de Ministros (segunda posição entre todos os setores e áreas governativas), fruto de um crescimento acentuado em relação ao ano anterior. Os setores das Infraestruturas Digitais e dos Prestadores de Serviços de Internet continuam a ter relevância. A área governativa Educação e Ciência, Tecnologia e Ensino Superior registou uma descida significativa relativamente a 2020.

O *phishing*/*smishing* continua a ser o tipo de incidente registado pelo CERT.PT mais frequente. A engenharia social ocupa a segunda posição, o que representa uma subida acentuada em relação ao ano anterior, seguida da distribuição de *malware*. O sistema infetado por *malware* perdeu relevância, passando da terceira para a sétima posição no *ranking* geral.

As marcas mais simuladas nos ataques de *phishing*/*smishing* são as da Banca, seguidas das marcas de Transportes e Logística e das referentes a plataformas de *emails*. Os ataques de engenharia social são sobretudo de *vishing*, mas também *sextortion* e alguma CEO Fraud.

O número de observáveis registados pelo CERT.PT decresceu 22% em relação ao ano anterior. Algumas das variações no número de observáveis registados têm origem metodológica, mas não todas. O serviço vulnerável continua a ser o tipo de observável mais registado. A *botnet drone* registou um crescimento assinalável, de 29%, em contraciclo com os restantes tipos de observáveis.

Os Prestadores de Serviços de Internet e as Infraestruturas Digitais são os setores com mais observáveis registados (primeira e segunda posições entre setores e áreas governativas). A Educação e Ciência, Tecnologia e Ensino Superior é a área governativa que se destaca a este respeito (na terceira posição entre setores e áreas governativas), ao contrário do que se verifica no registo de incidentes.

INCIDENTES REGISTADOS PELOS MEMBROS DA RNCSIRT

Anualmente, a RNCSIRT realiza um inquérito interno através do qual é possível recolher dados sobre os principais incidentes de cibersegurança registados pelos seus membros. O Observatório de Cibersegurança apoia a realização deste inquérito em articulação com o secretariado da RNCSIRT. Nesta análise evita-se realizar comparações diretas com os anos anteriores devido ao facto de todos os anos entrarem novos membros para a RNCSIRT, fazendo com que o universo de respondentes se altere de formas que podem ser significativas, prejudicando a validade de uma comparação (por exemplo, em 2021 havia 45 membros e em 2022 o número subiu para 51).

Não obstante esta questão, os dados recolhidos neste contexto permitem aceder a um panorama relativo a um conjunto muito significativo de entidades que têm elevadas responsabilidades no país quanto à cibersegurança, visto muitas delas prestarem serviços fundamentais.

Durante 2021, o conjunto de membros da RNCSIRT que responderam a este inquérito e que autorizaram a partilha destes dados (29) registou 46 327 incidentes de cibersegurança. O mês com mais incidentes registados foi o de outubro, o qual contribuiu para que o quarto trimestre fosse aquele que tivesse mais volume de registos, bem como o segundo semestre comparando com o primeiro, dados semelhantes aos do CERT.PT, exceto no que se refere ao mês com mais incidentes, que no caso do CERT.PT foi novembro (os dados da RNCSIRT incluem os do CERT.PT enquanto membro desta rede).

Incidentes registados pela RNCSIRT, em 2021, e mês, trimestre e semestre com mais registos

	Total	Mês c/mais	Trimestre c/mais	Semestre c/mais
2021	46327	out. (4894)	4º (14212)	2º (26079)

Tabela 9 | RNCSIRT

Além do mês de outubro, destacam-se os dois meses seguintes, novembro e dezembro, como os que registaram mais incidentes. Portanto, o final de 2021 foi o período com mais incidentes registados entre os membros da RNCSIRT que responderam ao inquérito.

Número de incidentes registados pela RNCSIRT, 2021 – por mês

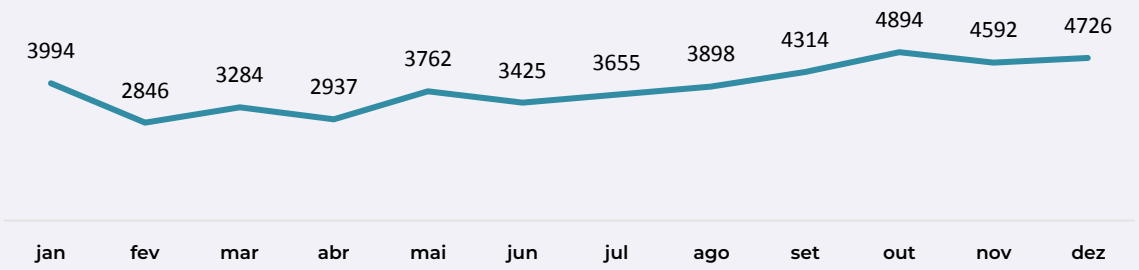


Figura 11 | RNCSIRT

Os tipos de incidentes mais registados pela RNCSIRT são a tentativa de *login*, a exploração de vulnerabilidade e o *scanning*. Comparando com os dados do CERT.PT, verifica-se que o *phishing/smishing* e a engenharia social têm menos relevância no conjunto da RNCSIRT do que no CERT.PT em particular, padrão já identificado nos anos anteriores. Não obstante, o *phishing/smishing* surge na quinta posição na RNCSIRT.

Incidentes registados pelo CERT.PT vs. RNCSIRT, 2021 – Top 10*

2021 CERT.PT				2021 RNCSIRT (inclui CERT.PT)				
RK	Tipo	Nº	%	RK	Tipo	Nº	%	RNCSIRT em relação a CERT.PT no RK
1º	Phishing/Smishing	715	40	1º	Tentativa de *login*	7375	16	+
2º	Engenharia social	246	14	2º	Outro – Sem tipo	5060	11	+
3º	Distribuição de *malware*	226	13	3º	Exploração de vulnerabilidade (tent. Intrusão)	4383	9	+
4º	Comprometimento de conta não privilegiada	114	6	4º	Scanning	3821	8	+
5º	Utilização Ilegítima de nome de terceiros	80	4	5º	Phishing/Smishing	3418	7	-
6º	Indeterminado (outro)	50	3	6º	Acesso não autorizado	3282	7	+
7º	Sistema infetado (*malware*)	46	3	7º	Sistema infetado (*malware*)	2684	6	=
8º	Sistema vulnerável (vulnerabilidade)	44	2	8º	Modificação não autorizada	2464	5	+
9º	Modificação não autorizada (35 ransomware)*	38	2	9º	Indeterminado (outro)	1930	4	-
10º	Exploração de vulnerabilidade (tent. Intrusão)	37	2	10º	Distribuição de *malware*	1553	3	-

Tabela 10 | CERT.PT e RNCSIRT

No que diz respeito aos cinco tipos de incidentes de cibersegurança mais registados pela RNCSIRT ao longo do ano é notório o papel da tentativa de *login* nos números de janeiro, outubro e dezembro. Durante o mês de novembro, o *phishing* teve particular relevância.

Número de incidentes registados pela RNCSIRT, 2021 – Top 5, por mês

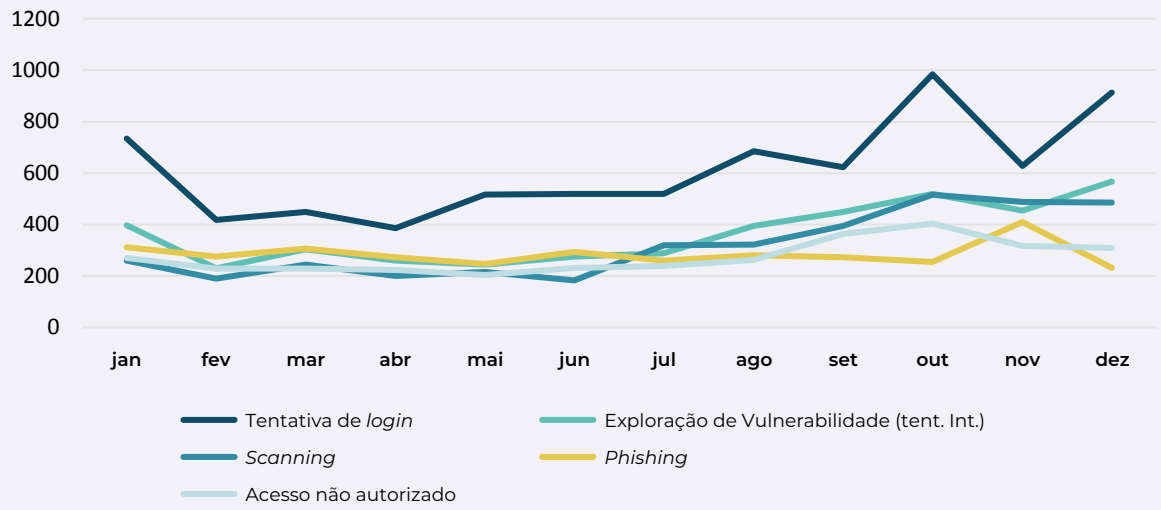


Figura 12 | RNCSIRT

DESTAQUES

O segundo semestre de 2021 foi o período no qual se registaram mais incidentes entre os membros da RNCSIRT, com particular incidência no último trimestre.

Os tipos de incidentes mais registados pela RNCSIRT foram a tentativa de *login*, a exploração de vulnerabilidade e o *scanning*. O *phishing/smishing* foi menos relevante do que no âmbito do CERT.PT, mas ainda assim ocupou a quinta posição.

A tentativa de *login* teve particular influência no aumento do número de incidentes durante os meses de outubro e dezembro de 2021.

NOTIFICAÇÕES À CNPD SOBRE VIOLAÇÕES DE DADOS PESSOAIS

Ao longo do ano a CNPD recebe notificações de casos de violações de dados pessoais[4], abrindo processos que podem ser contabilizados no seu número. A partir do presente ano, além deste indicador, é possível partilhar mais alguns elementos sobre as características dos valores fornecidos pela CNPD.

O presente Relatório tem acompanhado a evolução do indicador referente ao número de notificações recebidas pela CNPD desde maio de 2018, verificando-se um contínuo crescimento no volume de notificações, com especial relevância para a variação entre 2019 e 2020, a qual registou um crescimento de 25%. Entre 2020 e 2021, a variação é menor, correspondendo a um aumento de 6% no número de notificações, tendo passado de 301 para 318.

Notificações à CNPD de violações (de segurança) de dados pessoais, entre 2018 e 2021*

	Total	Tend. %
2018 (desde maio)	160	N/A
2019	240	N/A
2020	301	+25
2021	318	+6

* Nos termos do artigo 33º do Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD), na aceção do artigo 4º, alínea 12), do RGPD.

Tabela 11 | CNPD

As notificações recebidas pela CNPD provêm na sua maioria de entidades privadas, em 79% dos casos. Portanto, os restantes 21% correspondem a notificações de entidades públicas.

Notificações por Entidades Privadas e Entidades Públicas, registadas pela CNPD, 2021

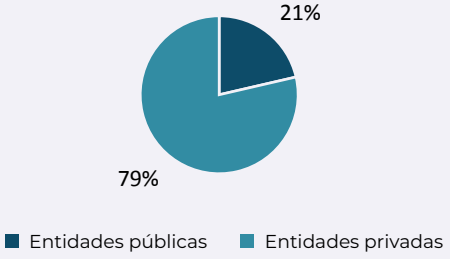


Figura 13 | CNPD

4 Nos termos do artigo 33º do Regulamento (UE) 2016/679 – Regulamento Geral sobre a Proteção de Dados (RGPD), na aceção do artigo 4º, alínea 12), do RGPD, a menos que a violação não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares.

Os setores e atividades que, no âmbito privado, mais notificações realizaram à CNPD por violações de dados pessoais foram o Comércio e Serviços, com 25%, a Banca e Seguros, com 13%, e a Consultoria, com 8%. O Comércio e Serviços, bem como a Banca e Seguros, são aqueles que mais notificações realizaram se considerarmos o conjunto dos setores e atividades públicos e privados, como é possível verificar na tabela 12. Entre os setores e atividades públicos, a Administração Local destaca-se com 40% das notificações, seguida do Ensino Superior, com 35%, e da Administração Central, com 15%. No conjunto do público e do privado, a Administração Local encontra-se na terceira posição, com 8% das notificações.

Notificações por setores e atividades, públicos e privados, recebidas pela CNPD, 2021

RK	Setores e Atividades Privados	Nº	% Privado	% Total
1º	Comércio e Serviços	78	25	31
2º	Banca e Seguros	42	13	17
3º	Consultoria	24	8	10
4º	Indústria	21	7	8
5º	Turismo e Restauração	20	6	8
6º	Saúde	19	6	8
7º	Internet e Comunicações	18	6	7
8º	Educação	16	5	6
9º	Cultura, Média e Desporto	6	2	2
10º	TIC	6	2	2
RK	**Setores e Atividades Públicos**	**Nº**	**% Público**	**% Total**
1º	Administração Local	27	40	8
2º	Ensino Superior	24	35	8
3º	Administração Central	10	15	3
4º	Saúde	5	7	2
5º	Outro	2	3	1

Tabela 12 | CNPD

A violação de dados pessoais implica o comprometimento de pelo menos um dos princípios da segurança de informação (confidencialidade, integridade e/ou disponibilidade)[5]. Entre as notificações recebidas pela CNPD, a confidencialidade surge como o princípio mais afetado, em 64% dos casos, seguido da disponibilidade, em 13%, e de casos em que os três princípios são afetados, em 8%.

5 Em conformidade com a alínea b) do n.º 1 do artigo 32º do RGPD.

Princípios comprometidos de acordo com as notificações recebidas pela CNPD, 2021*

RK	Princípios comprometidos	Nº	%
1º	Confidencialidade	204	64
2º	Disponibilidade	41	13
3º	Confidencialidade/Disponibilidade/Integridade	27	8
4º	Integridade	20	6
5º	Confidencialidade/Disponibilidade	10	3
6º	Confidencialidade/Integridade	8	3
7º	Disponibilidade/Integridade	8	3

* Esta informação é baseada nas notificações feitas à CNPD e não em verificações inspetivas realizadas pela CNPD, pelo que pode não retratar com rigor, em todos os casos, um quadro completo dos acontecimentos.

Tabela 13 | CNPD

Do ponto de vista do acumulado das notificações por cada princípio afetado, a confidencialidade confirma a sua preponderância como princípio atingido, em 62% dos casos, seguida da disponibilidade, em 22%. O ataque à integridade está presente em apenas 16% das notificações. Portanto, poder-se-á dizer que grande parte das violações de dados pessoais notificadas dizem respeito à divulgação indevida de informação e não à sua destruição ou impossibilidade de acesso à mesma.

Acumulado - Princípios comprometidos de acordo com as notificações recebidas pela CNPD, 2021*

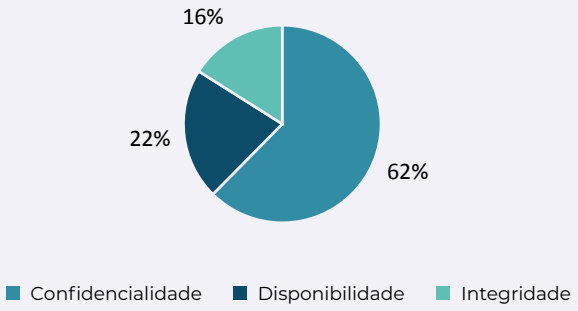


Figura 14 | CNPD

De acordo com as notificações enviadas à CNPD, o tipo de incidente mais frequente que conduziu à violação de dados foi a falha humana, em 24% dos casos, seguida do *ransomware*, em 22%, e das ações fraudulentas, em 14%. Dada a sua importância entre os incidentes registados pelo CERT.PT, também merece referência o *phishing*/engenharia social pela sua quarta posição e presença em 12% das situações.

Origem dos incidentes de acordo com as notificações recebidas pela CNPD, 2021*

RK	Origem dos incidentes	Nº	%
1º	Falha humana	77	24
2º	Ransomware	70	22
3º	Ações fraudulentas (utilização indevida de recursos, usurpação de identidade)	42	13
4º	Phishing/Engenharia Social	38	12
5º	Falhas aplicacionais (desenho, implementação e/ou configuração)	32	10
6º	Exploração de outras vulnerabilidades	30	9
7º	Outras	12	4
8º	Perda ou furto de equipamento	9	3
9º	Malware	8	3

* Esta informação é baseada nas notificações feitas à CNPD e não em verificações inspetivas realizadas pela CNPD, pelo que pode não retratar com rigor, em todos os casos, um quadro completo dos acontecimentos.

Tabela 14 | CNPD

DESTAQUES

Entre 2020 e 2021 verificou-se um aumento de 6% no número de notificações enviadas à CNPD, de 301 para 308.

Na sua maioria, em 79% dos casos, as notificações provêm de entidades privadas. As restantes, em 21%, são originadas por entidades públicas.

Os setores e atividades com mais notificações são o Comércio e Serviços, com 25% dos casos, seguido da Banca, com 13% (ambos de entidades privadas), e da Administração Local, com 8% (entidades públicas).

O princípio de segurança da informação mais frequentemente comprometido entre os casos reportados por notificação à CNPD foi o da confidencialidade, presente em 62% das situações.

Entre as notificações enviadas, a origem mais frequente para os incidentes em causa foi a falha humana, em 24%, o *ransomware*, em 22%, e as ações fraudulentas, em 13%.

CIBERCRIME

Em paralelo aos incidentes de cibersegurança existem os registos de cibercrime. Nem sempre os primeiros resultam nos segundos, mas, em princípio, existe um potencial cibercrime num incidente de cibersegurança e vice-versa. Neste capítulo, analisam-se os dados disponibilizados pela Direção-Geral da Política de Justiça (DGPJ) sobre crimes participados, condenações e arguidos; os números sobre as denúncias ao Gabinete Cibercrime da Procuradoria-Geral da República (PGR); e as estatísticas da Linha Internet Segura (LIS) da Associação Portuguesa de Apoio à Vítima (APAV).

Estes dados tanto se referem a casos que se revelaram crimes efetivos (os de condenados, por exemplo), como a situações ligadas a participações e denúncias, que podem não resultar em condenações. Além disso, alguns indicadores são de crimes estritamente informáticos, designados de "cibercrimes dependentes" por resultarem de ataques à segurança da informação por uma via necessariamente informática (como o *ransomware* ou o DDoS), mas muitos são "ciberinstrumentais", isto é, crimes que utilizam os meios informáticos como instrumentos para a sua execução, mas, de alguma forma, poderiam utilizar outros meios, como é o casos de diversos tipos de burla realizados *online* (para uma melhor compreensão desta distinção, ver Bravo, 2022 e Europol, 2021).

REGISTOS DA CIBERCRIMINALIDADE EM PORTUGAL (DGPJ)

A DGPJ produz as principais estatísticas relativamente à justiça em termos de criminalidade. Todos os anos esta instituição colabora na realização do presente Relatório, disponibilizando estatísticas sobre os cibercrimes registados pelas autoridades, os condenados e os arguidos. Estes números dizem respeito a crimes categorizados como informáticos (mencionados na Lei do Cibercrime) e àqueles que se referem explicitamente a meios informáticos (a devassa por meio informático e a burla informática/comunicações) – o conjunto dos crimes informáticos e dos que se referem a meios informáticos designa-se de "crimes relacionados com a informática". Apesar do rigor destes números, eles não capturam todo o espectro de crimes realizados *online*, pelo que as denúncias à PGR e à APAV são particularmente relevantes porque alargam o espectro de crimes considerados.

O número de crimes relacionados com a informática registados pelas autoridades policiais entre 2020 e 2021 aumentou, de 22 076 para 23 409, respetivamente, correspondendo a um crescimento de 6%. Não obstante, o número de registos relativos a crimes estritamente informáticos (do âmbito da Lei do Cibercrime, mas incluídos nos relacionados com a informática) decresceu 11%. Esta situação, como se verá, deve-se sobretudo a um incremento no número de registos de crime de burla informática/comunicações.

Número de crimes relacionados com a informática e crimes informáticos (incluídos nos relacionados com a informática) registados pelas autoridades policiais, entre 2009 e 2021

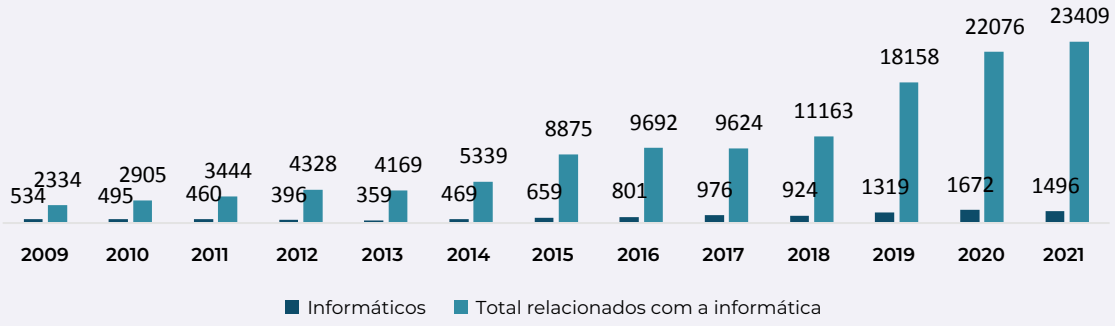


Figura 15 | DGPJ

O crescimento de 6% verificado em 2021 no total de crimes relacionados com a informática foi significativamente menor do que em 2019 e 2020. Em 2019, registou-se um crescimento de 63% e, em 2020, de 22%. No que diz respeito a crimes estritamente informáticos a mudança é mais significativa, na medida em que se passou de crescimentos da ordem dos 43% em 2019 e 27% em 2020 para um decrescimento de 11% em 2021. Esta situação poderá ser explicada pela ocorrência de um ajuste, no âmbito dos crimes informáticos, para níveis pré-pandemia e por uma importância ainda crescente dos crimes ciberinstrumentais, como a burla *online*.

Crimes relacionados com a informática e crimes informáticos (incluídos nos relacionados com a informática) registados pelas autoridades policiais, entre 2009 e 2021, variação (%)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Rel. Informática	+24	+19	+26	-4	+28	+66	+9	-1	+16	+63	+22	+6
Cri. Informáticos	-7	-7	-14	-9	+31	+41	+22	+22	-5	+43	+27	-11

Tabela 15 | DGPJ

Entre os crimes relacionados com a informática registados pelas autoridades, a burla informática/comunicações continua a destacar-se como a que apresenta mais registos (91% do total), tendo passado de 19 855 registos em 2020 para 21 374 em 2021, um crescimento de 8%. O acesso/interceção ilegítimos (3% do total) surge como o segundo tipo de crime com mais registos, mas o que apresenta o maior volume entre os crimes informáticos. Não obstante, este crime decresceu 17% face ao ano anterior.

Crimes relacionados com a informática registados pelas autoridades policiais, 2020 e 2021 – Top 5

2020				2021				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Tendência absoluta %	Lugar RK
1º	Burla informática/comunicações	19 855	90	1º	Burla informática/comunicações	21374	91	+8	=
2º	Acesso/interceção ilegítimos	764	3	2º	Acesso/interceção ilegítimos	632	3	-17	=
3º	Devassa p/meio de informática	549	2	3º	Devassa p/meio de informática	539	2	-2	=
4º	Falsidade informática	503	2	4º	Falsidade informática	523	2	+4	=
5º	Sabotagem informática	270	1	5º	Sabotagem informática	227	1	-16	=

Tabela 16 | DGPJ

Observando na figura 16 a evolução do número de crimes informáticos registados pelas autoridades policiais, tendo em conta os três tipos de crimes mais registados, verifica-se que o acesso/interceção ilegítimos foi de forma consistente o crime com mais registos, seguido da falsidade informática e da sabotagem informática. Entre 2020 e 2021, apenas a falsidade informática apresentou uma subida no seu volume, passando de 503 para 523 casos.

Número de crimes informáticos registados pelas autoridades policiais, entre 2009 e 2021 - Top 3

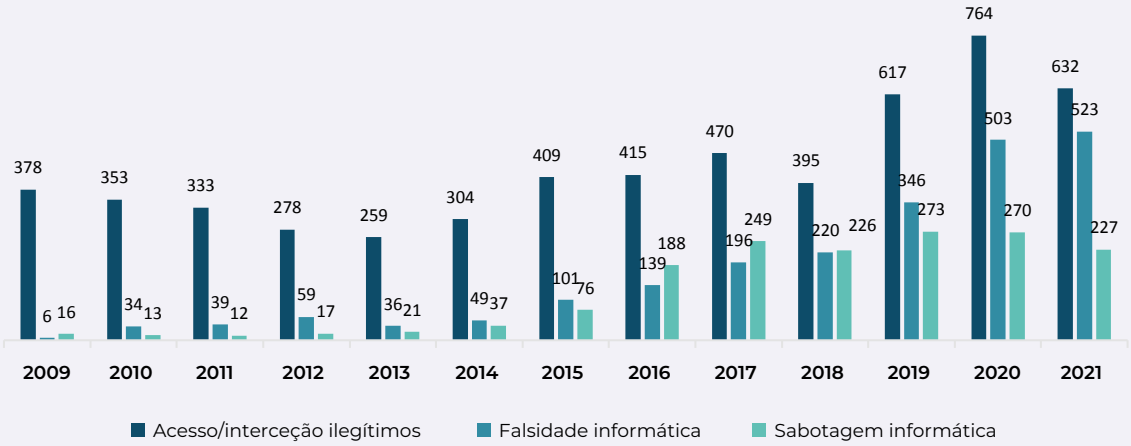


Figura 16 | DGPJ

Entre os crimes não incluídos na Lei do Cibercrime e explicitamente relacionados com a informática, a burla informática/comunicações mantém-se como o crime mais frequente desde 2009, com particular relevância para os últimos três anos.

Número de crimes de devassa por meio informático e burla informática/comunicações registados pelas autoridades policiais, entre 2009 e 2021

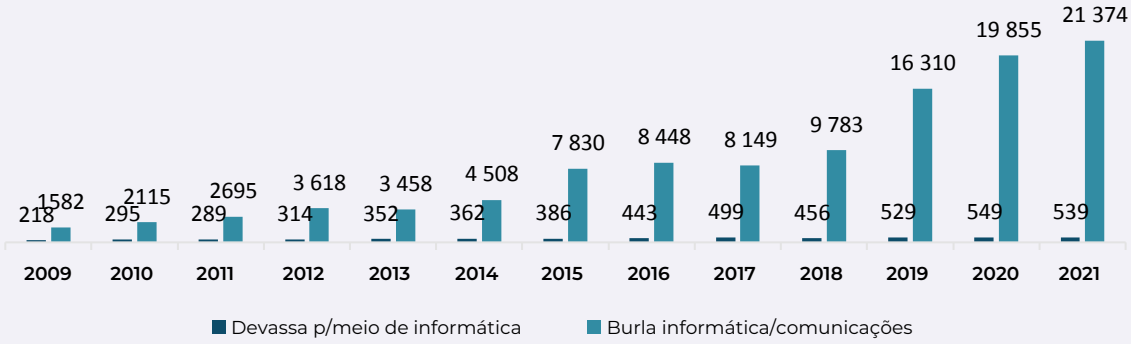


Figura 17 | DGPJ

Comparando os números de crimes relacionados com a informática com a totalidade de crimes registados pelas autoridades policiais em Portugal, verifica-se uma tendência decrescente no número total de crimes registados, embora tenha havido um ligeiro incremento em 2021 (0,9%), e uma tendência crescente entre os crimes relacionados com a informática.

Números totais de todos os crimes e de relacionados com a informática registados pelas autoridades policiais, entre 2009 e 2021

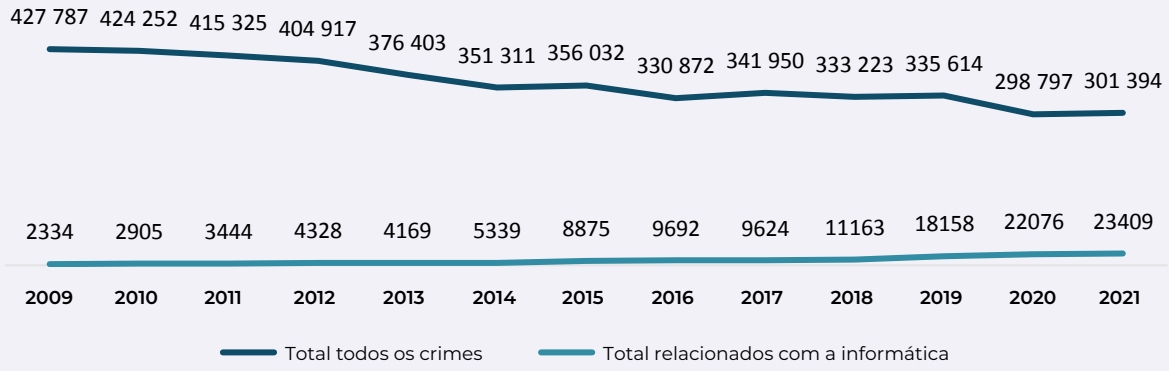


Figura 18 | DGPJ

Estas duas tendências divergentes expressam-se num crescimento da proporção de crimes relacionados com a informática em relação ao total de crimes registados pelas autoridades policiais. Desde 2009 que se regista, em geral, um aumento na percentagem destes crimes relativamente ao total. Entre 2020 e 2021, esta dinâmica manteve-se, com um crescimento de 7,4% para 7,8%. Não obstante, comparando com as variações de 2019 e 2020, de cerca de 2 pp, em 2021 esta variação é menor, de apenas 0,4 pp.

Percentagem de crimes relacionados com a informática em relação ao total de crimes registados pelas autoridades policiais, entre 2009 e 2021

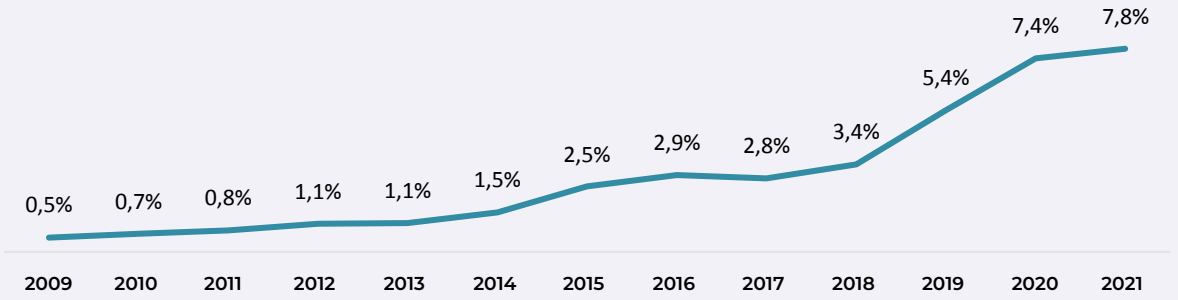


Figura 19 | DGPJ

No que diz respeito aos condenados em processos-crime em julgamento em tribunais de primeira instância, no momento de publicação do presente documento, apenas existem dados até 2020, mas que representam uma atualização relativamente ao Relatório do ano passado. O número de condenados neste âmbito decresceu em 2020 em relação ao ano anterior, de 255 para 144 (menos 44%), considerando todos os relacionados com informática, e de 87 para 35 (menos 60%), tendo em conta apenas os crimes informáticos.

Número de condenados em processos crime em fase de julgamento findos nos trib. 1ª instância, por crimes relacionados com a informática e crimes informáticos (incluídos nos relacionados com a informática), entre 2009 e 2020

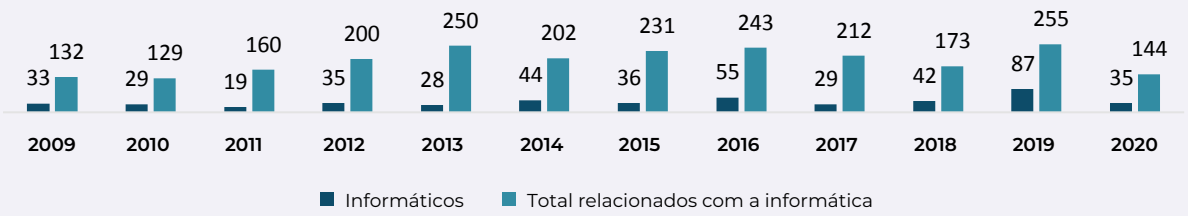


Figura 20 | DGPJ

O decréscimo de 44% no número de condenados por crimes relacionados com a informática foi acompanhado por um decréscimo no número de arguidos, de 441 para 282, isto é, uma descida de 36%. Considerando o total de condenados em Portugal, relativamente a todo o tipo de crime, também se verifica uma tendência decrescente, mas não tão acentuada: menos 23% no número total de condenados (de 47 053 em 2019 para 36 382 em 2020) e menos 24% no de arguidos (de 70 335 em 2019 para 53 204 em 2020). Esta situação poderá ser explicada por uma menor atividade dos tribunais resultante da pandemia da Covid-19.

Arguidos vs Condenados em processos-crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes relacionados com a informática, entre 2009 e 2020, variação %

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Arguidos	284	269	331	422	530	445	471	502	483	405	441	282
Variação %	N/A	-5	23	27	26	-16	6	7	-4	-16	9	-36
Condenados	132	129	160	200	250	202	231	243	212	173	255	144
Variação %	N/A	-2	24	25	25	-19	14	5	-13	-18	47	-44

* Verificam-se ligeiras atualizações aos números de alguns dos anos comparando com a publicação do ano anterior.

Tabela 17 | DGPJ

Em 2020, manteve-se o padrão de a burla informática/comunicações ser o crime com mais condenados, seguida da falsidade informática e do acesso ilegítimo. Não obstante, qualquer destes crimes teve menos condenados do que em 2019, embora a proporção da burla informática/comunicações em relação ao total tenha aumentado. A reprodução ilegítima de programa protegido (igual ao acesso ilegítimo) e o dano relativo a dados/programas registam-se como novas entradas, com 6 e 3 condenados, respetivamente.

Condenados em processos-crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes relacionados com a informática, 2019 e 2020 – Top 5*

2019				2020				Ordenação	
RK	Crime	Nº	%	RK	Setor	Nº	%	Tendência absoluta %	Lugar RK
1º	Burla informática/comunicações	166	65	1º	Burla informática/comunicações	108	75	-35	=
2º	Falsidade informática	70	27	2º	Falsidade informática	19	13	-73	=
3º	Acesso Ilegítimo	8	3	3º	Acesso Ilegítimo	6	4	-25	=
4º	Sabotagem Informática	3	1	4º	Reprodução ileg. prog. protegido	6	4	N/A	+
5º	N/A	N/A	N/A	5º	Dano Rel. Dados/Programas	3	2	N/A	+

Tabela 18 | DGPJ

Aspetos sociodemográficos relevantes em Portugal 2020

Sexo A maioria dos condenados singulares é homem, em 64% dos casos.

Idade A faixa etária com mais condenados singulares é a compreendida entre os 21 e os 29 anos de idade, correspondendo a 29% dos casos, seguida da faixa etária entre os 30 e os 39 anos, com 27%.

DESTAQUES

O número de crimes relacionados com a informática registados pelas autoridades policiais cresceu 6% em 2021 face ao ano anterior. Todavia, o número de crimes estritamente informáticos decresceu 11%. O número total de todos os crimes registados em Portugal aumentou 0,9%.

A proporção de crimes relacionados com a informática em relação ao total de crimes registados cresceu de 7,4% em 2020 para 7,8% em 2021.

A burla informática/comunicações continua a destacar-se como o crime relacionado com a informática com mais registos (91% do total). Segue-se o acesso/interceção ilegítimos (com 3%), o crime estritamente informático com mais casos.

A burla informática/comunicações continua a ser o tipo de crime relacionado com a informática com mais condenados (75% dos casos), seguido da falsidade informática (13%), crime especificamente da Lei do Cibercrime.

A maioria dos condenados singulares por crimes relacionados com a informática é homem e pessoas com idades compreendidas entre os 21 e os 39 anos.

O número de condenados e de arguidos por crimes relacionados com a informática decresceu 44% e 36%, respetivamente, em 2020 face a 2019.

DENÚNCIAS AO GABINETE CIBERCRIME DA PGR

Uma das formas que se encontra em Portugal de monitorizar as tendências no cibercrime para lá da Lei do Cibercrime ou dos crimes explicitamente relacionados com a informática é através da análise que o Gabinete Cibercrime da PGR realiza a partir das denúncias que recebe, utilizando uma abordagem mais abrangente daquilo que é integrável nesta categoria.

Em 2021, a tendência de subida no número de denúncias ao Gabinete Cibercrime mantém-se, não só tendo em conta que esta se regista constantemente desde 2016, como também se for considerada a variação muito acentuada entre 2019 e 2020, para quase o triplo de casos (182%), coincidindo com o início da pandemia da Covid-19, nível de subida que quase se repete em 2021, com um crescimento para pouco mais do dobro dos casos registados em 2020 (113%). O mês com mais denúncias em 2021 foi fevereiro, um momento particularmente marcado pelo confinamento social. Tal como em 2020, o segundo trimestre e o primeiro semestre foram os períodos específicos que apresentaram mais denúncias ao longo do ano.

Denúncias recebidas pelo Gabinete Cibercrime da PGR, entre 2016 e 2021*

	Total	Tend. %	Mês c/mais	Trimestre c/mais	Semestre c/mais
2016 (desde fevereiro)	108	N/A	S/D	S/D	S/D
2017	155	+44	S/D	S/D	S/D
2018	160	+3	S/D	S/D	S/D
2019	193	+21	S/D	S/D	S/D
2020	544	+182	Mai. (51)	2º (219)	1º (305)
2021	1160	+ 113	Fev. (133)	2º (300)	1º (594)

* Denúncias recebidas no *email* cibercrime@pgr.pt. Nem todas são encaminhadas para inquérito. "Cibercrime" entendido no seu sentido lato: "Comummente, inclui-se na expressão cibercrime um alargado conjunto muito heterogéneo de tipos legais de crime. Além dos ilícitos descritos na Lei do Cibercrime (Lei n.º 109/2009) assim acontece também com muitos outros crimes, quer incluídos no Código Penal, quer em diversas outras fontes legais avulsas" (PGR, 2022, p. 3).

Tabela 19 | PGR (2022)

Comparando o número de denúncias por mês em 2021 com o ano anterior, verifica-se que, enquanto em 2020 ocorreu uma grande concentração de denúncias no mês de abril (131), em 2021 ocorreram pelo menos dois picos importantes, em fevereiro (133) e julho (128). Os meses com mais confinamento social foram, precisamente, em 2020, abril, e em 2021, fevereiro (CNCS, 2021). Também se verifica que, em 2021, abril foi o único mês com menos denúncias do que no período homólogo.

Número de denúncias recebidas pelo Gabinete Cibecrime da PGR, 2020 e 2021 - por mês

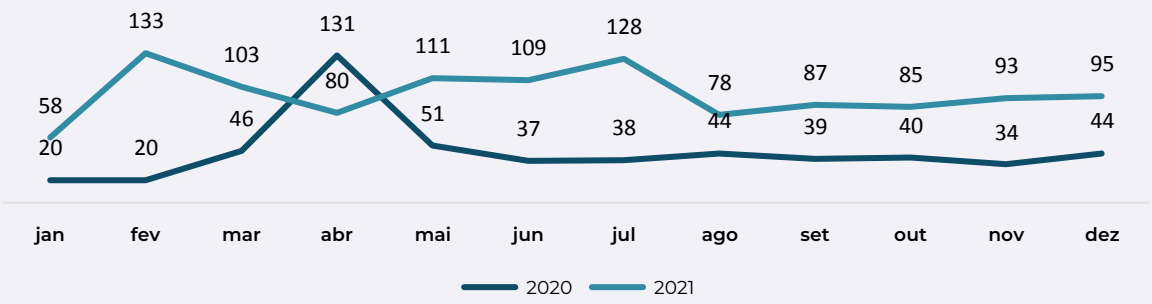


Figura 21 | PGR (2022)

Não obstante a tendência de subida no que se refere a denúncias, o número de encaminhamentos para inquérito não acompanha esta subida de forma paralela (em 41%, comparando com os 113% de denúncias) e o número de encaminhamentos por cada denúncia diminuiu, de 0,3 em 2020 (valor consitente entre 2018 e 2020), para 0,2 em 2021. [6]

Encaminhamentos para inquérito enviados pelo Gabinete Cibercrime da PGR por cada denúncia, entre 2016 e 2021

	Denúncias	Encaminhadas p/inquérito	Tend. Enc. Inq. %	Encaminhadas p/denúncia
2016 (desde fevereiro)	108	25	N/A	N/A
2017	155	59	+136	0,4
2018	160	50	-15	0,3
2019	193	67	+34	0,3
2020	544	138	+106	0,3
2021	1160	195	+41	0,2

Tabela 20 | PGR (2022)

Através de uma análise mensal é possível verificar que o ano de 2021, embora tenha sido um ano com mais denúncias do que 2020, foi um ano em que apenas durante o mês de fevereiro se atingiu o valor máximo de 0,3 encaminhamentos por denúncia, quando no ano anterior, em vários momentos, se atingiu o valor de 0,4.

6 A PGR apresenta pelo menos duas razões que explicam esta situação: algumas denúncias referem-se ao mesmo caso, conduzindo apenas a um inquérito, como acontece com muitas situações de *phishing*, e algumas denúncias repetem denúncias anteriores por outras vias, não se justificando abertura de novo inquérito.

Número de encaminhamentos para inquérito por cada denúncia à PGR, 2020 e 2021 – por mês

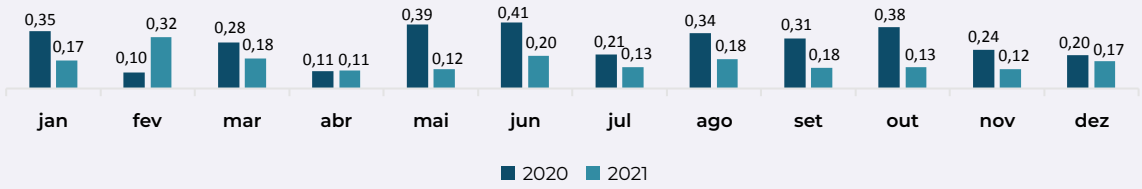


Figura 22 | PGR (2022)

A criminalidade mais frequente a que se referem as denúncias e os inquéritos considerados nesta análise apresenta algumas alterações relevantes em 2021, mas também bastantes elementos de estabilidade, comparando com o ano anterior. A alteração mais importante é a descida acentuada da preponderância dos casos relativos às defraudações na utilização da aplicação de pagamentos MBway, que em 2020 foi a atividade criminal mais frequente registada neste âmbito. Esta diminuição de casos terá relação com algumas detenções realizadas pela Polícia Judiciária (PJ) de indivíduos que praticavam esta atividade criminosa. O *phishing*, em especial aquele que procura a captura de dados de cartões de crédito, e diversos tipos de burlas *online* continuam a ser muito dominantes, tal como no ano anterior. É notória a importância da engenharia social e de ações maliciosas que passam pela manipulação de pessoas utilizando meios informáticos e o seu poder de simulação. As falsas chamadas em nome da empresa Microsoft são uma nova entrada que interessa realçar na medida em que também foi identificada com algum volume por parte do CERT.PT. O tipo de incidentes mais registados por este – o *phishing* e a engenharia social - coincidem no *modus operandi* com a criminalidade mais frequente entre as denúncias ao Gabinete Cibercrime da PGR.

Criminalidade mais frequente com base no registo de denúncias ao Gabinete Cibercrime, da PGR, 2020 e 2021*

2020		2021		
RK	**Criminalidade mais frequente**	**RK**	**Criminalidade mais frequente**	**Lugar RK**
1º	Defraudações na utilização de MBway	1º	Phishing, em especial a dados de cartões de crédito	+
2º	Phishing	2º	Burlas *online*	+
3º	Ransomware	3º	Burlas com páginas *web* "falsas"	+
4º	CEO *fraud*	4º	Burlas com criptoativos e outros produtos financeiros	+
5º	Burlas *online*	5º	Burlas em relações pessoais	+
6º	Burlas com relacionamentos e criptomoedas	6º	CEO fraud	-
7º	Burlas com páginas *web* falsas	7º	Ataques informáticos (p. ex., DDoS, intrusão ou *ransomware*)	+
8º	Divulgação de dados privados e fotografias	8º	Falsas chamadas em nome da Microsoft	+
9º	Stalking (perseguição) e *sextortion*	9º	Divulgação de fotografias e outra informação pessoal	-
10º	Discurso de ódio *online*	10º	Stalking (perseguição) e *sextortion*	-
11º	Violação de direito de autor	11º	Discurso de ódio *online*	-
12º	N/A	12º	Violação de direito de autor	-
13º	N/A	13º	Defraudações na utilização MBWAY	-

* Não são apresentados números concretos em relação a esta criminalidade. Todavia, elenca-se de forma decrescente a criminalidade mais frequente que predomina no âmbito das denúncias e inquéritos acima referidos. Em alguns casos, a terminologia adotata altera ligeiramente, mas sem comprometer a comparabilidade conceptual. Nos casos de novas entradas, assume-se que correspondem a uma subida.

Tabela 21 | PGR (2021 e 2022)

DESTAQUES

O número de denúncias ao Gabinete Cibercrime continua a aumentar de forma constante desde 2016, mas a partir de 2020 a variação anual torna-se mais acentuada, com uma subida para quase o triplo em 2020 (182%) e pouco mais do dobro em 2021 (113%).

Os meses com mais denúncias (abril em 2020 e fevereiro em 2021) correspondem aos períodos de maior confinamento social fruto da pandemia da Covid-19.

Em 2021, o número de encaminhamentos para inquérito por cada denúncia à PGR diminuiu em relação ao ano anterior, de 0,3 para 0,2.

O *phishing* e variados tipos de burla através de meios digitais continuam a ser as formas de criminalidade mais denunciadas ao Gabinete Cibercrime da PGR. As defraudações através da plataforma MBway registaram uma descida acentuada relativamente ao ano anterior.

LINHA INTERNET SEGURA

A LIS é uma plataforma de atendimento telefónico ao público que apoia vítimas de cibercrime e presta esclarecimentos com o objetivo de tornar a Internet mais segura. Permite também a realização de denúncias de conteúdos ilegais, como de pornografia infantil ou discurso de ódio. A LIS é gerida pela APAV e está enquadrada nas atividades do Consórcio Centro Internet Segura, coordenado pelo CNCS. Existem duas áreas de intervenção da LIS: a dimensão Helpline, que presta apoio a vítimas de cibercrime e aconselha na adoção de comportamentos seguros na Internet; e a dimensão Hotline, que recebe denúncias de conteúdos ilegais disponíveis na Internet ligados à pornografia infantil e ao discurso de ódio.

Processos de atendimento e apoio da Linha Internet Segura, APAV, entre 2019 e 2021*

	Total	Tend. %	Mês c/mais	Trimestre c/mais	Semestre c/mais
2019	827	N/A	Set. (98)	3º (222)	2º (442)
2020	1164	+41	Mar. (154)	1º (356)	1º (711)
2021	1626	+40	Abr. (441)	2º (737)	1º (1071)

* Nas suas duas vertentes: atendimento e denúncia.

Tabela 22 | APAV (2020, 2021 e 2022)

A tendência de subida no número de processos de atendimento e apoio registados pela LIS mantém-se. Em 2021, registaram-se 1626 processos, o que corresponde a uma subida de 41%, uma variação semelhante à do ano anterior, que havia sido de 40%.

Número de processos de atendimento e apoio da Linha Internet Segura, APAV, entre 2019 e 2021 - por mês

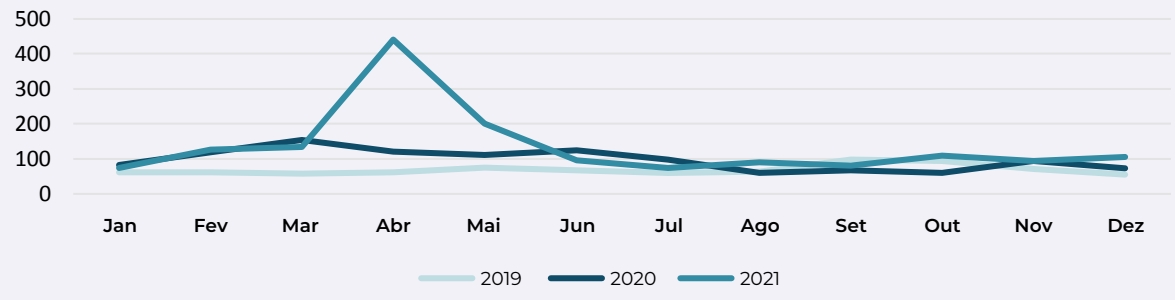


Figura 23 | APAV (2020, 2021 e 2022)

A variação mensal em 2021 apresenta uma diferença importante comparando com os dois anos anteriores: o elevado número de processos registados em abril (441). Em 2019 e 2020 não se verificou nenhum pico semelhante.

Crimes e outras formas de violência registados pela Helpline, APAV, entre 2019 e 2021*

	Total	Tend. %
2019	102	N/A
2020	587	+475
2021	454	-23

* Cada vítima pode ser alvo de mais do que um tipo de crime.

Tabela 23 | APAV (2020, 2021 e 2022)

Embora o número de processos esteja a aumentar, o total de crimes registados no âmbito específico da Helpline diminuiu 23%, de 587 em 2020 para 454 em 2021. Em 2020 registou-se, diferentemente, uma subida muito acentuada, de 475%.

Crimes e outras formas de violência registados pela Helpline, APAV, 2020 e 2021 – Top 10*

2020				2021				Ordenação	
RK	**Crimes e outras formas de violência**	**Nº**	**%**	**RK**	**Crimes e outras formas de violência**	**Nº**	**%**	**Tendência absoluta %**	**Lugar RK**
1º	Ameaça	172	29	**1º**	Sextortion	134	30	+ 294	+
2º	Difamação/Injúrias	45	8	**2º**	Burla	54	12	+ 440	+
3º	Violência doméstica	35	6	**3º**	Furto de identidade	37	8	+ 48	+
4º	Sextortion	34	6	**4º**	Difamação/Injúrias	34	7	- 24	-
5º	Gravação de fotografias ilícitas	31	5	**5º**	Gravação de fotografias ilícitas	33	7	+ 6	=
6º	Ofensas à integridade física	31	5	**6º**	Ameaça	21	5	- 88	-
7º	Furto de identidade	25	4	**7º**	Acesso ilegítimo	16	4	N/A	+
8º	Outros crimes	23	4	**8º**	Violência doméstica	15	3	- 57	+
9º	Perseguição/Stalking	21	4	**9º**	Cyberbullying	12	3	+ 71	+
10º	Bullying	20	3	**10**	Perseguição/Stalking	12	3	- 43	-

* Cada vítima pode ser alvo de mais do que um tipo de crime.

Tabela 24 | APAV (2021 e 2022)

Relativamente ao tipo de crimes e outras formas de violência registados pela Helpline, verifica-se uma forte subida da *sextortion* em 2021, passando da quarta posição para a primeira, uma subida de 294% em relação ao ano anterior. A burla, que não constava no Top 10 de 2020, passa a ocupar a segunda posição, seguida do furto de identidade. A ameaça apresenta uma descida de 88% face ao ano anterior, ocupando agora a sexta posição, quando em 2020 surgia na primeira.

Registos realizados na dimensão Hotline, pela APAV, 2020 e 2021

	Total	Tend. %
2019	701	N/A
2020	760	+8
2021	1167	+54

Tabela 25 | APAV (2020, 2021 e 2022)

Na dimensão Hotline verifica-se uma subida no número de registos bastante significativa em 2021, com 1167 registos, mais 54% do que em 2020. Entre 2019 e 2020 a variação foi de apenas 8%.

O tipo de registo na dimensão Hotline mais frequente é o de conteúdos de abuso sexual de menores, que representa mais de dois terços do volume total em 2020 e 2021. Os restantes registos dizem respeito a discurso de ódio.

Tipos de registos realizados na dimensão Hotline, pela APAV, 2020 e 2021

2020				2021				Ordenação	
RK	**Crimes e outras formas de violência**	**Nº**	**%**	**RK**	**Crimes e outras formas de violência**	**Nº**	**%**	**Tendência absoluta %**	**Lugar RK**
1º	Conteúdos de abuso sexual de menores	544	72	**1º**	Conteúdos de abuso sexual de menores	787	67	**+** 45	**=**
2º	Discurso de ódio	216	28	**2º**	Discurso de ódio	380	33	**+** 76	**=**

Tabela 26 | APAV (2021 e 2022)

Especificamente em relação a conteúdos de abuso sexual de menores, em 2021 foram categorizadas 1929 imagens deste tipo, mais 156 do que em 2020. Também se verifica um aumento no número de denúncias de conteúdos de abuso sexual de menores alojados em Portugal, que passaram de 5 em 2020 para 40 em 2021.

Número de imagens e conteúdos alojados em Portugal de abuso sexual de menores registados pela Linha Internet Segura, APAV, 2020 e 2021

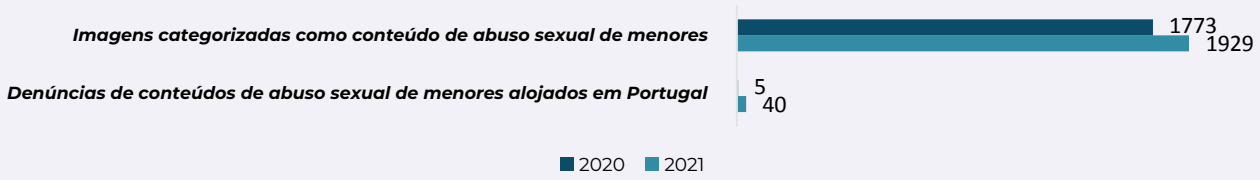


Figura 24 | APAV (2021 e 2022)

Aspetos sociodemográficos relevantes em Portugal 2021

Sexo A percentagem de homens (42%) e de mulheres (44%) identificados como vítimas no âmbito da Helpline é idêntico (os restantes não se identificaram), ao contrário do ano anterior, em que a percentagem de mulheres era significativamente superior (61% de mulheres para 27% de homens).

Idade As idades mais representadas entre as vítimas identificadas no âmbito da Helpline são as compreendidas entre os 25 e os 34 anos (10%) e os 35 e 44 anos (11%).

DESTAQUES

Verifica-se, em 2021, uma subida de 40% no número de processos de atendimento e apoio registados pela APAV no âmbito da LIS. Esta variação é semelhante à de 2020, que foi de 41%.

O mês de abril de 2021 registou um número particularmente alto de processos, com 441 registos.

O número de crimes registados na dimensão Helpline decresceu 23% em 2021 face ao ano anterior. Entre 2019 e 2020 havia ocorrido uma subida de 457%.

A *sextortion*, a burla e o furto de identidade foram os crimes e outras formas de violência mais registados na dimensão Helpline em 2021, verificando-se uma subida acentuada das duas primeiras.

Na dimensão Hotline, em 2021, houve um crescimento no número de registos, em 54%, mantendo-se o predomínio dos conteúdos de abuso sexual de menores. O número de imagens e conteúdos alojados em Portugal identificados a este respeito também aumentou.

Síntese do Capítulo Incidentes e Cibercrime, em 2021

O número de incidentes de cibersegurança registados pelo CERT.PT continua a crescer, mas com menos intensidade do que em 2020.

Os setores mais afetados pelos incidentes de cibersegurança registados pelo CERT.PT são a Banca, as Infraestruturas Digitais e os Prestadores de Serviços de Internet. A área governativa com mais incidentes registados é a Presidência do Conselho de Ministros.

O *phishing/smishing*, a engenharia social e a distribuição de *malware* são os tipos de incidentes mais registados pelo CERT.PT.

No âmbito da RNCSIRT, os tipos de incidentes mais registados são a tentativa de *login*, a exploração de vulnerabilidades e o *scanning*.

Registou-se um ligeiro aumento no número de notificações sobre violações de dados à CNPD.

Os setores e atividades com mais notificações à CNPD são o Comércio e Serviços, a Banca e a Administração Local.

A confidencialidade é o princípio de segurança da informação mais afetado nos casos notificados à CNPD, sendo que as origens mais frequentes dos incidentes são a falha humana, o *ransomware* e as ações fraudulentas.

O número de crimes relacionados com a informática registados pelas autoridades policiais cresceu face ao ano anterior, embora menos do que em 2019 e 2020. Contudo, o número de crimes estritamente informáticos decresceu. A criminalidade em geral cresceu um pouco, mas significativamente menos do que os crimes relacionados com a informática. Proporcionalmente, há mais crimes relacionados com a informática em relação ao total de crimes registados do que em 2020.

A burla informática/comunicações é o crime relacionado com a informática com mais registos, tal como nos anos anteriores, e é a principal causa para o crescimento dos crimes relacionados com a informática. O acesso/interceção ilegítimos é o crime estritamente informático com mais registos, mas decresceu em comparação com o ano anterior. Pode concluir-se que os crimes ciberinstrumentais têm mais peso no aumento da cibercriminalidade este ano do que os ciberdependentes.

A burla informática/comunicações é o tipo de crime relacionado com a informática com mais condenados, seguido da falsidade informática (dados referentes a 2020).

Regista-se um decréscimo acentuado no número de condenados e arguidos por crimes relacionados com a informática (dados referentes a 2020).

O número de denúncias ao Gabinete Cibercrime da PGR voltou a aumentar de forma muito acentuada.

O *phishing* e variados tipos de burla constituem as denúncias mais frequentes ao Gabinete Cibercrime. As denúncias de fraudes através da plataforma MBway diminuíram de modo significativo.

No âmbito da LIS também se verificou um aumento no número de processos de atendimento registados, tal como no ano anterior.

Na dimensão Helpline da LIS, a *sextortion*, a burla e o furto de identidade foram os crimes e outras formas de violência mais registados.

> Relação com as seguintes linhas de ação da ENSC: E2 a, E2 s, E3 b, E3 c, E4 f e E4 h (ver anexo).

D. AMEAÇAS E TENDÊNCIAS

Enquanto no capítulo anterior se apresentam dados sobre incidentes e indicadores de cibercrime que efetivamente se verificaram, neste capítulo desenvolve-se uma análise sobre as ameaças percecionadas (agentes de ameaça, por exemplo), bem como sobre as tendências relativamente ao que aconteceu ou poderá acontecer. Estas perspetivas têm como base principal os contributos através de entrevistas e conteúdos escritos dos parceiros institucionais deste Relatório, resultando de aproximações, com base na experiência, a situações que são por natureza dinâmicas.

AMEAÇAS

No que diz respeito às perceções sobre ameaças, expõem-se de seguida os resultados de um inquérito sobre perceção de risco realizado pelo CNCS à sua comunidade de entidades com quem tem protocolo de colaboração, a que se segue uma panorâmica sobre os principais agentes de ameaça a atuar no ciberespaço de interesse nacional e respetivas metodologias de ataque.

PERCEÇÃO DE RISCO - RESULTADOS DE INQUÉRITO A COMUNIDADE CNCS

À semelhança do ano passado, o CNCS lançou o inquérito *Perceção de risco no ciberespaço de interesse nacional 2021/2022*, dirigido às entidades com quem tem protocolos de cooperação, em particular aos pontos de contacto nessas organizações, avaliando a sua perceção de risco relativamente ao ciberespaço de interesse nacional. O tipo de organizações e indivíduos em causa encontram-se em posições de relevância e nível de especialização em cibersegurança que os torna particularmente elegíveis para uma auscultação sobre os principais riscos percecionados por quem lida com estas matérias.

Para 98% dos inquiridos, o risco de alguma entidade sofrer um incidente de cibersegurança aumentou em 2021, mais 4 pp do que no ano anterior. Este resultado mostra que, numa lógica cumulativa, a perceção de risco tem sido crescente de ano para ano. Não obstante, enquanto cerca de 77% dos respondentes, em 2020, assumiram que a pandemia da Covid-19 influenciou essa perceção, em 2021 esse valor atingiu apenas os 65%. Quanto à perspetiva sobre 2022, a perceção de que estes riscos continuarão a aumentar verifica-se em 87% dos inquiridos, em linha com o inquérito do ano anterior, o qual apresenta o valor de 86%.

Tendência de risco para o ciberespaço de interesse nacional, em 2020, 2021 e perspetivando 2022

	2020	2021	Tend./pp
O risco de alguma entidade sofrer um incidente de cibersegurança neste ano	Aumentou	94%	98%	+4
A pandemia de Covid-19 influenciou a perceção quanto ao risco neste ano	Sim, aumentou	77%	65%	-12
O risco de alguma entidade sofrer um incidente de cibersegurança no próximo ano	Aumentou	86%	87%	+1

Tabela 27 | CNCS

O tipo de ciberameaças consideradas mais relevantes em 2021 continuam a ser o *phishing*, o *ransomware* e a engenharia social, à semelhança do ano anterior, em que as posições no *ranking* eram exatamente as mesmas. Contudo, verifica-se uma subida significativa em termos absolutos da perceção quanto à relevância do *ransomware*, que subiu de 65% para 89% dos respondentes a assinalarem a sua importância.

Quanto à perspetiva sobre 2022, a importância do *ransomware* sai de novo reforçada, ocupando a primeira posição entre as ciberameaças mais relevantes, quando em 2021 se encontrava na segunda posição.

Perceção sobre ciberameaças mais relevantes em 2020, 2021 e perspetivando 2022*

2020			2021			Ordenação		Perspetivando 2022		
RK	**Tipo**	**%**	**RK**	**Tipo**	**%**	**Tend./ pp**	**Lugar RK**	**Tipo**	**%**	**Tend./RK 2021/2022**
1º	Phishing/Smishing	89	1º	Phishing/Smishing	89	=	=	Ransomware	93	+
2º	Ransomware	65	2º	Ransomware	89	+ 24	=	Phishing/Smishing	87	-
3º	Engenharia social	58	3º	Engenharia social	65	+ 7	=	Engenharia social	74	=
4º	Exploração de vulnerabilidade	52	4º	Exploração de vulnerabilidade	59	+ 7	=	Exploração de vulnerabilidade	70	=
5º	SPAM	47	5º	SPAM	46	- 1	=	Software malicioso	52	+
6º	Comprometimento de conta	47	6º	Comprometimento de conta	41	- 6	=	Comprometimento de conta	50	=
7º	Software malicioso	41	7º	Software malicioso	48	+ 7	=	Scanning aos sistemas	46	+
8º	Tentativa de *login*	35	8º	Tentativa de *login*	35	=	=	DoS/DDoS	33	+
9º	Scanning aos sistemas	30	9º	Scanning aos sistemas	35	+ 5	=	SPAM	30	-
10º	DoS/DDoS	27	10º	DoS/DDoS	30	+ 3	=	Tentativa de *login*	28	-

*Múltiplas respostas possíveis.

Tabela 28 | CNCS

Quanto aos agentes de ameaça percecionados como os mais relevantes em 2021, a que responderam 61% dos inquiridos, sobressaem os cibercriminosos, os hacktivistas e os atores estatais. Estes últimos adquirem, assim, uma relevância que não tinham em 2020 nas perceções dos inquiridos. Quanto à perspetiva sobre 2022, indicada por 57% dos inquiridos, os cibercriminosos continuam a ser o grupo considerado mais relevante, mas verifica-se uma subida, relativamente a 2021, dos agentes estatais e dos ciberterroristas. Curiosamente, estes últimos, na realidade, têm muito menos relevância real do que é percecionado, se considerarmos os dados objetivos sobre a matéria, distorção que já existia no ano passado, mas que se agrava este ano.

Perceção sobre agentes de ameaça mais relevantes em 2020, 2021 e perspetivando 2022*

2020			2021			Ordenação		Perspetivando 2022**		
RK	Tipo	%	RK	Tipo	%	Tend./ pp	Lugar RK	Tipo	%	Tend./RK 2021/2022
1º	Cibercriminosos	89	1º	Cibercriminosos	93	+ 4	=	Cibercriminosos	92	=
2º	Hacktivistas	50	2º	Hacktivistas	57	+ 7	=	Atores estatais	62	+
3º	Ameaças internas	48	3º	Atores estatais	43	+ 9	+	Ciberterroristas****	50	+
4º	Script kiddies	36	4º	Ciberterroristas****	32	+ 5	+	Hacktivistas	46	-
5º	Atores estatais	34	5º	Script kiddies	29	- 7	-	Empresas	27	+
6º	Ciberterroristas****	27	6º	Ameaças internas	21	- 27	-	Ameaças internas	23	=
7º	Empresas	5	7º	Cyber-offender ***	21	N/A	N/A	Script kiddies	19	-
8º	Outro(s)	2	8º	Empresas	11	+ 6	-	Cyber-offender	19	-
9º			9º	Outro(s)	0	- 2	-	Outro(s)	0	=

*Múltiplas respostas possíveis.
** 67% capazes de identificar em 2020 e 61% em 2021. Perspetivando 2022, respondem 57%.
*** Nova categoria introduzida apenas este ano.
**** Dada a mediatização de algumas ações destes agentes e a dificuldade que persiste na sua identificação em termos operacionais, a perceção sobre os ditos, mesmo entre especialistas, pode não coincidir com outras fontes e dados empíricos deste Relatório. O capítulo "Agentes de Ameaça relevantes para o ciberespaço de interesse nacional" procura apresentar uma hierarquização com base em todos os dados disponíveis.

Tabela 29 | CNCS

Quando questionados sobre as tecnologias emergentes que representam um maior desafio para a cibersegurança em 2021, a Computação em Nuvem e a Internet das Coisas foram as mais selecionadas. Perspetivando 2022, é notória a importância acrescida dada ao 5G, apesar daquelas duas continuarem a ser consideradas as mais desafiantes.

Perceção sobre as tecnologias emergentes que representaram um desafio maior para a cibersegurança, em 2021 e perspetivando 2022*

	2021**		2022		
RK	Tipo	%	Tipo	%	Tend./RK 2021/2022
1º	Computação em Nuvem	85	Internet das Coisas	80	+
2º	Internet das Coisas	74	Computação em Nuvem	78	-
3º	Inteligência Artificial	35	5G	61	+
4º	5G	22	Inteligência Artificial	52	-
5º	Computação Quântica	13	Computação Quântica	28	=
6º	Nenhuma	0	Nenhuma	0	=

*Múltiplas respostas possíveis.
**Não se efetuam comparações com o inquérito do ano passado porque a formulação da pergunta alterou ligeiramente.

Tabela 30 | CNCS

Por fim, questionados sobre o nível de capacitação do ciberespaço de interesse nacional comparativamente ao ano anterior, 48% dos inquiridos responderam que consideram que o ciberespaço está mais capacitado (mais 3 pp do que no anto anterior), 41% que está igualmente capacitado (mais 6 pp do no ano anterior) e apenas 7% afirmam que está menos capacitado (menos 5 pp do que em 2020).

Em termos de resiliência a ciberataques, em 2020 e 2021, o ciberespaço de interesse nacional está:

	2020	2021	Tend./pp.
Mais capacitado	45%	48%	+3
Igualmente capacitado	35%	41%	+6
Menos capacitado	12%	7%	-5
Não sei	8%	4%	-4

Tabela 31 | CNCS

Destaques

Verifica-se, entre a comunidade de entidades com protocolos de colaboração com o CNCS, uma perceção de que o risco de alguma entidade sofrer um incidente de cibersegurança em Portugal aumentou em 2021, para 98% dos inquiridos, mais 4 pp do que em 2020. A pandemia teve menos influência nesta perceção do que no ano anterior. Perceciona-se que em 2022 este risco continuará a subir, para 87% dos inquiridos.

Para esta comunidade, o *phishing*, o *ransomware* e a engenharia social são os tipos de ciberameaças percecionados como os mais relevantes em 2021, com particular subida do *ransomware*, o qual também ganha relevância quando se perspetiva 2022.

Os agentes de ameaça percecionados como os mais relevantes são os cibercriminosos, os hacktivistas e os atores estatais, sendo que estes últimos adquirem importância acrescida comparando com 2020 e perspetivando 2022.

As tecnologias emergentes percecionadas como as mais desafiantes para a cibersegurança são a Computação em Nuvem e a Internet das Coisas. Quando se perspetiva 2022, o 5G adquire um crescendo de notoriedade.

Para 48% dos inquiridos o ciberespaço está mais capacitado face ao ano anterior.

AGENTES DE AMEAÇA RELEVANTES PARA O CIBERESPAÇO DE INTERESSE NACIONAL

Um incidente de cibersegurança remete, na vasta maioria das ocasiões, para uma ação hostil dinamizada por um agente de ameaça que cumpre às instâncias competentes identificar, antecipar preventivamente e responsabilizar. O já longo histórico de prossecução de agentes de ameaça permitiu, à escala nacional e internacional, a conceptualização dos mesmos em blocos tipológicos definidos, sendo a delimitação dessas atribuições decorrente de vetores essenciais como a identidade, as motivações, o comportamento operacional e a sofisticação técnica dos atacantes.

A aplicação deste género de exercício a Portugal faz-se neste Relatório tendo como ponto de partida os dados estatísticos disponíveis quanto ao tipo de incidentes, mas também os contributos através de entrevistas e envio de conteúdos por parte dos diversos parceiros na realização deste documento. Considerados os principais agentes, faz-se uma seleção dos incidentes e indicadores de cibercrime nacionais mais importantes (considerando os dados apresentados na primeira parte deste Relatório) e cruzam-se os mesmos com a tipologia de agentes principais identificados, compondo um quadro compreensivo das ameaças ao ciberespaço de interesse nacional. Esta matriz tem uma representação gráfica (quadro 1) no início deste Relatório, no tópico "Análise Global" do Sumário Executivo.

Durante 2021, e perspetivando 2022, mantiveram-se como relevantes os mesmos tipos de agentes de ameaça identificados em 2020: os cibercriminosos e os atores estatais com um maior destaque, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas.

A. Cibercriminosos

O que são:

Em geral, os cibercriminosos caracterizam-se por ser indivíduos ou grupos que agem ilicitamente com o objetivo de obter ganhos financeiros. Com frequência, a sua constituição configura formas de crime organizado *online*. Poderá, em caso pontuais, ocorrer uma comunhão de interesses ou de oportunidades entre Estados e cibercriminosos, passando os segundos a atuar como *proxies* operacionais a favor de um Estado diretor.

O que fazem:

No ciberespaço de interesse nacional, os cibercriminosos tiveram e continuam a ter uma atividade relativamente intensa. As suas ações procuram, em particular, a cifragem extorsionista de sistemas e de infraestruturas informáticas, a captura de dados sensíveis, como dados bancários e de credenciais de acesso a contas, e a realização de fraudes/burlas, além de outras metodologias de extorsão. O *phishing* (bem como as variantes de *smishing* e *vishing*) é um dos vetores de ataque mais utilizados por estes agentes para a implementação de acessos remotos encobertos ou para a captura de informação sensível, dirigindo-se sobretudo a cidadãos ou utilizadores profissionais e utilizando temáticas diversas, como as ligadas à Banca ou a Serviços Postais.

Alguns destes ataques resultam em comprometimentos de contas, nomeadamente quando são capturadas credenciais de acesso. O *ransomware* também é um dos resultados das ações destes agentes de ameaça com cada vez maior impacto. Este *malware*, que cifra a informação das vítimas sob um pedido de resgate para a sua recuperação, pode ser instalado em dispositivos através de *emails* ou mediante a exploração de vulnerabilidades nos sistemas, por exemplo. Esta ameaça atinge principalmente organizações e não indivíduos.

Um outro tipo de prática muito comum entre os cibercriminosos é a fraude e a burla *online*. Muitos dos casos registados pelo Gabinete Cibercrime, pela CNPD, pela DGPJ ou pela APAV, por exemplo, são deste tipo. Em geral, implicam um dano patrimonial na vítima e uma simulação fraudulenta de uma marca ou de uma pessoa (por exemplo, um comprador ou um vendedor), que conduz a vítima a um engodo (por exemplo, a transferência de dinheiro para o agente criminoso). É notório um crescente número de casos relacionados com páginas falsas de marcas conhecidas ou de investimentos em criptomoedas.

Durante 2021, verificou-se ainda que estes agentes de ameaça intensificaram as suas ações de reconhecimento de vulnerabilidades nas infraestruturas nacionais para posterior exploração e realização de intrusões e/ou a instalação de *malware*, algo a que não é alheia a identificação de diversas vulnerabilidades importantes em 2021.

Quem atingem:

Os cibercriminosos, em Portugal, atingem sobretudo os setores da Banca, da Saúde e da Educação/Ensino Superior, bem como as PME e os cidadãos em geral.

B. Atores Estatais

O que são:

Por atores estatais entendem-se agentes de ameaça que atuam sob a direção estratégica e/ou direta de um Estado, sendo um escopo tradicionalmente composto por coletivos de operadores a atuarem na proximidade de serviços de informações ou diretamente integrados nas suas estruturas orgânicas. Estes agentes de ameaça executam ações hostis no ciberespaço a favor dos preceitos estratégicos do seu Estado e em evidente correlação com os desígnios programáticos das sua política externa, militar ou económico-financeira. Alguns destes agentes de ameaça são designados de "ameaças persistentes avançadas" (APT, no acrónimo em inglês).

Na vasta maioria dos eventos observados, as atividades de atores estatais concentram-se na execução de operações de ciberespionagem, orientadas para o comprometimento persistente e encoberto de infraestruturas informáticas detentoras de informação sensível ou de valor estratégico que pretendem exfiltrar de forma não detetada e recorrente. A estas ações de ciberespionagem acrescem casos, com menor expressão quantitativa, mas de elevada gravidade, correlacionados com atos de cibersabotagem, com o fito de causarem disrupção holística ou setorial em alvos externos.

Num número crescente de ocasiões estas ações cibernéticas hostis são, também, dinamizadas por Estados, à escala global, em benefício da sua política doméstica, da sua projeção global ou no âmbito de operações mais latas de natureza híbrida, onde ciberataques concorrem para o sucesso de estratégias de vasto escopo que incluem também, por exemplo, linhas de atuação no domínio da propaganda e da desinformação para a disrupção da normalidade democrática das sociedades.

O que fazem:

A materialização desta ameaça no ciberespaço de interesse nacional ocorre em moldes coincidentes com o observado ao longo de todo o espaço comunitário e transatlântico, observando-se o empenho de uma crescente variedade de metodologias ofensivas com vista ao comprometimento das suas vítimas institucionais, tradicionalmente adstritas ao setor público e às áreas de soberania.

Tratando-se de atores oportunistas que prezam a anonimização da sua identidade e natureza funcional, os atores estatais privilegiam, cada vez mais, o empenho de metodologias ofensivas generalistas, desprovidas de uma assinatura de propriedade exclusiva, sendo, hoje, recorrente observar-se o recurso a métodos operacionais coincidentes com os empe-

nhados por agentes da cibercriminalidade ou do hacktivismo. Entre estes destacam-se o uso de *phishing* e spear *phishing*; a criação de domínios próximos do âmbito governamental para favorecer o typosquatting e o acesso a sites fraudulentos; bem como ações de reconhecimento e de mapeamento de vulnerabilidades para posterior exploração.

Quem atingem:

Os atores estatais procuram atingir vítimas detentoras de acessos ou de informação com reconhecido valor estratégico. Estas vítimas tendem a ser, na vasta maioria das ocasiões, de natureza público-governamental, não se devendo, contudo, desconsiderar a gravidade desta tipologia de ciberameaças contra alvos privados, nomeadamente infraestruturas críticas e serviços essenciais.

C. Ameaças Internas Negligentes

O que são:

A ameaça interna diz respeito a um agente que compromete a cibersegurança de uma organização a partir do seu interior. Este comprometimento pode ser voluntário (por vingança ou dinheiro, por exemplo); resultado de um condicionamento (por efeito de chantagem sobre um colaborador, por exemplo); ou negligente (quando um trabalhador, involuntariamente, compromete a sua organização através de um comportamento descuidado, como a partilha de credenciais em resultado de um *phishing*).

O que fazem:

Ainda que os outros tipos de ameaça interna possam existir em Portugal, a negligente é particularmente relevante, na medida em que resulta dos casos em que alguém clica num *link* ou anexo maliciosos ou partilha credenciais de acesso a contas, colocando em causa, sem o desejar, a segurança da informação da sua organização. Também inclui outras ações de engenharia social, como através de telefone, no sentido de permitir acessos remotos ou instalação de *malware* nos dispositivos de uma entidade. Este agente não atua isoladamente, é instrumentalizado por outros agentes de ameaça, como os cibercriminosos ou os atores estatais.

O comprometimento de contas, privilegiadas ou não, é uma das consequências mais notórias deste tipo de agente de ameaça, quer porque este não utiliza uma palavra-passe suficientemente forte e é descoberta por força-bruta ou tentativa-erro, quer porque a mesma é revelada através de um ataque de *phishing* ou de uma exfiltração de dados. Alguns agentes de ameaça conseguem comprometer também o

múltiplo fator de autenticação, através, por exemplo, de SIM *swapping*, quando o *smartphone* serve esse propósito.

Quem atingem:

Este tipo de agente de ameaça é constituído sobretudo por colaboradores de organizações, nomeadamente da Administração Pública ou de operadores de serviços essenciais quando os alvos são mais dirigidos, mas virtualmente qualquer organização quando os ataques são generalizados.

D. Cyber-offenders

O que são:

Os *cyber-offenders* dizem respeito aos agentes de ameaça que atuam com motivações pessoais, frequentemente de contornos passionais ou reputacionais. Correspondem sobretudo a indivíduos, e não a grupos, que agridem, perseguem ou prejudicam outros indivíduos de forma criminosa *online*. Quando alguns grupos atuam com intuitos meramente destrutivos podem caber do ponto de vista motivacional neste tipo de agente de ameaça.

O que fazem:

Estes indivíduos realizam ações como o *stalking* (perseguição), a *sextortion* ou o discurso de ódio *online*, registados, por exemplo, pelo Gabinete Cibercrime da PGR, ou a difamação e injúrias, as ameaças, o *cyberbullying*, a violência doméstica, ou outras ações várias com contornos de abuso sexual, presentes nos dados partilhados pela APAV. Este domínio nem sempre é captado pelos registos de incidentes de cibersegurança ou pelos indicadores de cibercrime, principalmente porque nem sempre são registados como tendo caráter digital, ainda que ocorram no ciberespaço.

Quem atingem:

Os *cyber-offenders* podem atingir qualquer cidadão, na medida em que atuam no âmbito das interações sociais quotidianas.

E. Hacktivistas

O que são:

Os hacktivistas são grupos organizados, de modo formal ou informal, que desenvolvem atividades no ciberespaço com o objetivo de realizar afirmações ideologicamente orientadas. Portanto, não atuam com objetivos económicos ou geopolíticos. Por vezes, confundem-se nas suas motivações com aspetos ligados à reputação e exibição, alguns deles mais próprios da categoria de *cyber-offender*.

O que fazem:

Em Portugal, em 2021, os hacktivistas mantêm um volume de atividade irregular, cuja intensidade depende muito do ciclo de vida de cada novo grupo. As suas ações conduziram sobretudo à realização de *defacement*s com o fim de interferir com a reputação *online* de instituições consideradas relevantes para a transmissão de uma mensagem. Algumas das suas atividades podem também procurar a exfiltração e a exposição de dados. Tradicionalmente, estes agentes de ameaça costumam usar a negação de serviço distribuída com o fim de prejudicar a reputação das instituições alvo.

Quem atingem:

Os alvos mais comuns dos hacktivistas são a Administração Pública e os Órgãos de Soberania, bem como entidades ou pessoas com peso institucional em função da afirmação ideológica que pretendem realizar.

DESTAQUES

Em Portugal, os tipos de agentes de ameaça mais relevantes são os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas.

Os cibercriminosos utilizam em particular o *phishing*/*smishing*/*vishing*, o *ransomware* e a fraude/burla *online* como métodos para atingir os seus objetivos; os atores estatais, em Portugal, realizam ataques de *phishing* e *spear phishing* e procuram o comprometimento de contas, bem como a exploração de vulnerabilidades para a realização de intrusões.

TENDÊNCIAS

No que diz respeito às principais tendências, apresenta-se de seguida uma perspetiva sobre as tendências internacionais com potencial impacto no país, bem como uma análise às principais prospetivas para o ciberespaço de interesse nacional para 2022 e 2023.

AMEAÇAS INTERNACIONAIS COM POTENCIAL DE IMPACTO EM PORTUGAL

O contexto pandémico continua a ser explorado por agentes de ameaça com o objetivo de desenvolverem operações de cibercrime e campanhas de ciberespionagem em vários domínios, visando a obtenção de proveitos financeiros e a exfiltração de dados pessoais, informação sensível, credenciais de acesso, propriedade intelectual, industrial e comercial. Os atores estatais e os cibercriminosos permanecem como os principais agentes de ameaça no desenvolvimento de operações ofensivas no ciberespaço contra cidadãos e entidades públicas e privadas.

Em 2021, os ataques de *ransomware* tiveram, à escala global, um crescimento substancial contra vários setores de atividade, tendo sido observado, em diversas situações, que os atacantes conseguiram aceder e perturbar temporariamente o funcionamento de infraestruturas críticas, particularmente do setor energético.

Com o agravamento de tensões geopolíticas e de conflitos entre alguns Estados, determinados atores estatais continuam a desenvolver campanhas de ciberespionagem para aceder a informações sensíveis, bem como a desencadear operações no ciberespaço para sabotar, desestabilizar e afetar a credibilidade de entidades e indivíduos a nível global, e particularmente em países do espaço Euro-Atlântico.

1. Tendências identificadas:

Intensificação da exploração dos ciberataques no contexto da confrontação híbrida

Os ciberataques têm continuado a ser uma ferramenta relevante em contextos de confrontação híbrida, em diferentes geografias. O leque de opções para causar perturbações em tempos de paz ou guerra apresenta-se variado, desde as ex-

filtrações de dados e publicação na Internet (*hack & leak*), o comprometimento de sistemas de controlo industrial ou de infraestruturas críticas, os ataques de DDoS, até aos ataques que visam a destruição de dados de organizações.

A investigação aos incidentes, e a sua imputação, tende a continuar a ser dificultada pela maior sofisticação de alguns atacantes, tanto os que contam com apoio estatal, como os ligados ao cibercrime. Por outro lado, a existência de diferentes normativos nacionais para regular a atividade criminal no ciberespaço tende a criar dificuldades para estabelecer bases de cooperação entre países, ainda que mitigada, pelo menos na UE, por um ímpeto regulatório que, a tempo, tenderá a proporcionar interoperabilidade neste domínio.

Cadeias de fornecimento continuam a ser visadas por cibergrupos sofisticados

Desde 2020 que tem aumentado a frequência dos ataques que usam cadeias de fornecimento para aceder aos sistemas de clientes, por um lote estrito de cibergrupos com mais recursos e conhecimentos. O ataque à fornecedora de serviços de Tecnologias de Informação Kaseya, pelo grupo de *ransomware* REvil, em julho de 2021, foi demonstrativo da forma como os atacantes podem explorar as dependências de serviços informáticos para extorquir ou causar outros danos em clientes. Fornecedores de produtos/serviços via *cloud*, gestoras de serviços partilhados e operadoras de telecomunicações/Internet têm sido os principais alvos destes ataques, ao permitirem aceder a um maior número de vítimas. O ataque à empresa de *software* Solarwinds, que marcou 2020, mas cujos efeitos se estenderam para 2021, também se integrou neste tipo de metodologia que interfere nas cadeias de fornecimento.

Estes ataques tendem a beneficiar do contexto pandémico, pelo facto de mais organizações estarem a depender de serviços digitais para assegurar o trabalho remoto e devido aos confinamentos de equipas de trabalho, aumentando os riscos de falhas operacionais.

Vulnerabilidades descobertas em 2021 com potencial de exploração posterior

A 9 de dezembro de 2021, uma equipa de segurança do grupo Alibaba detetou uma falha se segurança crítica no *software* «Log4j» (usada para configurar *logs* de aplicações), que permitia a um atacante executar código remoto e assumir o controlo de sistemas, tendo a vulnerabilidade (“Log4Shell”) sido corrigida num *patch* disponibilizado a 18 de dezembro de 2021. O caso acresce a duas outras vulnerabilidades críticas detetadas, também em 2021, no programa de *emails* da Microsoft «Exchange Server» (“ProxyLogon” e “ProxyShell”).

Estas vulnerabilidades têm sido exploradas por um lote alargado de *hackers* desde que foram tornadas públicas, identificando-se potencial para estes terem instalado *malware* nos dispositivos das vítimas para garantir persistência de acesso (mesmo depois de instalados os *patches*) – o que obriga à adoção de medidas de monitorização adicionais. A "Log4j" integra a programação de base de um leque diverso de outras aplicações (bancos, serviços públicos, Tecnologias de Informação, etc.), incluindo aplicações asseguradas por fornecedores, o que eleva o potencial de o incidente ter um número de vítimas muito alargado.

Dispersão dos ataques *ransomware* por pequenos operadores do cibercrime

A comercialização de diferentes serviços de *ransomware* (*Ransomware*-as-a-Service - RaaS) tem prosperado na pandemia, sendo crescente a procura por "licenças" de uso destes serviços por operadores individuais e o surgimento de novos grupos de *ransomware*. O RaaS aumenta a monetização para os grupos organizados que vendem estes serviços.

Considera-se que o RaaS deverá continuar a atrair operadores, motivados pela perspetiva de monetização, alimentada pelos casos de empresas que continuam a aceitar pagar os resgates. Outras tendências prendem-se com a crescente relevância dos *access brokers* (que vendem acessos a sistemas comprometidos) e a maior frequência dos ataques de tripla e quádrupla extorsão (adoção de procedimentos adicionais para pressionar as vítimas a pagar, como a negação de serviços, o *leak* de dados, o acesso a redes de clientes, etc.).

Autoridades procuram robustecer as respostas aos ciberataques

Tem sido observado um esforço de diversos países na organização das respostas aos ciberataques, através de uma toolbox de diferentes medidas. Estima-se que, com maior frequência, diferentes autoridades deverão assumir respostas crescentemente multifacetadas contra os agentes da ameaça, ao mesmo tempo que poderá verificar-se um esforço de maior articulação e cooperação entre países neste domínio. A revisão da 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 dos sistemas de informação em toda a UE, também poderá significar a criação de mais mecanismos de prevenção e resposta a ciberataques.

2. Indicadores de incidentes e cibercrime internacionais em 2021

Complementando a informação apresentada no tópico anterior, é possível identificar em alguns documentos de organizações internacionais um conjunto de ameaças que assolaram 2021, nomeadamente em relatórios da Agência da União Europeia para a Cibersegurança (ENISA), da Europol e do Fórum Económico Mundial (WEF). Nestas fontes, o *ransomware* surge de forma transversal como problema importante. De destacar também as práticas relacionadas com a engenharia social e as ameaças através do *email*, como o *phishing*. Qualquer destas fontes refere que 2021 manteve a tendência do ano anterior de aumento dos incidentes de cibersegurança, dos indicadores de cibercrime e dos riscos associados a estas ameaças, como é possível verificar no quadro que se segue.

Tendências das principais ameaças ao ciberespaço segundo relatórios internacionais

Fonte	*Threat Landscape 2021* **ENISA (2021)**	*Internet Organised Crime Threat Assessment 2021* **Europol (2021)**	*Global Cybersecurity Outlook 2022* **WEF (2022)**
Ameaças	_ Ransomware _ Malware _ Cryptojacking _ Ameaças relacionadas com o *email* _ Ameaças contra dados _ Ameaças à disponibilidade e à integridade _ Desinformação _ Ameaças não maliciosas _ Ataques às cadeias de fornecimentos	_ Ransomware _ Mobil malware _ DDoS com intuitos de monetarização _ Pornografia infantil *online* _ Fraudes em compras *online* _ Phishing e engenharia social _ Fraudes relativas a investimentos, BEC/CEO Fraud e com cartões de crédito	_ Ransomware _ Engenharia social _ Ameaça interna
Tendência	"Cybersecurity attacks have continued to **increase** through the years 2020 and 2021, not only in terms of vectors and numbers but also in terms of their impact." (p. 7)	"Ransomware continues to dominate and **proliferate**" (p. 20); "the number of mobile malware reports to law enforcement has **increased** significantly" (p. 23); "Investment fraud has become a significant concern, as phishing and social engineering have further **increased** to generate considerable criminal proceeds." (p. 28); "The shift from physical shopping to e-commerce has further led to an **increased** criminal focus on e-skimming" (p. 33); "Web marketplaces for the sale of illicit goods and services has **increased**" (p. 36)	"The threat of ransomware continues to **grow**" (p. 14); "As digitalization continues to proliferate and new technologies are introduced cyber risk will inevitably **grow**" (p. 29)

Quadro 3 | ENISA, Europol e WEF

Destaques

Em 2021, a nível internacional, destacam-se alguns aspetos que têm potencial impacto em Portugal: incremento das ameaças híbridas; persistência de ataques às cadeias de fornecimento; descoberta de vulnerabilidades relevantes e posterior exploração por agentes de ameaça; proliferação de ataques de *ransomware*; tentativa de resposta comum ao nível dos Estados.

Relatórios da ENISA, da Europol e do WEF são unânimes no destaque dado ao *ransomware*, aos ataques que aproveitam as vulnerabilidades do fator humano e ao reconhecimento de um aumento generalizado dos incidentes, do cibercrime e dos riscos no ciberespaço internacional.

PROSPETIVAS PARA O CIBERESPAÇO DE INTERESSE NACIONAL EM 2022/2023

Considerando os dados e os contributos disponíveis, neste tópico elencam-se algumas prospetivas consideradas plausíveis para 2022 e 2023 no âmbito da cibersegurança em Portugal. Um exercício de prospetiva como este é acompanhado por um elevado nível de incerteza, fruto do caráter dinâmico da realidade e do contexto atual.

Níveis de incerteza próprios do contexto pandémico a serem substituídos pelas incertezas do contexto de conflito na Ucrânia, iniciada no primeiro trimestre de 2022, e a emergência de ameaças híbridas, nomeadamente a possibilidade de ações próprias de atores estatais, como a sabotagem e disrupção de serviços da Administração Pública, dos Órgãos de Soberania e dos operadores de serviços essenciais.

Continuidade de ameaças ligadas à exploração das fragilidades do fator humano, como o *phishing* e o *spear phishing*, e variadas formas de burla *online*, com tendência para, no âmbito em particular do cibercrime, crescer com estes fins a utilização das redes sociais e das plataformas de vendas *online*, bem como o uso de temas ligados às criptomoedas.

Manutenção do crescimento dos casos de *ransomware*, quer para dupla extorsão (ameaça de destruição e divulgação), quer de outras formas de ameaça a acompanhar cada caso.

A exploração de violações de dados com credenciais de acesso, bem como o comprometimento de contas através dessa exposição ou outras formas de captura de credenciais, tenderá a ser um modo de intrusão e exfiltração com potencial de impacto negativo na proteção de dados pessoais e sensíveis.

Crescente exploração de vulnerabilidades técnicas em sistemas, por exemplo, para ataques às cadeias de fornecimento, com o objetivo de realizar intrusões e instalar *malware*.

Maior rapidez dos agentes de ameaça na exploração de vulnerabilidades *zero-day* antes da possibilidade de se concretizarem as respetivas correções através de atualizações (por exemplo, casos crescentes de *bug bounties* em que, apesar da entidade em causa ser avisada da vulnerabilidade, a mesma também é partilhada com cibercriminosos).

Crescente relevância das tecnologias móveis, como os *smartphones*, e de dispositivos da esfera da Internet das Coisas, enquanto superfícies de ataque, devido à sua intensa utilização individual, menor fronteira entre usos privados e usos profissionais e cultura de segurança menos madura do que noutros dispositivos.

Destaques

Em termos de prospetivas para o ciberespaço de interesse nacional em 2022 e 2023, destaca-se o seguinte: o contexto de conflito na Ucrânia com potencial de impacto para o ciberespaço de interesse nacional, nomeadamente no que diz respeito à ação de atores estatais; continuidade na exploração das fragilidades do fator humano; crescimento dos casos de *ransomware*; violações de dados para uso de credenciais de acesso; continuidade da exploração de vulnerabilidades; exploração em particular de vulnerabilidades *zero-day*; relevância das tecnologias móveis como superfícies de ataque.

Síntese do Capítulo Ameaças e Tendências, em 2021

Verifica-se um aumento na perceção de risco de alguma entidade sofrer um incidente de cibersegurança em 2021, de acordo com o inquérito à comunidade de entidades com protocolo de colaboração com o CNCS – no entanto, os inquiridos consideram que o ciberespaço está mais capacitado.

Os tipos de ciberameaças consideradas mais relevantes por estas entidades são o *phishing*, o *ransomware* e a engenharia social. Os agentes de ameaça tidos como mais importantes são os cibercriminosos, os hacktivistas e os atores estatais.

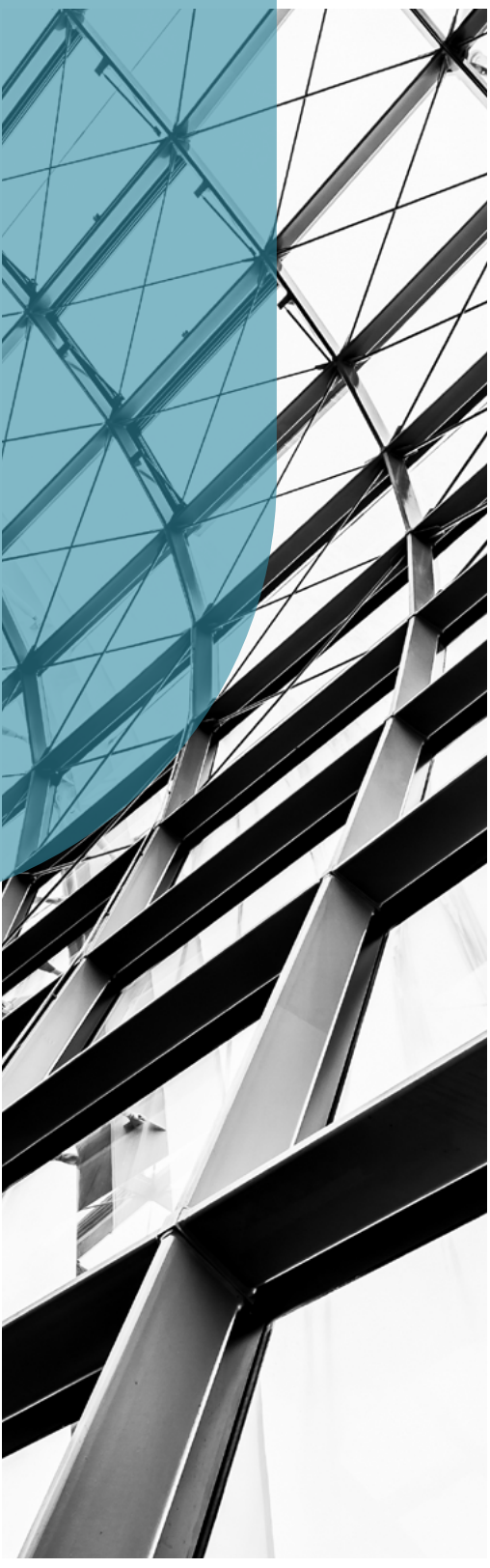
Efetivamente e não apenas ao nível das perceções, os tipos de agentes de ameaça mais significativos em Portugal durante 2021 e perspetivando 2022 são os cibercriminosos e os atores estatais, seguidos da ameaça interna negligente, dos *cyber-offenders* e dos hacktivistas.

Os cibercriminosos tendem a utilizar como técnicas de ataque o *phishing*/*smishing*/*vishing*, o *ransomware* e a fraude/burla *online*, enquanto entre os atores estatais predomina o uso do *phishing* e do *spear phishing*, o comprometimento de contas e a exploração de vulnerabilidades com o fim de realizar intrusões.

A nível internacional, assiste-se a um aumento dos incidentes e do cibercrime e a um conjunto de tendências com potencial impacto em Portugal, como as ameaças híbridas, os ataques à cadeia de fornecimento, a exploração de vulnerabilidades e o *ransomware*.

A nível nacional, perspetiva-se para 2022 e 2023 como possíveis tendências o incremento de ações de atores estatais no contexto de conflitos internacionais, a continuação da exploração do fator humano, a persistência dos casos de *ransomware*, o comprometimento de contas em resultado de violações de dados, a exploração de vulnerabilidades e a crescente importância das tecnologias móveis como superfícies de ataque.

Relação com as seguintes linhas de ação da ENSC: E2 a, E2 c, E2 r, E2 s, E3 b, E4 b e E4 h (ver anexo).



E. BRIEFING DA ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO

O contributo deste Relatório para o acompanhamento da ENSC reveste-se de um caráter distinto de outros Relatórios, como o relativo ao tema Sociedade de 2021, visto os indicadores de incidentes e de cibercrime estarem associados a muitas dinâmicas exógenas. Além disso, os dados e as análises aqui apresentadas, enquanto resultados, dizem respeito sobretudo ao contexto de ameaça que as ações da ENSC enfrentam e menos às ações concretas empreendidas pelas entidades que executam a ENSC. Não obstante, muitas das linhas de ação materializam-se em grande medida na realização deste documento, pois trata-se de um Relatório que resulta da qualidade da cooperação entre entidades que são chamadas à concretização da ENSC através do respetivo Plano de Ação.

O tema abrangido pela linha de observação Riscos e Conflitos inclui pelo menos três eixos da ENSC: o Eixo 2 - Prevenção, educação e sensibilização; o Eixo 3 - Proteção do ciberespaço e das infraestruturas; e o Eixo 4 - Resposta às ameaças e combate ao cibercrime (E2 a, E2 c, E2 r, E2 s, E3 b, E3 c, E4 b, E4 f, e E4 h – ver anexo). Em geral, as várias linhas de ação integradas nestes eixos que se relacionam com o presente documento dizem respeito à promoção da cooperação entre entidades para partilha de informação e identificação das principais ameaças. Do ponto de vista da promoção da coordenação entre entidades e da produção de conhecimento sobre ameaças, o Relatório sobre o tema Riscos & Conflitos de 2022 é, ele próprio e o processo que o precede, um exemplo de concretização das linhas de ação orientadas a estes propósitos. Este é um documento que resulta da colaboração entre

entidades para a partilha de informação e produção de um quadro de ameaças comum.

Não obstante, o volume de incidentes de cibersegurança e os indicadores de cibercrime continuam a apresentar uma tendência crescente. O aumento que se tem verificado nos últimos anos resulta, em parte, de diversos fatores exógenos, como referido: o contexto internacional ou a adoção de novos processos de trabalho alicerçados na esfera digital provocada pela pandemia. Eventualmente, algum crescendo seria inevitável, pese embora os esforços das autoridades no sentido de prevenir ou reagir a incidentes de cibersegurança. Ainda assim, é uma tendência negativa quanto ao impacto da ENSC que deve ser considerada, nomeadamente tendo em conta a capacidade de as atividades previstas em Plano de Ação da ENSC fazerem face ao número de incidentes e de cibercrimes registados. Portanto, é importante reforçar os processos no sentido de prevenir com mais eficácia os incidentes de cibersegurança, em última análise o objetivo da ENSC e deste Relatório.

F. RECOMENDAÇÕES E RECURSOS

RECOMENDAÇÕES GERAIS	Formar os profissionais com responsabilidades a nível técnico para a necessidade de ativarem a conservação de registos (*logs*) de serviços na Internet para análise após a eventual ocorrência de incidentes, por um período mínimo de 6 meses, preferencialmente um ano; Formar as chefias das organizações em vários aspetos ligados à cibersegurança, em particular para a importância do Regime Jurídico da Segurança do Ciberespaço e respetiva regulamentação; Promover junto dos indivíduos em geral a denúncia de incidentes e cibercrimes por forma a melhor monitorizar estas atividades e contribuir para a realização de investigações.

Quadro 4 | CNCS

Ciberameaças principais	RECOMENDAÇÕES POR CIBERAMEAÇA	
	Comportamento individual	**Comportamento organizacional**
Phishing/ Smishing	Não clicar em *links* ou anexos de *emails* ou SMS suspeitos, verificar a origem dos *emails*, não partilhar dados sensíveis solicitados por *email*, confirmar noutras fontes os pedidos de transferências bancárias	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, realizar simulações de *phishing* e aplicar as melhores práticas e *standards* de segurança ao nível da configuração do *email* organizacional, no âmbito de políticas de segurança definidas
Ransomware	Aplicar as recomendações relativas ao *phishing,* salvaguardar cópias de segurança em localização secundária e desconectada da rede, manter o antivírus atualizado, evitar navegar em *websites* sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida	Formar os colaboradores relativamente às recomendações relativas ao *phishing* e *email,* salvaguardar cópias de segurança em localização secundária e desconectada da rede, manter o antivírus atualizado, evitar navegar em *websites* sem garantias de segurança, não utilizar dispositivos USB de origem desconhecida, ações monitorizadas por políticas de segurança definidas
Fraude/Burla *online*	Desconfiar de ofertas demasiado boas para serem verdade, não partilhar dados sensíveis em plataformas não reconhecidas, não transferir dinheiro sem verificar noutras fontes o destino e essa necessidade, desconfiar de solicitações por	Desenvolver ações de sensibilização contra a engenharia social junto dos colaboradores, garantir que os colaboradores confirmam o destino e a necessidade das transferências bancárias solicitadas, utilizar carteiras virtuais ou

	parte de terceiros de alterações das configurações de aplicações como a MBway, utilizar carteiras virtuais ou cartões temporários nos pagamentos *online*, verificar a veracidade dos *websites* de vendas e privilegiar aqueles que utilizam HTTPS	cartões temporários nos pagamentos *online* a fornecedores, verificar a veracidade dos *websites* de fornecedores e privilegiar aqueles que utilizam HTTPS
Comprometimento de contas ou tentativa	Utilizar palavras-passe fortes e alterá-las sempre que se suspeite de comprometimento, aplicar as recomendações relativas ao *phishing*, aplicar o múltiplo fator de autenticação	Aplicar de forma contínua as políticas de segurança definidas quanto às palavras-passe em particular, promovendo o cumprimento de requisitos mínimos de dimensão e complexidade, monitorizar e bloquear ataques de força-bruta, registar os eventos, aplicar o múltiplo fator de autenticação
Vulnerabilidades e sua exploração	Manter os sistemas e as aplicações atualizadas com as últimas atualizações de segurança	Manter os sistemas e as aplicações atualizadas com as últimas atualizações de segurança de forma regular, ação monitorizada por políticas de segurança definidas

Quadro 5 | CNCS

Recursos do CNCS de suporte a estas recomendações	
Para indivíduos	**Para organizações**
MOOCs Cidadão Ciberseguro, Cidadão Ciberinformado, Consumidor Ciberseguro e Cidadão Cibersocial; Documentos de Boas Práticas	Quadro Nacional de Referência para a Cibersegurança; Roteiro para as Capacidades Mínimas em Cibersegurança; Cibercheckup; Webcheck; Referencial de Competências em Cibersegurança
Estes recursos podem ser encontrados no *website* do CNCS: https://www.cncs.gov.pt	

Quadro 6 | CNCS

G. NOTAS CONCLUSIVAS

O *Relatório Cibersegurança em Portugal - Riscos e Conflitos 2022* é marcado pela continuidade da pandemia em 2021, mas também pelas perspetivas futuras reconfiguradas pelos acontecimentos que ocorreram durante o primeiro trimestre de 2022, nomeadamente alguns ataques com impacto relevante no ciberespaço de interesse nacional e a invasão da Ucrânia por parte da Federação Russa.

É mais fácil caracterizar o passado do que perspetivar o futuro. Este Relatório tem esse duplo objetivo: procura perspetivar o futuro considerando tendências passadas e ter em conta as expetativas daqueles que direta e indiretamente contribuem para a elaboração deste documento. O contexto desta edição acarreta tantas incertezas como o contexto de 2020, ano em que surge a pandemia. Contudo, as incertezas do presente têm uma natureza diferente: por um lado, o contexto atual é menos singular do que a pandemia comparando com experiências do passado; por outro, é um contexto que acarreta desafios conhecidos, como as ameaças híbridas, que se podem revelar mais difíceis para a cibersegurança do que aqueles que foram colocados pela pandemia. Só o desenrolar dos acontecimentos futuros poderá clarificar esta questão.

Não obstante as incertezas que persistem, foi possível determinar a existência de algumas ameaças relativamente às quais existem formas de mitigação, também partilhadas neste Relatório e desenvolvidas em maior profundidade em vários conteúdos disponibilizados no *website* do CNCS. Um dos objetivos deste documento é precisamente fazer acompanhar a maior consciência sobre as principais ameaças de um conjunto de capacidades de prevenção e de reação adequadas. Para o efeito, é essencial que cada organização se capacite e que cada indivíduo siga as melhores práticas

de cibersegurança, independentemente da emergência de ameaças mais ou menos graves ou de acontecimentos globais com impacto nacional. Só numa lógica de investimento com efeitos a longo prazo e com o uso do princípio da precaução se pode ter alguma possibilidade de proteção num ciberespaço cada vez mais decisivo para o bem-estar social.

H. NOTAS METODOLÓGICAS

O presente Relatório é realizado através da combinação de dados disponíveis em fontes abertas, estatísticas e perspetivas partilhadas pelos parceiros e dados produzidos pelo CNCS. Com base nesta informação, apresenta-se uma leitura integrada destes vários elementos procurando ter uma visão panorâmica, considerando as redundâncias entre fontes e os potenciais impactos dos eventos. A identificação dos agentes de ameaça e das ciberameaças mais relevantes resultou deste método de compreensão transversal, procurando respeitar as taxonomias de origem, mas adaptando-as em alguns casos para uma leitura comum (a respeito dos agentes de ameaça, sem dados quantitativos inequívocos, os contributos qualitativos do Serviço de Informações de Segurança, do Serviço de Informações Estratégicas de Defesa, da PGR e da PJ foram essenciais, embora as opções metodológicas e conceptuais sejam da responsabilidade do CNCS). Para uma quantificação, estabeleceu-se uma pontuação com base no número de fontes que fazem referência a cada ameaça (de agentes e de ciberameaças). Em relação às ciberameaças, atribuiu-se também uma pontuação de 1 a 3 (baixo, médio e alto, respetivamente) relativamente ao potencial de impacto. A soma das menções (redundâncias) com o potencial de impacto produziu um *ranking* em que um maior número de pontos representa uma maior relevância de cada agente de ameaça e ciberameaça.

Os dados do CERT.PT resultam da sua própria atividade de registo e análise de incidentes, assente em notificações externas, identificação por via interna e fontes de observáveis. Os valores partilhados sobre os incidentes por parte da RNCSIRT são fruto de inquérito realizado pela própria RNCSIRT (com apoio do CNCS), entre os dias 1 e 21 de fevereiro de 2022, aos 52 membros desta rede, obtendo-se 29 respostas válidas. Os números da CNPD, da DGPJ, da PGR e da APAV foram partilhados por estas entidades no âmbito da parceria na realização do presente Relatório. O inquérito *Perceção de risco no ciberespaço de interesse nacional 2021/2022* foi realizado pelo CNCS de 3 a 21 de janeiro de 2022 aos pontos de contacto nas organizações com protocolo de colaboração com o CNCS, obtendo-se 46 respostas válidas. As restantes perspetivas relativas a ameaças e tendências foram elaboradas a partir dos contributos dos parceiros deste Relatório, através de entrevistas por videoconferência ou respostas por escrito a perguntas enviadas.

I. ENTIDADES PARCEIRAS

AP2SI - Associação Portuguesa para a Promoção da Segurança da Informação

APAV - Associação Portuguesa de Apoio à Vítima

Comando de Operações de Ciberdefesa

Comissão Nacional de Proteção de Dados

Direção-Geral da Política de Justiça

Direção-Geral de Estatísticas da Educação e Ciência

Direção-Geral de Política de Defesa Nacional

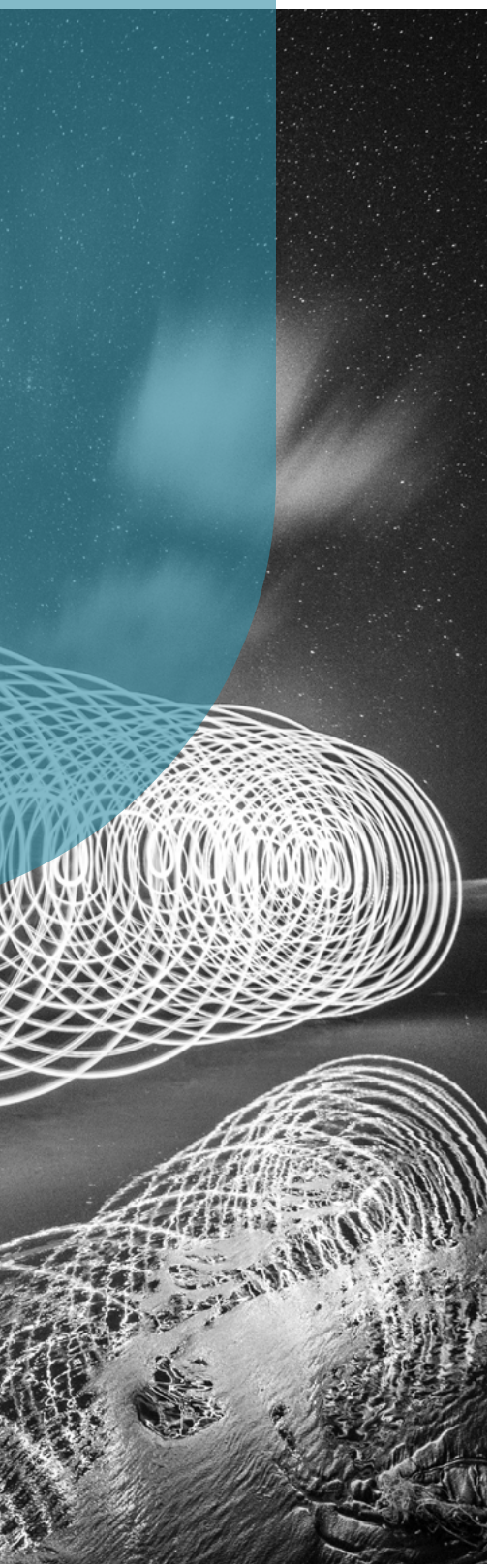
Gabinete Cibercrime da Procuradoria-Geral da República

Polícia Judiciária - Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T)

Rede Nacional de CSIRTs

Serviço de Informações de Segurança

Serviço de Informações Estratégicas de Defesa



J. O OBSERVATÓRIO DE CIBERSEGURANÇA DO CNCS

Um Observatório, por definição, analisa uma dada realidade com o objetivo de a tornar mais compreensível e, portanto, a ação em relação à mesma mais consciente e estratégica. 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 suportar a definição de políticas públicas. Com uma visão multidisciplinar, o Observatório de Cibersegurança sistematiza informação disponível ou promove a sua recolha nos domínios da Sociedade, Economia, Políticas Públicas, Ética e Direito, Riscos e Conflitos, bem como Inovação e Tecnologias Futuras.

Como modelo de governança, o Observatório de Cibersegurança funciona em duas esferas:

CONSELHO CONSULTIVO

> Constituído por académicos de cada uma das áreas científicas das Linhas de Observação, tem como missão avaliar, propor e discutir indicadores, pesquisas e produtos, bem como sugerir a elaboração de documentos e a realização de encontros. O Conselho Consultivo deve trabalhar como conjunto, mas, eventualmente, poderá ser dividido em grupos de trabalho setoriais. O Conselho Consultivo do Observatório de Cibersegurança: https://www.cncs.gov.pt/pt/observatorio/#conselho

PARCEIROS

> Numa lógica de envolvimento da comunidade, pretende criar-se relações no âmbito do Observatório de Cibersegurança com entidades da sociedade civil, com as quais se procura contactar e estabelecer parcerias. Estas entidades podem contribuir de três modos diferentes, dependendo das suas características, para o conhecimento sobre a cibersegurança em Portugal: produzindo estatísticas; desenvolvendo I&D; ou mediando a recolha de dados junto dos públicos-alvo.

Página do Observatório de Cibersegurança do CNCS: https://www.cncs.gov.pt/pt/observatorio/

K. TERMOS, ABREVIATURAS E SIGLAS

Ameaça: "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização."

(ISO/IEC 27032)

Ameaças híbridas: "embora as definições de ameaças híbridas variem e tenham de permanecer flexíveis para responder à sua natureza evolutiva, o conceito destina-se a abarcar a combinação de atividades coercivas com atividades subversivas, de métodos convencionais com métodos não convencionais (ou seja, diplomáticos, militares, económicos, tecnológicos) que podem ser utilizados de forma coordenada por intervenientes estatais ou não estatais para atingir objetivos específicos, mantendo-se, no entanto, abaixo do limiar de uma guerra formalmente declarada."

(CE e ARUNEPS, *Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*)

Ameaça Persistente Avançada: "um adversário que possui níveis sofisticados de especialização e recursos significativos que lhe permitem criar oportunidades para alcançar os seus objetivos através do uso de vários vetores de ataque (...) A ameaça persistente avançada: (i) procura concretizar os seus objetivos repetidamente durante um longo período de tempo; (ii) adapta-se aos defensores e aos seus esforços de resistência; e (iii) está determinada a manter o nível de interação necessário para atingir os seus objetivos."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Blacklist [lista negra]: "uma lista de entidades discretas, tais como *hosts* ou aplicações, que foram previamente consideradas estarem associadas a atividade maliciosa."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Botnet: "rede de computadores infetados [*drones*] por *software* malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados."

(TCE, *Desafios à Eficácia da Política de Cibersegurança da UE*)

Bug Bounty: um *bug bounty* é um programa que incentiva a procura, descoberta e descrição de *bugs* em *software* com base na oferta de uma recompensa. Muitas empresas oferecem uma recompensa deste tipo de modo a impulsionarem a melhoria dos seus produtos e serviços.

(adaptado de Techopedia)

CEO Fraud/Comprometimento de Email de CEO/Negócio: "A fraude de CEO/negócio acontece quando um funcionário de uma empresa é enganado de modo a pagar uma fatura falsa ou a fazer uma transferência não autorizada com a conta da empresa."

(Europol, Cyberscams)

Cibercrimes: "factos correspondentes a crimes previstos na Lei do Cibercrime e ainda a outros ilícitos penais praticados com recurso a meios tecnológicos, nos quais estes meios sejam essenciais à prática do crime em causa." [O cibercriminoso é aquele que pratica estes crimes; contudo, no âmbito dos agentes de ameaças, esta designação é atribuída àquele que pratica estes crimes com intenções sobretudo económicas].

(ENSC 2019-2023 [e ENISA, *Threat Landscape 2021*])

Ciberespaço: "consiste no ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação."

(ENSC 2019-2023)

Ciberespionagem: "esta ameaça geralmente tem como alvo os setores industriais, as infraestruturas críticas e estratégicas em todo o mundo, incluindo entidades governamentais, transportes, provedores de telecomunicações, empresas de energia, hospitais e bancos. Foca-se na geopolítica, no furto de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos."

(ENISA, *Threat Landscape 2018*)

Cibersegurança: "consiste no conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem."

(ENSC 2019-2023)

Ciberterrorismo: existe cada vez mais uma convergência entre terrorismo e ciberespaço. "Ao mesmo tempo que têm como motivação a realização de ciberataques, os Ciberterroristas têm

como objetivos o recrutamento e a monetarização". Não obstante este uso instrumental do ciberespaço, o principal objetivo deste agente de ameaça, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas.

(ENISA, *Threat Landscape 2018*)

Cyberbullying: "*bullying* realizado através da Internet ou telemóvel, envolvendo mensagens ofensivas ou maliciosas, emails, chats ou comentários, ou mesmo, em casos extremos, websites construídos com intenções maliciosas contra indivíduos ou certos grupos de pessoas."

(Richardson *et al., Internet Literacy Handbook*)

Cyber-offender: agente de ameaça que realiza ações como *sextortion* ou *cyberbullying* contra vítimas adolescentes e jovens adultos ou com nível semelhante de vulnerabilidade, provocando danos psicológicos e por vezes físicos nas vítimas. A extrapolação das ações deste tipo para outros contextos permite classificar este tipo de agente como alguém que realiza ações que visam meramente a disrupção e a perturbação de um alvo, sem que existam motivos económicos ou ideológicos claros ou expressos.

(Adaptado de ENISA, *Threat Landscape 2020* [extrapolação realizada por CNCS])

Command & Control (C&C): "a parte mais importante de uma *botnet* é a designada infraestrutura de comando e controlo (C&C). Esta infraestrutura é constituída por *bots* e pela entidade de controlo que tanto pode ser centralizada como distribuída. São usados pelo *bot master* um ou mais protocolos de comunicação para comandar os computadores das vítimas e coordenar as suas ações (...) A infraestrutura de C&C serve tipicamente como a única forma de controlar *bots* numa *botnet*."

(ENISA, *Botnets: Detection, Measurement, Disinfection & Defence*)

E-skimming: *skimming* realizado por via eletrónica – o *skimming* "envolve a duplicação da faixa magnética de um cartão bancário, frequentemente através de dispositivos escondidos em terminais ATM". Por via eletrónica, atinge-se o mesmo fim através de métodos de pagamento *online*.

(Europol, *Payment Fraud e Europol Internet Organized Crime Thread Assessment*)

Defacement [defacing]: "alteração ilícita de páginas *web*".

(ENISA, *Abordagem Gradual de Criação de uma CSIRT*)

Desinformação: "toda a informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público."

(ERC, *A Desinformação - Contexto Europeu e Nacional*)

Engenharia Social: "o ato de enganar um indivíduo no sentido de este revelar informação sensível, assim obtendo-se acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança."

(NIST, *Digital Identity Guidelines*)

Força-bruta: "em criptografia, um ataque que explora todas as possíveis combinações para encontrar uma chave que combine com a correta."

(NIST, *De-Identification of Personal Information*)

Hacktivistas: agentes de ameaças "orientados a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais."

(ENISA, *Threat Landscape 2018*)

Incidentes: "eventos com um efeito adverso real na segurança das redes e dos sistemas de informação."

(Lei n.º 46/2018, de 13 de agosto)

Insider [Ameaça Interna]: "a ameaça interna pode existir em todas as empresas ou organizações. Qualquer colaborador atual ou ex-colaborador, sócio ou fornecedor, que tenha, ou tenha tido, acesso aos ativos digitais da organização, pode abusar, voluntaria ou involuntariamente, desse acesso. Os três tipos mais comuns de ameaças internas são: *insider* malicioso, que age intencionalmente; *insider* negligente, que é desleixado ou não está em conformidade com as políticas e instruções de segurança; e *insider* comprometido, que age involuntariamente como instrumento de um atacante real."

(ENISA, *Threat Landscape 2018*)

Intrusion Detection Systems (IDS): "produto de *hardware* ou *software* que recolhe e analisa informação de várias áreas num computador ou rede de modo a identificar possíveis falhas de segurança, que incluem intrusões (ataques a partir do exterior da organização) e má utilização (ataques a partir do interior da organização)."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Malware [Software Malicioso]: "programa que é introduzido num sistema, geralmente de forma encoberta, com a intenção de comprometer a confidencialidade, a integridade ou a dis-

ponibilidade dos dados da vítima, de aplicações ou do sistema operativo, ou perturbando a vítima."

(NIST, *IR 7298 Revision 2, Glossary of Key Information Security Terms*)

Observável (instância): "representa uma efetiva observação específica que ocorreu no domínio ciber. As propriedades detalhadas desta observação são específicas e não ambíguas."

(STIX)

Phishing: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de *emails* ou mensagens para que estes abram anexos maliciosos, cliquem em URL inseguros, revelem as suas credenciais através de páginas de *phishing* aparentemente legítimas [*pharming*], façam transferências de dinheiro, etc."

(ENISA, *Threat Landscape 2018*)

Ransomware: tipo de *malware* que permite que "um atacante se apodere dos ficheiros e/ou dispositivos de uma vítima, bloqueando a possibilidade de esta poder aceder-lhes. Para a recuperação dos ficheiros, é exigido ao proprietário um resgate em criptomoedas."

(ENISA, *Threat Landscape 2018*)

Sextortion: "a prática de forçar alguém a fazer algo, particularmente a realizar atos sexuais [ou a pagar um resgate], através de uma ameaça de publicação de dados ou imagens de natureza íntima ou com cariz sexual da vítima [ameaça que por vezes não corresponde a uma possibilidade efetiva, apresentando-se detalhes técnicos, como a palavra-passe da vítima, de modo a tornar a ameaça mais credível]".

(Adaptado de *Cambridge Advanced Learner's Dictionary & Thesaurus*)

Scan/Scanning: "Ataques baseados em pedidos realizados a um sistema com o intuito de descobrir pontos fracos. Também inclui processos de teste para recolha de informações sobre sistemas, serviços e contas. Exemplos: *fingerd*, consultas DNS, ICMP, SMTP (EXPN, RCPT, etc.), *scanning* de portos.."

(RNCSIRT, *Taxonomia Comum da Rede Nacional de CSIRT*)

Script kiddies: indivíduos com poucas competências na realização de ciberataques, mas que, ainda assim, os conseguem realizar através da aquisição de ferramentas de *hacking* fáceis de adquirir e usar. "Estas ferramentas podem tornar-se meios com muito alcance nas mãos de grupos com poucas capacidades. Além disso, quando se tenta quantificar o conhecimento disponível e poder de ataque dos *script kiddies*, consegue-se

ter um vislumbre de um dos desafios de cibersegurança: jovens com alguma orientação podem tornar-se muito eficientes em ações de *hacking*."

(ENISA, *Threat Landscape 2019*)

SIM *swapping*: "ocorre quando um agente malicioso, através de técnicas de engenharia social, adquire controlo sobre o cartão SIM do telemóvel da vítima utilizando dados pessoais furtados."

(Europol, *SIM swapping – a mobile phone scam*)

Smishing: "(combinação das palavras SMS e *phishing*) é a tentativa por atacantes de obter dados pessoais, financeiros ou de segurança por mensagem de texto".

(Europol, *Cyberscams*)

Typosquatting: técnica usada para atrair o tráfego para um *website* redirecionando gralhas comuns em termos de pesquisa ou de *websites* populares. Quem pratica esta atividade pode tentar vender produtos, instalar *malware* no dispositivo de um utilizador ou até mesmo fazer uma declaração política. A versão extrema do *typosquatting* é semelhante ao *phishing*, em que um *website* impostor imita um website real, proporcionando assim ao utilizador uma falsa impressão de que acedeu ao *website* correto. O *typosquatting* também é referido como sequestro de URL.

(adaptado de Techopedia)

Violação de dados pessoais: "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento."

(RGPD)

Vishing: uso de mensagens de voz ou de chamadas telefónicas para roubar identidades e recursos financeiros. O termo resulta da combinação de *voice* e *phishing*.

(adaptado de Techopedia)

Vulnerabilidade: "falha em *software* ou componentes de hardware que permite que um atacante efetue ações que normalmente não seriam permitidas."

(CERT Carnegie Mellon University)

APAV: Associação Portuguesa de Apoio à Vítima.

CERT.PT: Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei 46/2018) [CERT - Computer Emergency Response Team].

C&C: Command and Control.

C/V: Com Vulnerabilidades.

CNCS: Centro Nacional de Cibersegurança.

CNPD: Comissão Nacional de Proteção de Dados.

CVE: Vulnerabilidades e Exposições Comuns [Common Vulnerabilities and Exposures].

DGPJ: Direção-Geral da Política de Justiça.

DoS/DDoS: Negação de Serviço Distribuída [Distributed Denial of Service].

ENISA: Agência da União Europeia para a Cibersegurança.

ENSC: Estratégia Nacional de Segurança do Ciberespaço 2019-2023.

N/A: Não se aplica.

INE: Instituto Nacional de Estatística.

PGR: Procuradoria-Geral da República.

PME: Pequenas e Médias Empresas.

RGPD: Regulamento Geral sobre a Proteção de Dados.

RNCSIRT: Rede Nacional de Equipas de Resposta a Incidentes de Segurança Informática [CSIRT-Computer Security Incident Response Team].

RK: Ranking.

S/D: Sem Dados.

S/V: Sem Vulnerabilidades.

UE: União Europeia.

L. REFERÊNCIAS PRINCIPAIS

(última consulta de links a 27/04/2022)

RELATÓRIOS

ENISA (2021) *ENISA Threat Landscape 2021*. ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA (2020) *ENISA Threat Landscape 2020*. ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

ENISA (2019) *ENISA Threat Landscape 2018*. ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

ENISA (2011) *Botnets: Detection, Measurement, Disinfection & Defence*. ENISA-European Union Agency for Cybersecurity.

Disponível em https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence

ERC (2019) *A Desinformação - Contexto Europeu e Nacional*. Entidade Reguladora da Comunicação.

Disponível em https://www.parlamento.pt/Documents/2019/abril/desinformacao_contextoeuroeunacional-ERC-abril2019.pdf

Europol (2021) *Europol Internet Organized Crime Thread Assessment 2021*. Europol EC3.

Disponível em https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf

Europol (2020) *Europol Internet Organized Crime Thread Assessment 2020*. Europol EC3.

Disponível em https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

PGR (2022) *Nota Informativa Cibercrime: Denúncias Recebidas 2021*. Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime.

Disponível em https://cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias-de-cibercrime-25-01-2022.pdf

PGR (2021) *Nota Informativa Cibercrime: Denúncias Recebidas 2020*. Ministério Público, Procuradoria-Geral da República, Gabinete Cibercrime.

Disponível em https://cibercrime.ministeriopublico.pt/pagina/cibercrime-em-2020-denuncias-recebidas

TCE (2019) *Desafios à Eficácia da Política de Cibersegurança da UE*. Tribunal de Contas Europeu.

Disponível em https://www.eca.europa.eu/pt/Pages/DocItem.aspx?did=49416

WEF (2022) *Global Cybersecurity Outlook 2022*. World Economic Forum.

Disponível em https://www.weforum.org/reports/global-cybersecurity-outlook-2022/

OUTROS DOCUMENTOS

APAV (2022) *Estatísticas 2021 Linha Internet Segura*. APAV - Associação Portuguesa de Apoio à Vítima.

Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_APAV_LinhaInternetSegura_2021.pdf

APAV (2021) *Estatísticas 2020 Linha Internet Segura*. APAV - Associação Portuguesa de Apoio à Vítima.

Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_LIS_2020.pdf

APAV (2020) *Estatísticas 2019 Linha Internet Segura*. APAV - Associação Portuguesa de Apoio à Vítima.

Disponível em https://apav.pt/apav_v3/images/pdf/Estatisticas_Linha_Internet_Segura_2019.pdf

Bravo, R. (2022) *Segurança da Informação, Cibersegurança e Cibercrime: contributos para um alinhamento de conceitos* (no prelo).

Disponível em https://www.academia.edu/40494857/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o_e_ciberseguran%C3%A7a_aspetos_pr%C3%A1ticos_e_legisla%C3%A7%C3%A3o

CE e ARUNEPS (2016) *Comunicação Conjunta ao Parlamento Europeu e ao Conselho, Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia)*. Comissão Europeia e Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança.

Disponível em https://op.europa.eu/en/publication-detail/-/publication/c35240f2-fca1-11e5-b713-01aa75ed71a1/language-pt

CNCS (2021) *Boletim 04/2021. Observatório de Cibersegurança*. Centro Nacional de Cibersegurança.

Disponível em https://www.cncs.gov.pt/docs/boletim-observatorio-setembro2021-1.pdf

ENISA (2006) *Abordagem Gradual de Criação de uma CSIRT*.

ENISA – Agência da União Europeia para a Cibersegurança.

Europol (2018) *Cyberscams*. Europol EC3.

Disponível em https://www.europol.europa.eu/sites/default/files/documents/pt_0.pdf

ISO/IEC 27032:2012(en) *Information technology - Security techniques - Guidelines for cybersecurity.* International Standards Organization.

Disponível em https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en

NIST (2017) *Digital Identity Guidelines*. National Institute of Standards and Technology.

Disponível em https://pages.nist.gov/800-63-3/sp800-63-3.html

NIST (2015) *De-Identification of Personal Information*. National Institute of Standards and Technology.

Disponível em https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8053.pdf

NIST (2013) *NIST IR 7298 Revision 2, Glossary of Key Information Security Terms*. National Institute of Standards and Technology.

Disponível em https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Richardson, J.; E. Milovidov; J.D. and Martin Schmalzried (2017) *Internet Literacy Handbook*. Council of Europe.

Disponível em https://edoc.coe.int/en/internet/7515-internet-literacy-handbook.html

RNCSIRT (2020) *Taxonomia Comum da Rede Nacional de CSIRT*. Rede Nacional CSIRT.

Disponível em https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf

LEGISLAÇÃO

Estratégia Nacional de Segurança do Ciberespaço:

https://www.cncs.gov.pt/docs/cncs-ensc-2019-2023.pdf

Lei do Cibercrime:

https://files.dre.pt/1s/2009/09/17900/0631906325.pdf

Regime Jurídico da Segurança do Ciberespaço:

https://www.cncs.gov.pt/docs/regime-jurdico-da-segurana-do-ciberespao.pdf

Regulamento Geral sobre a Proteção de Dados:

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=2961&tabela=leis

WEBSITES

https://csrc.nist.gov/glossary

https://dictionary.cambridge.org

https://stixproject.github.io

https://www.europol.europa.eu

https://www.kb.cert.org

https://www.redecsirt.pt

https://www.techopedia.com

ANEXO
Linhas de Ação da ENSC – Riscos e Conflitos 2022

Linhas de Ação da ENSC diretamente articuláveis com os indicadores deste relatório		I&C*	A&T
E2 a**	Reforçar os meios de recolha e processamento de informação e as capacidades de análise.		
E2 c	Antecipar a emergência, evolução e mutação das ameaças, possibilitando a adoção atempada de ações que acrescentem resiliência.		
E2 r	Promover programas de sensibilização específicos junto das instituições públicas e privadas, que robusteçam a vertente comportamental de segurança em ambiente digital, com base na partilha de conhecimento especializado sobre os agentes da ameaça e seus modos de atuação.		
E2 s	Sensibilizar as entidades nacionais para as respetivas vulnerabilidades específicas, passíveis de serem infiltradas, exploradas ou subvertidas no campo digital por agentes de ameaça diversos.		
E3 b	Promover o contínuo desenvolvimento das capacidades e maturidade das entidades nacionais na prevenção, deteção, resposta e recuperação perante cenários adversos à segurança do ciberespaço que possam produzir impactos nas suas redes e sistemas de informação e ecossistema que as caracteriza, consolidando a confiança mútua, a partilha de informação e conhecimento, e a cooperação célere e eficaz.		
E3 c	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.		
E4 b	Adequar, para efeitos de gestão de crises, as capacidades das Forças Armadas, das Forças e Serviços de Segurança e de outras entidades públicas e privadas, tendo em vista impulsionar uma abordagem integrada às ameaças e riscos em matéria de segurança do ciberespaço.		
E4 f	Reforçar a capacidade de resposta às ameaças, maximizando as sinergias criadas pela cooperação e confiança existentes entre as equipas de resposta a incidentes de segurança informática, potenciando a criação de novas equipas desta natureza em todas as entidades, públicas e privadas, com responsabilidade pela segurança das redes e sistemas de informação.		
E4 h	Consolidar e promover a capacidade nacional de conhecimento das ameaças à segurança do ciberespaço, de forma colaborativa entre as autoridades nacionais com responsabilidade nesta área e com a participação ativa das entidades do setor público e privado, produzindo e partilhando, desta forma, um conhecimento agregado que permita a antecipação dos impactos, a tomada de ações proativas e um melhor conhecimento da ameaça, por todos os envolvidos.		

* E2: Eixo 2 - Prevenção, educação e sensibilização; E3: Eixo 3 - Proteção do ciberespaço e das infraestruturas;
E4: Eixo 4 - Resposta às ameaças e combate ao cibercrime; I&C: Incidentes e Cibercrime; A&T: Ameaças e Tendências.
** Codificação atribuída com base no eixo em questão e na sequência pela qual surgem as linhas de ação, alinhadas com a ordem alfabética.

Quadro 7

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt • (+351) 210 497 400

Observatório
de **Cibersegurança**