CNCS
Centro Nacional de Cibersegurança
PORTUGAL

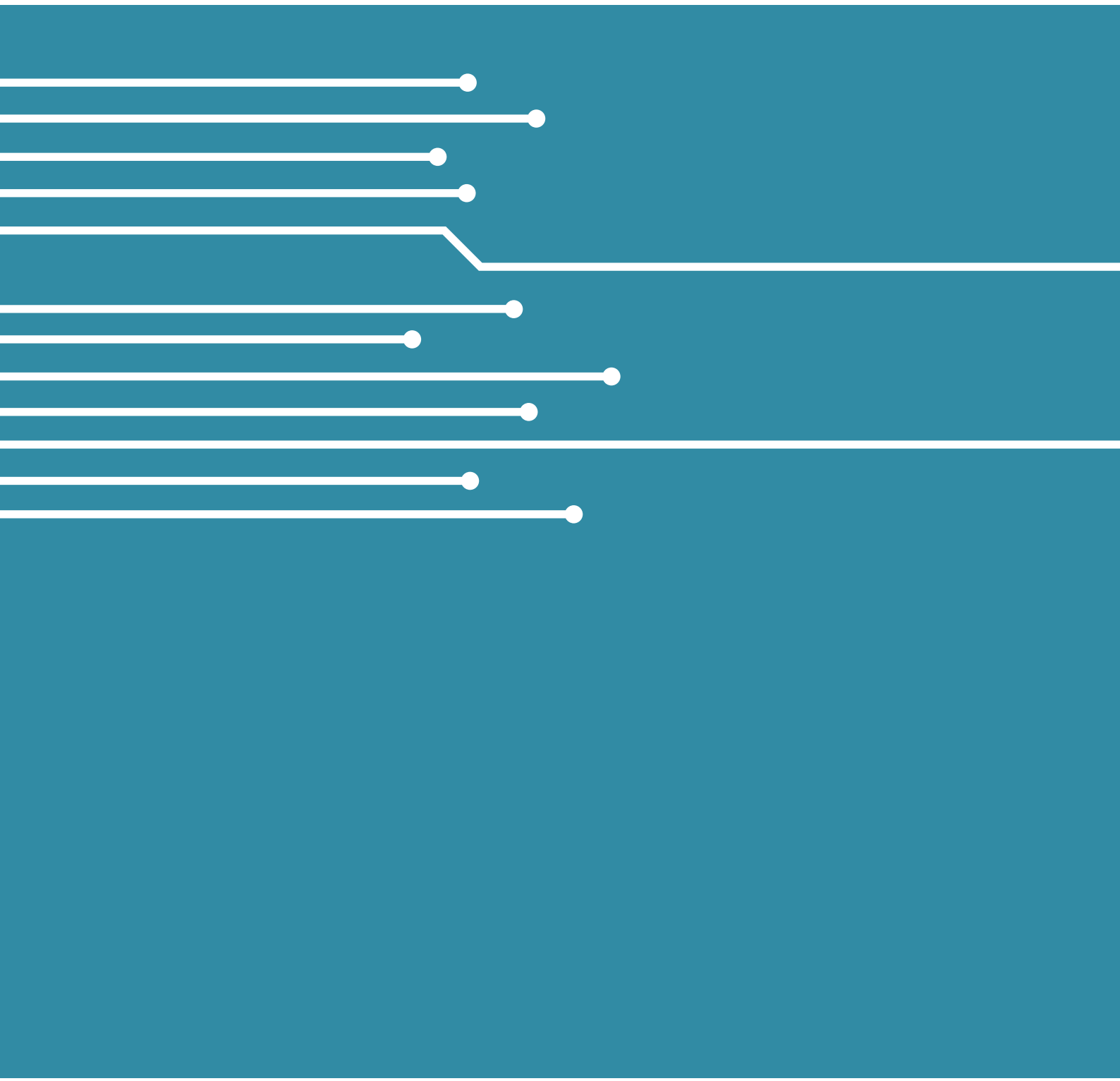
RELATÓRIO

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos

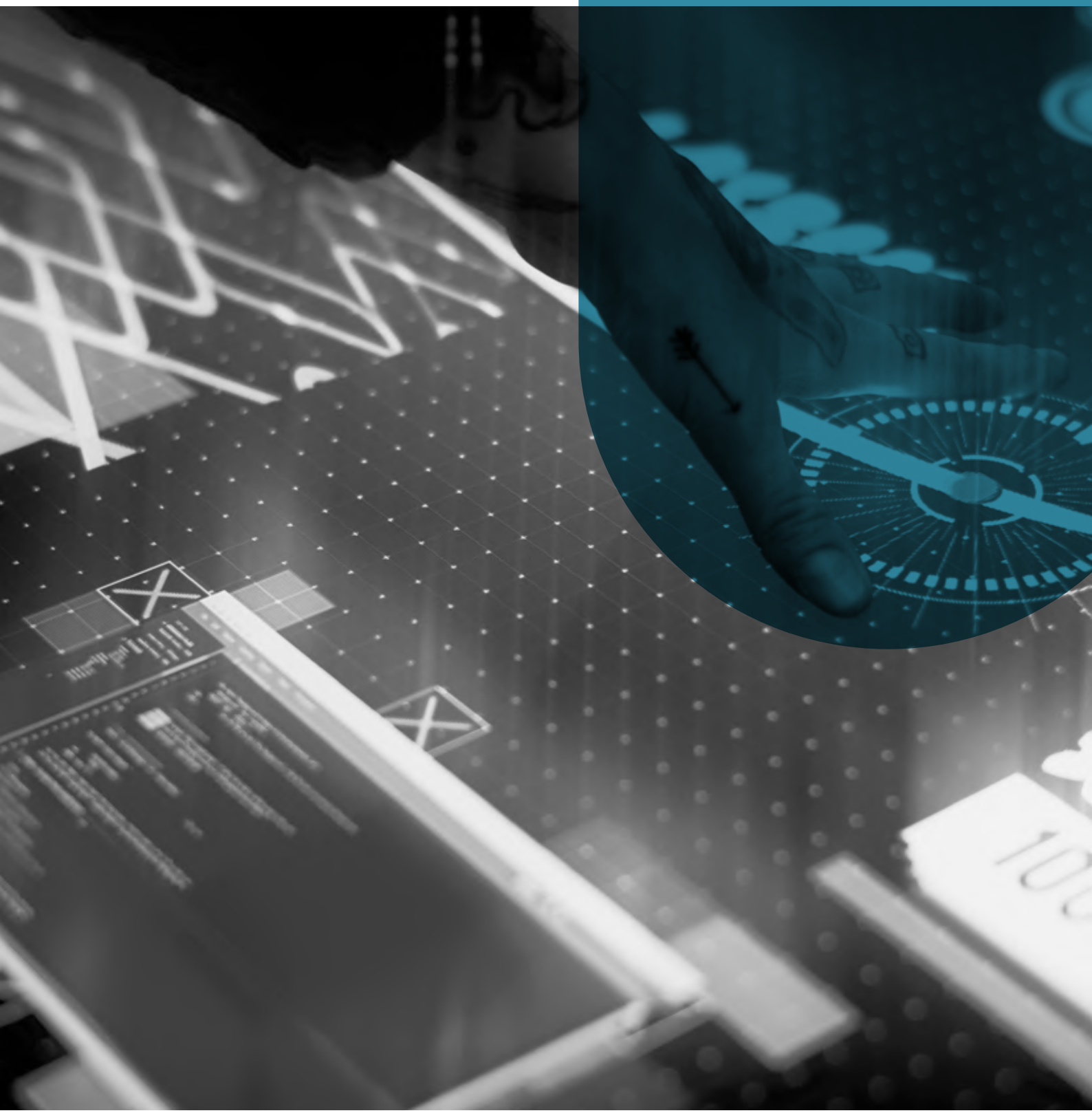
JUNHO DE 2020

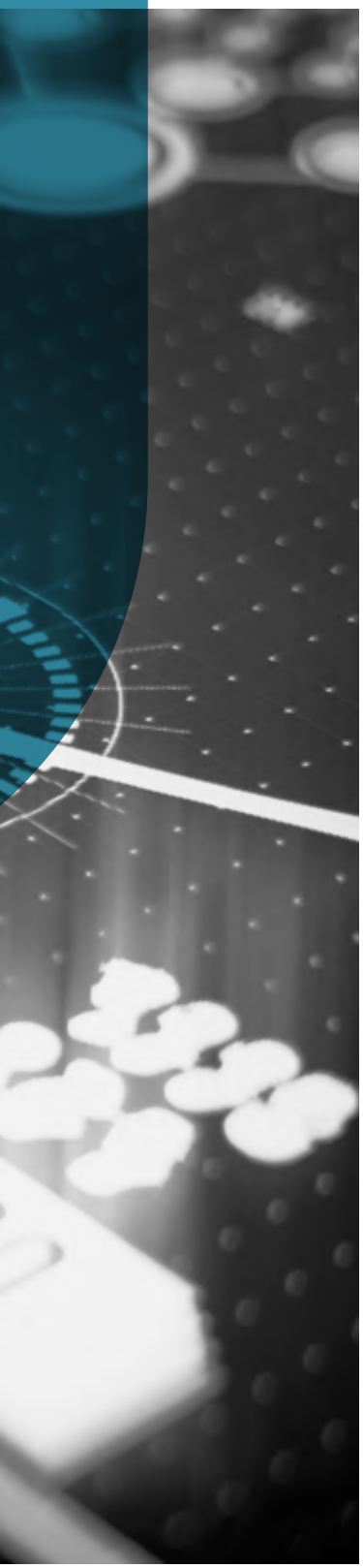
Observatório de **Cibersegurança**



ÍNDICE

Observatório de Cibersegurança





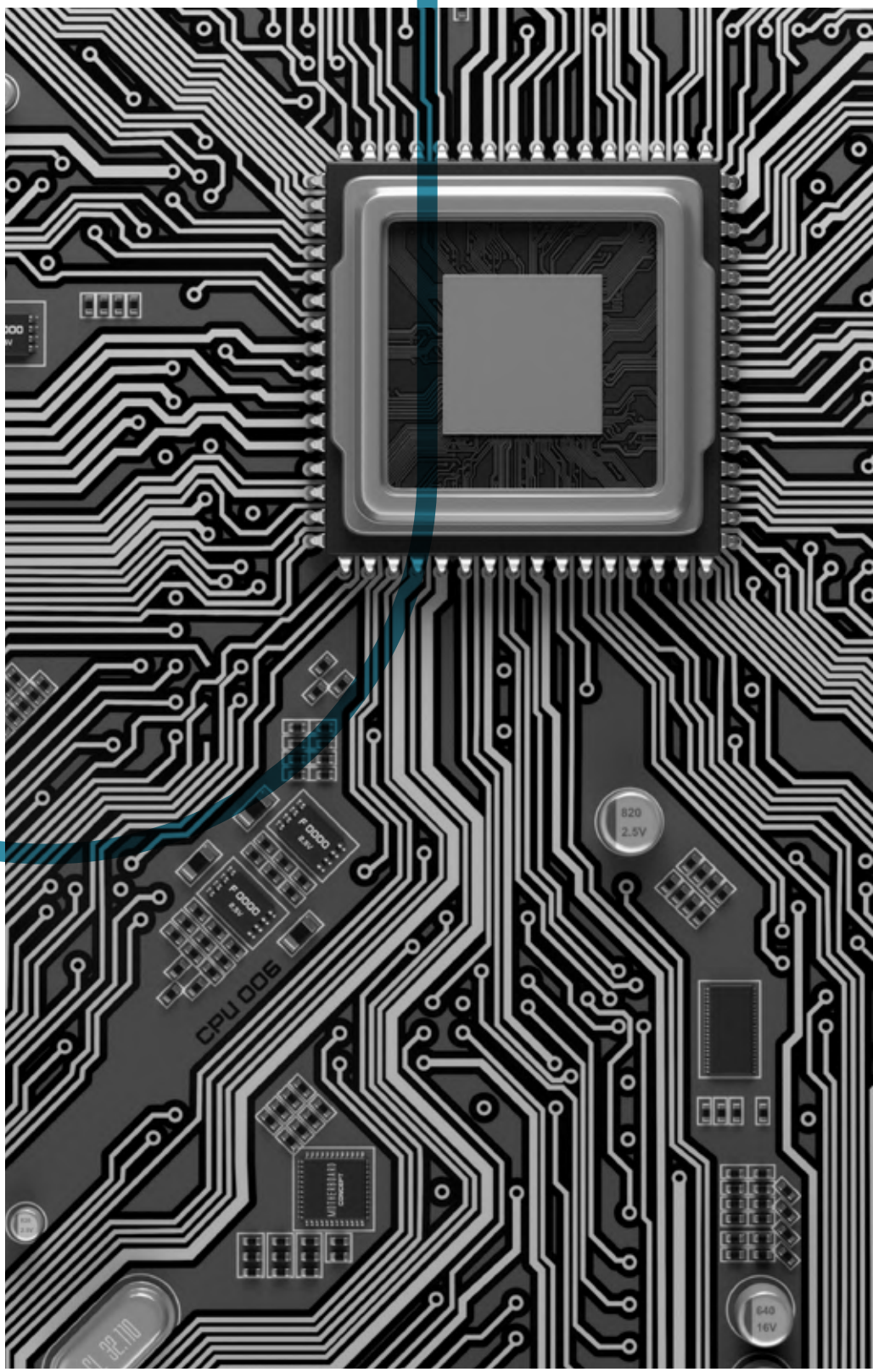
A. SUMÁRIO EXECUTIVO

O objetivo deste Relatório é analisar os principais indicadores de riscos e conflitos no âmbito da cibersegurança, com enfoque no ciberespaço de interesse nacional português, em relação ao ano de 2019, mas também considerando anos anteriores e possíveis desenvolvimentos futuros. Esta análise é dividida em dois blocos.

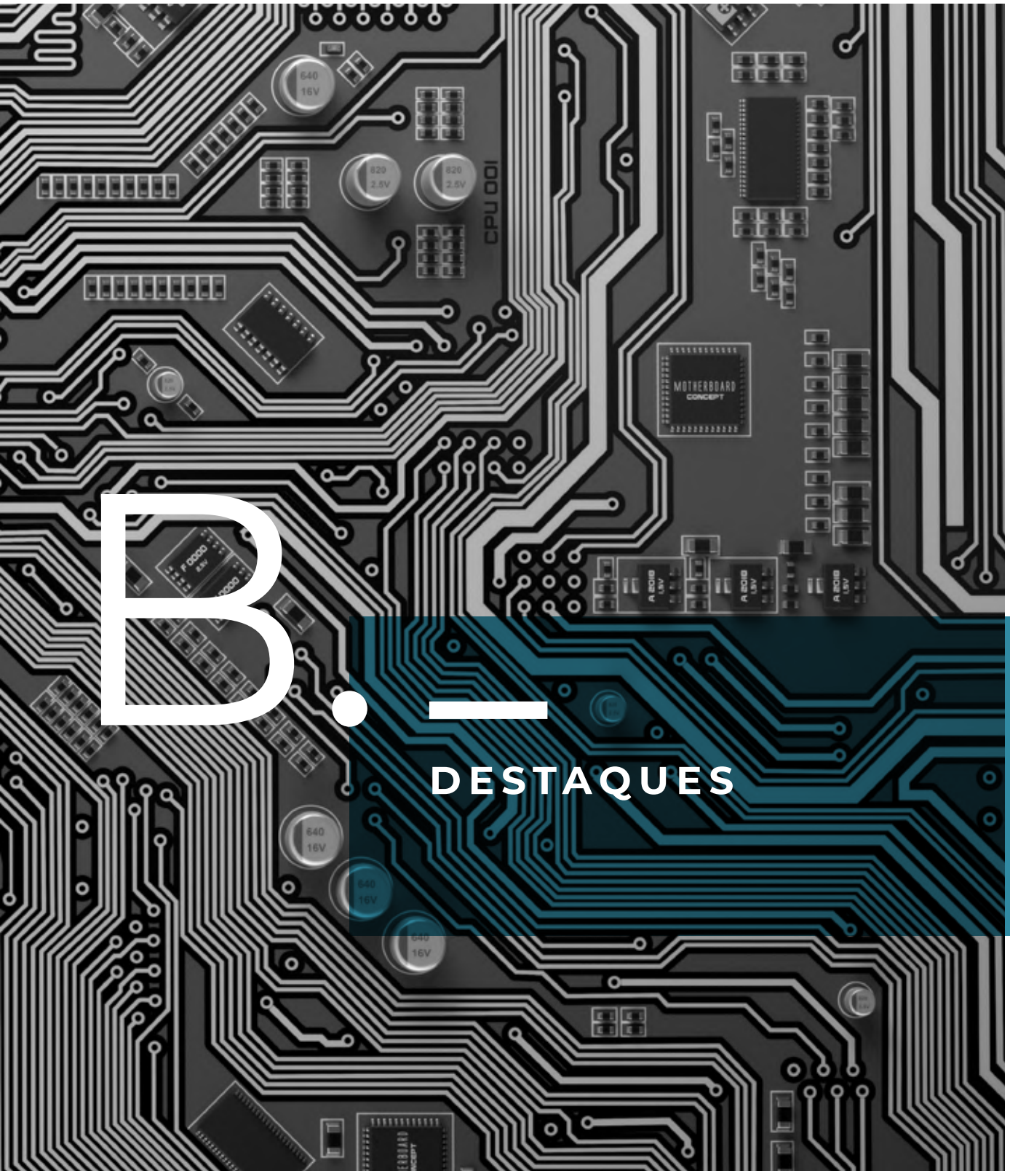
O primeiro bloco diz respeito a Atores e Incidentes, em que se apresentam e interpretam os principais indicadores sobre organizações e indivíduos a este respeito, sobretudo enquanto vítimas, bem como sobre os incidentes e os cibercrimes registados. Esta parte desenvolve-se com base em números que expressam acontecimentos confirmados, permitindo identificar os que são dominantes e algumas tendências.

O segundo bloco, Ameaças e Prospetivas, analisa agentes e táticas, técnicas e procedimentos que representam ameaças para a segurança do ciberespaço de interesse nacional, tendo em conta os acontecimentos confirmados em 2019 e aqueles que podem perspetivar-se para 2020 e 2021. As análises que esta parte expõe apresentam-se mais como hipóteses fortes do que como factos consumados, ainda que pretendam contribuir para a construção de horizontes de ação orientadores dos atores do ciberespaço.

Este documento utiliza algumas fontes abertas, mas também dados recolhidos diretamente pelo Centro Nacional de Cibersegurança (CNCS). Uma componente importante das análises realizadas resulta dos contributos dos vários parceiros ligados à Justiça e à Segurança que se prestaram a colaborar neste trabalho.

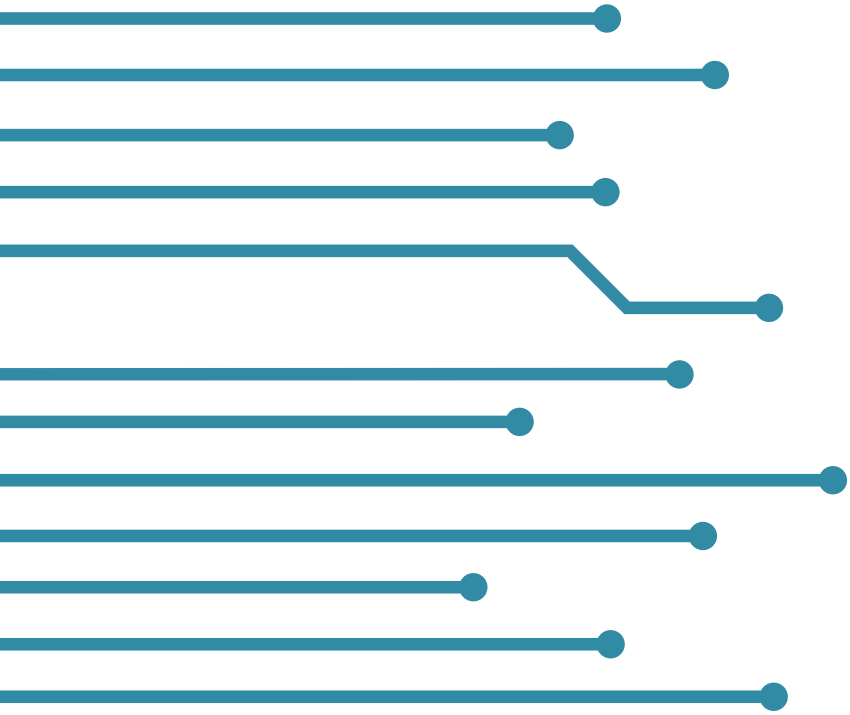

CPU 006

CNCS
Centro Nacional de Cibersegurança
PORTUGAL



B.1 DESTAQUES

Observatório
de **Cibersegurança**



Atores e Incidentes

Empresas e indivíduos em Portugal reconhecem menos do que na UE sofrer incidentes de cibersegurança, em 2019 (Eurostat).

8% DAS EMPRESAS PORTUGUESAS (13% na UE)

27% DOS INDIVÍDUOS PORTUGUESES (37% na UE)

As grandes empresas e as empresas de telecomunicação em Portugal e na UE são aquelas que mais reconhecem justificar incidentes de segurança de TIC, em 2019 (Eurostat).

14% DAS GRANDES EMPRESAS PORTUGUESAS

17% DAS EMPRESAS DE TELECOMUNICAÇÕES PORTUGUESAS

Há menos empresas em Portugal do que na UE com seguro contra incidentes de segurança de TIC, em 2019 (Eurostat).

10% EM PORTUGAL

21% NA UE

Em 2019, o tipo de incidente de segurança no uso de *internet* para fins privados que os indivíduos em Portugal reconhecem sofrer mais é o *phishing* (Eurostat).

18% EM PORTUGAL

28% NA UE

Em 2019, os portugueses com idades entre os 25 e os 34 anos e os portugueses com estudos superiores tendem a reconhecer mais do que outros que sofreram incidentes de segurança no uso da *internet* para fins privados (Eurostat).

35% 25-34 ANOS

18% 65-74 ANOS

COM ESTUDOS SUPERIORES **40%**

SEM ESTUDOS SUPERIORES **17%**

O *phishing* e a infeção por *malware* (inclui *ransomware*) são os tipos de incidentes mais registados em 2019 pelo CERT.PT e pela RNCSIRT (CERT.PT e RNCSIRT).

NO CERT.PT, **31%** SÃO *PHISHING*; **16%** SÃO INFEÇÕES POR *MALWARE*

NA RNCSIRT, **13%** SÃO *PHISHING*; **13%** SÃO INFEÇÕES POR *MALWARE*

Atores e Incidentes

2º

O segundo semestre de 2019 regista mais incidentes do que o primeiro, com destaque para o terceiro trimestre no CERT.PT e para o quarto trimestre na RNCSIRT (CERT.PT e RNCSIRT). A Linha Internet Segura também registou mais processos durantes estes períodos (APAV).

Durante 2019, as Infraestruturas Digitais (ID), os Prestadores de Serviços de Internet (PSI), a Educação, Ciência, Tecnologia e Ensino Superior (ECTES) e a Banca são os setores e áreas governativas mais afetados por incidentes e com mais observáveis identificados (CERT.PT).

19% DOS INCIDENTES EM ID

18% DOS INCIDENTES EM PSI

9% DOS INCIDENTES EM ECTES

8% DOS INCIDENTES NA BANCA

Entre 2018 e 2019 houve um aumento no número de incidentes registados e no número de vulnerabilidades identificadas pelo CERT.PT (CERT.PT).

+ 26% DE INCIDENTES

+ 139% DE VULNERABILIDADES

Entre 2009 e 2018 verifica-se um aumento constante da percentagem, entre todos os crimes registados no país, de crimes informáticos, de crime de devassa por meio informático e de crime de burla informática/comunicações (DGPJ).

0,6% DO TOTAL DE CRIMES EM 2009

3,4% DO TOTAL DE CRIMES EM 2018

O Gabinete de Cibercrime do Ministério Público registou um aumento no número de denúncias entre 2018 e 2019 (MP).

+ 21% DE DENÚNCIAS

+ 34% ENTRE AS QUE FORAM ENCAMINHADAS PARA INQUÉRITO

Os casos mais frequentes registados pela Linha Internet Segura, em 2019, são a burla, o furto de identidade e o *phishing* (APAV).

BURLA 20%

FURTO DE INDENTIDADE 12%

PHISHING 9%

Ameaças e Prospetivas

Os tipos de agentes de ameaças mais relevantes em 2019-2020 para Portugal são os cibercriminosos, os agentes estatais e os hacktivistas.

As ciberameaças mais concretizadas por estes agentes de ameaças são o *phishing*, *malware* (que inclui *ransomware*), compromissos de contas, exploração de vulnerabilidades, DDoS, *botnets* e *data breaches*.

Verifica-se, em 2019, um aumento do uso de produtos e serviços de cibercrime disponíveis *online* (cibercrime-como-serviço).

Tendência para, em 2020, haver mais articulação entre ameaças estatais e não estatais, com maior dificuldade de atribuição.

Tendências globais para certas tecnologias emergentes (Internet das Coisas, 5G, Inteligência Artificial, Computação Quântica e Plataformas em Nuvem) que aumentam a superfície e os vetores de ataque.

Persistência de problemas globais que promovem a fragmentação e a imprevisibilidade na governabilidade da cibersegurança a nível internacional, em 2020.

Importância global de certos cibercrimes que envolvem *ransomware*, fraude, *phishing* e ataques à cadeia de fornecimento, em 2020.

A pandemia de Covid-19 interfere em todas as previsões para 2020 e 2021: possível desaceleração da evolução de algumas tecnologias; ameaça à proteção dos dados pessoais; e aumento dos ciberataques que usam a engenharia social oportunista em relação a momentos de crise ou promovem a desestabilização social e política.

C. INTRODUÇÃO

O *Relatório Cibersegurança em Portugal – Linha de Observação Riscos & Conflitos* é o segundo Relatório lançado pelo Observatório de Cibersegurança do CNCS, depois de publicado o Relatório do âmbito da Linha de Observação Sociedade. O documento que ora se publica tem como objetivo apresentar números, análises e perspetivas sobre os riscos e os conflitos identificados no ciberespaço de interesse nacional durante o ano de 2019. Para o efeito, disponibiliza dados quanto a indicadores de Atores, Incidentes, Ameaças e Prospetivas.

Estes diferentes planos procuram abranger os aspetos mais relevantes da cibersegurança no que diz respeito ao risco e ao conflito e são divididos em dois capítulos principais: Atores e Incidentes, por um lado, e Ameaças e Prospetivas, por outro. O espírito que subjaz a esta distinção prende-se com a diferença entre acontecimentos que concretizam riscos, identificados no primeiro caso, e riscos que se mantêm como tal, no domínio do segundo. Não se pretende fazer uma análise de risco com os dados apresentados, mas fornecer instrumentos para que ela possa ser feita.

Quanto às fontes utilizadas, recorre-se a algumas que são abertas, como o Eurostat, mas também a Instituições nacionais ligadas à Justiça e à Segurança. Muitos dos dados têm como fonte principal o próprio CNCS e a Rede Nacional de CSIRT (RNCSIRT). Os diversos parceiros que colaboraram neste documento também participaram com análise e com as suas perspetivas qualitativas. Comparando com o Relatório da Linha de Observação Sociedade, este terá uma combinação mais proporcional entre componentes quantitativa e qualitativa. Nesse sentido, tende a realizar interpretações que conjeturam sobre o futuro, procurando, não obstante, suportá-las em dados ou na experiência dos parceiros do Relatório. Em termos de formato, os principais indicadores quantitativos são

enumerados e analisados, procurando, sempre que possível, considerar linhas temporais e comparações com a União Europeia. As análises qualitativas seguem uma abordagem mais aberta e menos esquemática.

No capítulo Atores e Incidentes apresentam-se dados sobre incidentes experienciados por empresas e indivíduos, recolhidos quer mediante questionários, quer nos registos efetuados pelo CERT.PT e pela RNCSIRT. Analisam-se ainda os números relativos ao cibercrime. No capítulo posterior, Ameaças e Prospetivas, identificam-se os agentes de ameaças considerados mais relevantes, o seu *modus operandi* e os aspetos técnicos e comportamentais críticos no futuro da cibersegurança em Portugal. Por fim, apresentam-se as notas conclusivas, as notas metodológicas, as entidades parceiras, o conselho consultivo e as referências principais.

D. TERMOS E ABREVIATURAS

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

(ISO/IEC 27032)

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, 2019, *Desafios à Eficácia da Política de Cibersegurança da UE*)

CEO Fraud/Compromisso de Email Corporativo: "ocorre quando um colaborador autorizado a fazer pagamentos é ludibriado [por alguém que se faz passar, frequentemente, pela chefia da organização] no sentido de pagar uma fatura falsa ou realizar uma transferência não autorizada da conta bancária da organização."

(Europol, *CEO/Business Email Compromise (BEC) fraud*)

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 Report 2018*])

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 roubo de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos."

(ENISA, *Threat Landscape Report 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 ameaças, em última análise, é a realização de ciberataques por razões típicas de grupos terroristas.

(ENISA, *Threat Landscape Report 2018*)

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*)

Data Breach: "termo utilizado para designar um incidente resultante de uma fuga ou exposição de dados (incluindo informação sensível relacionada com organizações ou simples detalhes pessoais de indivíduos, i. e., informação médica). Relaciona-se diretamente com os resultados de outras ciberameaças."

(ENISA, *Threat Landscape Report 2018*)

Deep Fake: "falsificações profundas, vídeos falsos realizados com recurso à inteligência artificial e à aprendizagem automática."

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

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 Guideline, 2017*)

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

(NIST, *De-Identification of Personal Information, 2015*)

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

(ENISA, *Threat Landscape Report 2018*)

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

(Lei 46/2018)

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 Report 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 disponibilidade 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)

Pharming: quando se é "redirecionado para *websites* falsos que solicitam informação pessoal."

(Eurostat, *Newsrelease ICT usage in households and by individuals in 2019*)

Phishing: "mecanismo de elaboração de mensagens que usam técnicas de engenharia social de modo a 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 Report 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 Report 2018*)

Scan: "envio de pacotes ou solicitações a outros sistemas de forma a obter informação para ser usada em ataque subsequente."

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

Script kiddies: indivíduos com poucas competências na realização de ciberataques 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 Report 2018*)

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.

APT: Ameaça Persistente Avançada [Advanced Persistent Threat].

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

CNCS: Centro Nacional de Cibersegurança.

CNPD: Comissão Nacional de Proteção de Dados.

DGPJ: Direção-Geral de Políticas de Justiça.

ENISA: Agência da União Europeia para a Cibersegurança.

ENSC: Estratégia Nacional de Segurança do Ciberespaço.

INE: Instituto Nacional de Estatística.

MP: Ministério Público.

PME: Pequenas e Médias Empresas.

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

TIC: Tecnologias de Informação e Comunicação.

TTP: Táticas, Técnicas e Procedimentos.

UE: União Europeia.

UE27: União Europeia excluindo o Reino Unido.

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

E.4 ATORES E INCIDENTES

Observatório de **Cibersegurança**

A cibersegurança, enquanto estado que se pretende garantir e manter, é constituída por atores que tanto podem ser uma ameaça a essa cibersegurança como vítimas da sua ausência. O incidente, por sua vez, é o evento adverso nas redes e nos sistemas de informação que coloca em causa a segurança esperada. Esta, em última análise, refere-se sempre a pessoas, os agentes, quer sejam responsáveis por ameaçar o ciberespaço, quer sejam aqueles cuja segurança, precisamente, é posta em causa.

Portanto, os atores e os incidentes têm uma relação próxima. Em princípio, um incidente pode ser remetido até à ação de um agente responsabilizável, direta ou indiretamente. Conseguir realizar esse processo significa atingir a atribuição, algo nem sempre possível e particularmente difícil em cibersegurança. Menos complexo é identificar a vítima ou o conjunto de vítimas. Não obstante, uma fatia importante dos dados sobre incidentes, quer resultantes de inquéritos, quer de notificações ou deteção automática, associam o incidente a um ator, ou procuram fazê-lo, pelo menos a uma vítima. Por essa razão, neste capítulo opta-se por juntar estas duas realidades, atores e incidentes, considerando que grande parte da informação disponível não as separa.

Este capítulo divide-se em três subcapítulos: Empresas e Indivíduos, o qual analisa dados do Eurostat sobre incidentes que afetam estes dois tipos de atores; Ciberespaço de Interesse Nacional, em que se recorre aos números do CERT.PT, da RNCSIRT e da CNPD sobre incidentes reportados; e Cibercrime, em que se analisa a informação disponibilizada pela DGPJ, pelo MP e pela APAV quanto ao universo criminal.

Neste capítulo, opta-se por apresentar a informação e a análise através de uma tabela com os números em consideração, seguida de gráficos que permitem a visualização de domínios e tendências, terminando com os destaques que fazem uma interpretação dos aspetos considerados mais importantes. No final de cada subcapítulo, apresenta-se uma síntese.

EMPRESAS E INDIVÍDUOS

As organizações, em particular as empresas, são um dos atores mais importantes do ciberespaço, visto constituírem grande parte do tecido económico. São, por isso, um representante importante da esfera profissional. Quanto ao espaço privado, os indivíduos, na sua vida não profissional, são o elemento a considerar quando pretendemos ter dados sobre o quotidiano individual e doméstico.

Apresentamos de seguida alguns dados do Eurostat sobre estes dois atores no que diz respeito à experiência de incidentes de cibersegurança. Quanto às empresas, recorre-se ao inquérito *Security incidents and consequences*[1], com números de 2019 sobre incidentes experienciados pelas empresas em Portugal.

1. Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: indisponibilidade de serviços TIC, 2019* (%)

	Portugal	UE27
***Todas as empresas** (10 pessoas empregadas ou mais)*	7	10
***Pequenas empresas** (10-49 pessoas empregadas)*	6	9
***Médias empresas** (50-249 pessoas empregadas)*	9	14
***PME** (10-249 pessoas empregadas)*	7	10
***Grandes empresas** (250 pessoas empregadas ou mais)*	11	19
Empresas do setor da elet., gás, vapor, ar cond. e água	7	11
Empresas de transportes e armazenamento	9	8
Empresas de informação e comunicação	12	16
Empresas do setor das TIC	10	15
Empresas de telecomunicações	17	22

*Sem contar com o setor financeiro.

Tabela 1 | Eurostat 2020a

1 A descrição da metodologia aplicada na recolha destes e dos restantes dados é descrita no capítulo "H. Notas Metodológicas".

Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: indisponibilidade de serviços TIC, 2019 (%)

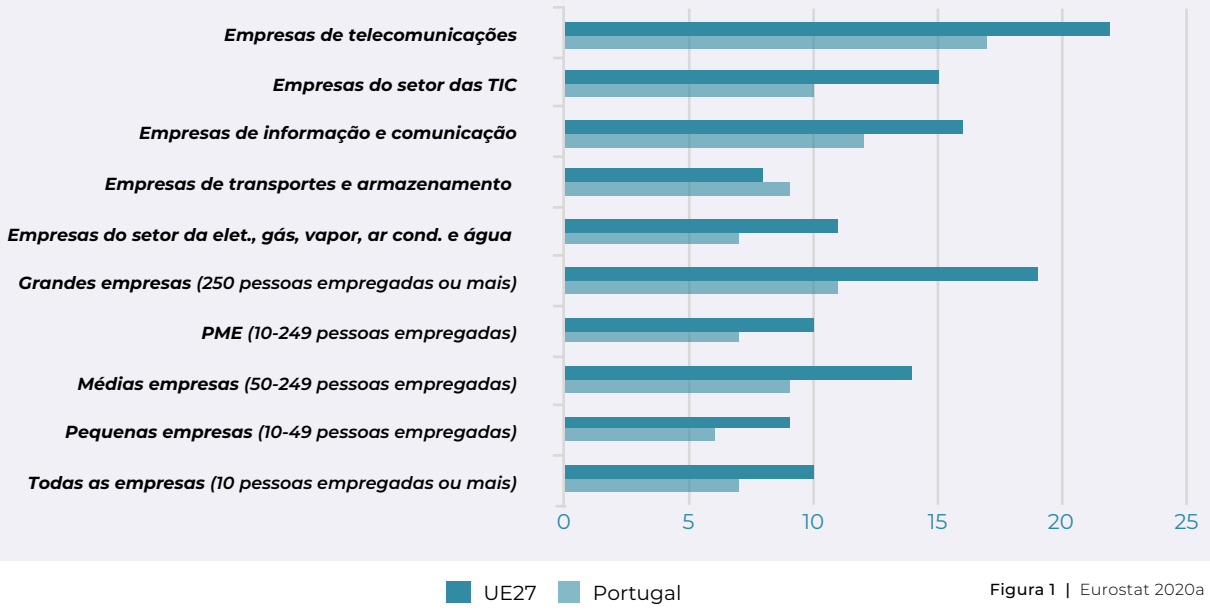


Figura 1 | Eurostat 2020a

DESTAQUES

Portugal apresenta percentagens quase sempre inferiores às médias da UE no que se refere às empresas que reconhecem ter experienciado incidentes de segurança de TIC em 2019 relacionados com indisponibilidade de serviço, sendo a única exceção as empresas de transportes e armazenamento (9% em Portugal e 8% na UE).

A maior discrepância em relação à UE ocorre no que diz respeito às grandes empresas, em que 19%, na UE, admitem ter sido vítimas de incidentes de indisponibilidade de serviço, enquanto em Portugal apenas 11% o admitiram.

Tanto em Portugal como na UE, o tipo de empresas que mais admitem ter sofrido este género de incidente foram as de telecomunicações (17% em Portugal e 22% na UE).

Entre os vários tipos de incidentes avaliados neste inquérito, o de indisponibilidade de serviço é o que todas as empresas mais reconhecem ter experienciado – 7% em Portugal e 10% na UE.

2. Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: destruição ou corrupção de dados, 2019* (%)

	Portugal	UE27
Todas as empresas (10 pessoas empregadas ou mais)	4	6
Pequenas empresas (10-49 pessoas empregadas)	3	5
Médias empresas (50-249 pessoas empregadas)	7	8
PME (10-249 pessoas empregadas)	4	6
Grandes empresas (250 pessoas empregadas ou mais)	5	10
Empresas do setor da elet., gás, vapor, ar cond. e água	5	6
Empresas de transportes e armazenamento	1	5
Empresas de informação e comunicação	2	6
Empresas do setor das TIC	2	6
Empresas de telecomunicações	0	6

*Sem contar com o setor financeiro.

Tabela 2 | Eurostat 2020a

Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: destruição ou corrupção de dados, 2019 (%)

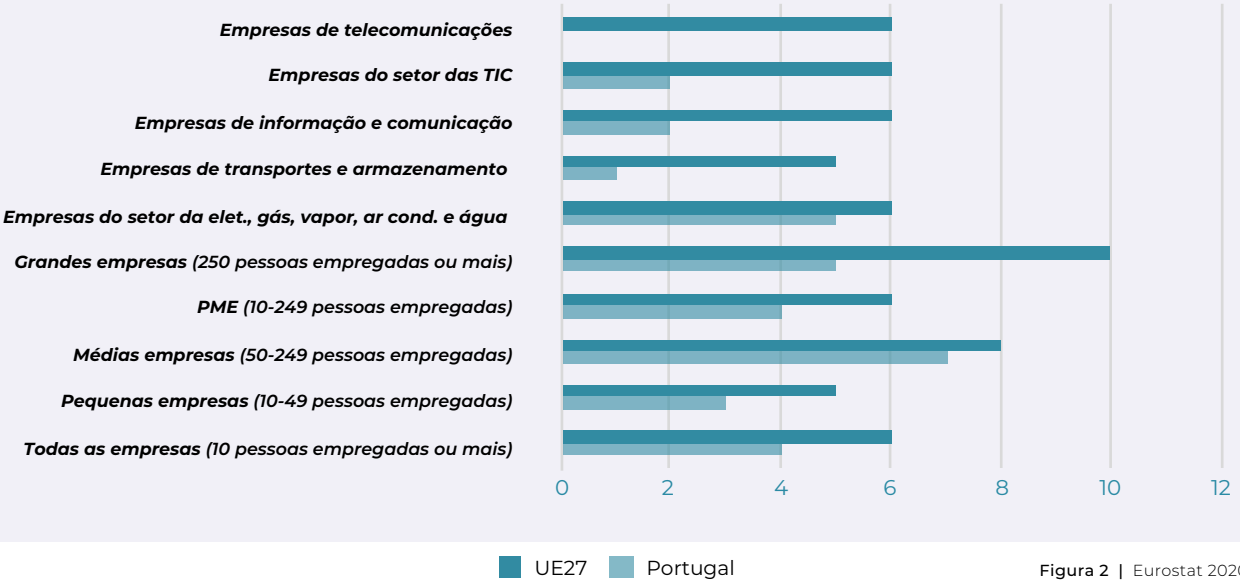


Figura 2 | Eurostat 2020a

DESTAQUES

Também no domínio dos incidentes de segurança de TIC respeitantes à destruição ou corrupção de dados, Portugal apresenta em 2019 percentagens inferiores às médias da UE relativas a empresas que assumem ter experienciado este tipo de incidentes.

As discrepâncias mais relevantes ocorrem nas empresas de telecomunicações (0% em Portugal e 6% na UE) e, mais uma vez, nas grandes empresas (5% em Portugal e 10% na UE).

3. Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: desocultação de dados confidenciais[2], 2019* (%)

	Portugal	UE27
***Todas as empresas** (10 pessoas empregadas ou mais)*	1	1
***Pequenas empresas** (10-49 pessoas empregadas)*	1	1
***Médias empresas** (50-249 pessoas empregadas)*	3	2
***PME** (10-249 pessoas empregadas)*	1	1
***Grandes empresas** (250 pessoas empregadas ou mais)*	3	4
Empresas do setor da elet., gás, vapor, ar cond. e água	2	2
Empresas de transportes e armazenamento	0	1
Empresas de informação e comunicação	1	2
Empresas do setor das TIC	2	2
Empresas de telecomunicações	0	4

*Sem contar com o setor financeiro.

Tabela 3 | Eurostat 2020a

Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC: desocultação de dados confidenciais, 2019 (%)

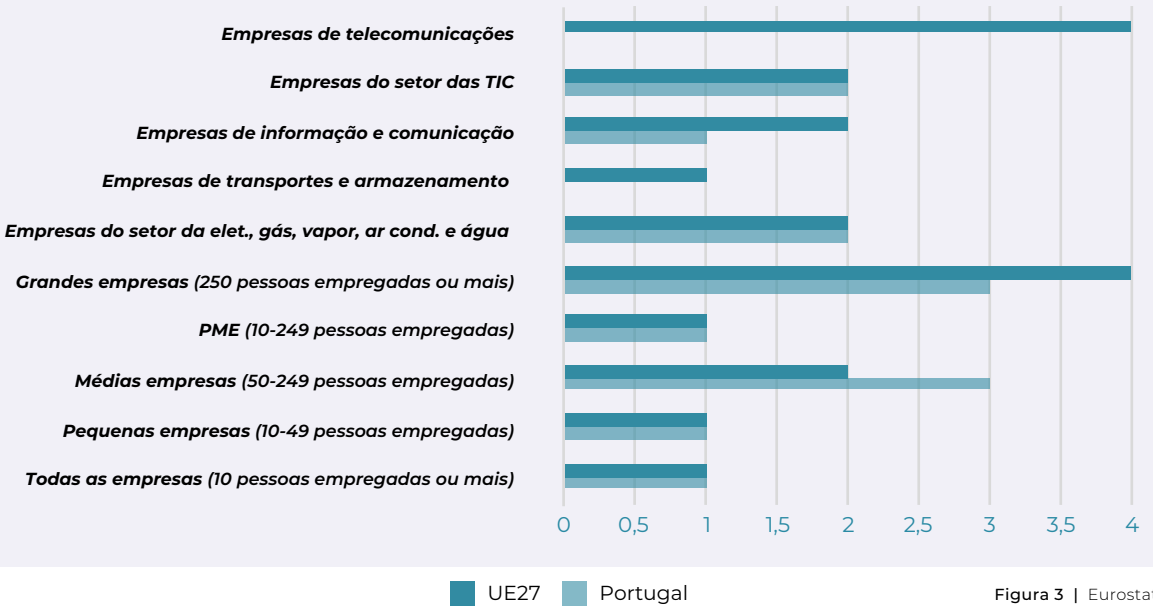


Figura 3 | Eurostat 2020a

2 Quando se faz referência a "dados confidenciais" não está incluída a informação classificada com o grau "Confidencial", conforme definido no SEGNAC 1.

Os incidentes de segurança de TIC relativos à desocultação de dados confidenciais são os menos reportados, comparando com os restantes tipos de incidentes, reconhecidos por apenas 1% da totalidade das empresas em Portugal e na UE.

Este tipo de incidentes é também aquele que mais aproxima Portugal das médias da UE, sendo as percentagens coincidentes para alguns tipos de empresas.

A discrepância com percentagem mais elevada para a UE verifica-se nas empresas de telecomunicações, que em Portugal não reportaram incidentes de desocultação de dados confidenciais (0% em Portugal e 4% na UE).

A discrepância com maior percentagem para Portugal verifica-se nas médias empresas (3% em Portugal e 2% na UE).

4. Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC (indisponibilidade de serviços de TIC, destruição ou corrupção de dados, desocultação de dados confidenciais), 2019* (%)

	Portugal	UE27
***Todas as empresas** (10 pessoas empregadas ou mais)*	8	13
***Pequenas empresas** (10-49 pessoas empregadas)*	8	12
***Médias empresas** (50-249 pessoas empregadas)*	11	18
***PME** (10-249 pessoas empregadas)*	8	13
***Grandes empresas** (250 pessoas empregadas ou mais)*	14	25
Empresas do setor da elet., gás, vapor, ar cond. e água	8	15
Empresas de transportes e armazenamento	9	11
Empresas de informação e comunicação	12	19
Empresas do setor das TIC	12	18
Empresas de telecomunicações	17	24

*Sem contar com o setor financeiro.

Tabela 4 | Eurostat 2020a

Empresas que experienciaram pelo menos uma vez problemas devido a um incidente de segurança de TIC (indisponibilidade de serviços de TIC, destruição ou corrupção de dados, desocultação de dados confidenciais), 2019 (%)

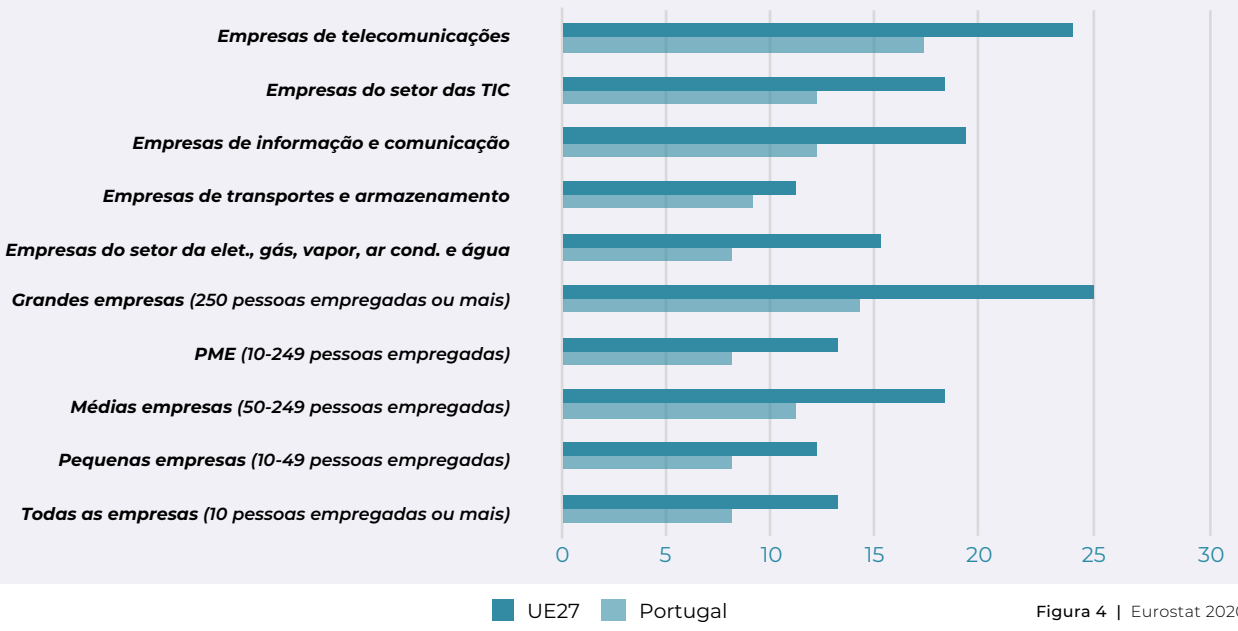


Figura 4 | Eurostat 2020a

Há menos empresas em Portugal a indicarem ter experienciado pelo menos um destes três tipos de incidentes de segurança de TIC, apresentando o país na generalidade percentagens inferiores às médias da UE. No que diz respeito a todas as empresas, 8% em Portugal e 13% na UE assumiram ter tido pelo menos um destes tipos de incidentes em 2019.

Existe maior discrepância nas grandes empresas (14% em Portugal e 25% na UE) e nas empresas de média dimensão (11% em Portugal e 18% na UE). Não obstante, em ambos os casos, são os tipos de empresas em termos de dimensão que mais relatam experienciar incidentes.

Em Portugal, no que diz respeito ao setor, é entre as empresas de telecomunicações (17%) que mais se indica ter experienciado incidentes de segurança de TIC – embora unicamente de indisponibilidade de serviço; tendência que também se verifica na UE (24%) – neste caso, nos vários tipos de incidentes de segurança.

O tipo de incidente que as empresas em Portugal e na UE mais reconhecem ter experienciado é o de indisponibilidade de serviço (7% em Portugal e 10% na UE), seguindo-se os incidentes relacionados com a destruição ou corrupção de dados (4% em Portugal e 6% na UE). A desocultação de dados confidenciais foi reportada apenas por 1% em Portugal e na UE.

5. Empresas que não experienciaram qualquer problema devido a um incidente de segurança relacionado com TIC (indisponibilidade de serviços de TIC, destruição ou corrupção de dados, desocultação de dados confidenciais), 2019* (%)

	Portugal	UE27
***Todas as empresas** (10 pessoas empregadas ou mais)*	91	84
***Pequenas empresas** (10-49 pessoas empregadas)*	91	85
***Médias empresas** (50-249 pessoas empregadas)*	89	81
***PME** (10-249 pessoas empregadas)*	91	85
***Grandes empresas** (250 pessoas empregadas ou mais)*	86	75
Empresas do setor da elet., gás, vapor, ar cond. e água	91	84
Empresas de transportes e armazenamento	91	86
Empresas de informação e comunicação	88	80
Empresas do setor das TIC	88	80
Empresas de telecomunicações	83	74

*Sem contar com o setor financeiro.

Tabela 5 | Eurostat 2020a

Empresas que não experienciaram qualquer problema devido a um incidente de segurança relacionado com TIC (indisponibilidade de serviços de TIC, destruição ou corrupção de dados, desocultação de dados confidenciais), 2019 (%)

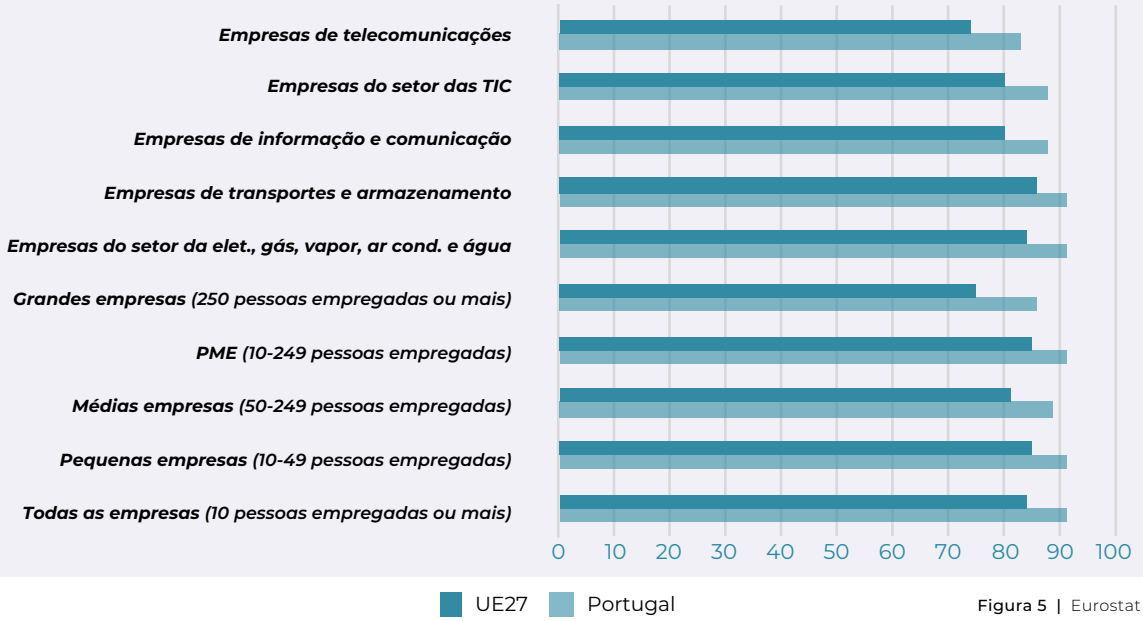


Figura 5 | Eurostat 2020a

Com alguma redundância em relação ao indicador anterior, mas não totalmente (pois exclui outras respostas para lá da afirmação ou da negação), estes dados mostram que em Portugal há mais empresas a afirmar não terem experienciado incidentes de segurança de TIC do que na UE. Por exemplo, em Portugal, considerando todas as empresas, 91% afirmam não ter experienciado incidentes, enquanto na UE os valores atingem os 84%.

A maior discrepância verifica-se entre as grandes empresas (86% em Portugal e 75% na UE), em consonância com o indicador anterior.

6. Empresas com seguro contra incidentes de segurança em TIC, 2019* (%)

	Portugal	UE27
***Todas as empresas** (10 pessoas empregadas ou mais)*	10	21
***Pequenas empresas** (10-49 pessoas empregadas)*	8	20
***Médias empresas** (50-249 pessoas empregadas)*	15	28
***PME** (10-249 pessoas empregadas)*	9	21
***Grandes empresas** (250 pessoas empregadas ou mais)*	21	35
Empresas do setor da elet., gás, vapor, ar cond. e água	10	19
Empresas de transportes e armazenamento	12	17
Empresas de informação e comunicação	20	43
Empresas do setor das TIC	22	42
Empresas de telecomunicações	21	36

*Sem contar com o setor financeiro.

Tabela 6 | Eurostat 2020a

Empresas com seguro contra incidentes de segurança em TIC, 2019 (%)

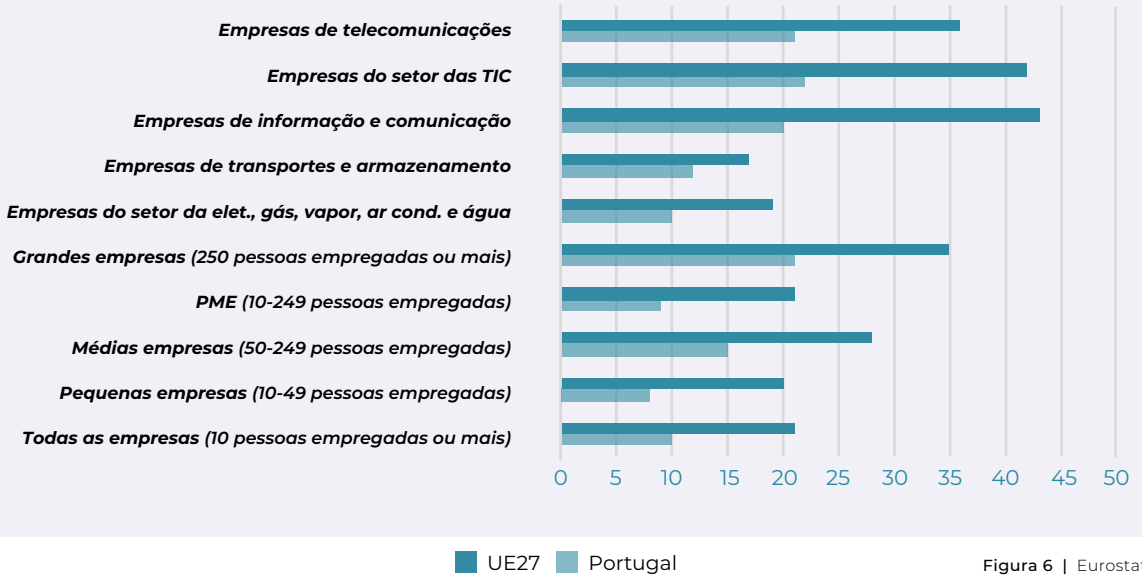


Figura 6 | Eurostat 2020a

DESTAQUES

Existem menos empresas em Portugal com seguro contra incidentes de segurança de TIC. Considerando todas as empresas, os valores são de 10% para Portugal e 21% para a média da UE.

As maiores discrepâncias verificam-se nas empresas de informação e comunicação (20% em Portugal e 43% na UE) e nas empresas do setor das TIC (22% em Portugal e 42% na UE).

Igualmente do Eurostat, com dados relativos a incidentes em 2019, mas concernentes a indivíduos quando usam a *internet* para fins privados, o inquérito *Security related problems experienced through using the internet for private purposes* é particularmente pertinente, nomeadamente porque permite fazer leituras sociodemográficas.

7. Indivíduos que experienciaram incidentes de segurança no uso da *internet* para fins privados, por tipo de incidente, 2019* (%)

	Portugal	UE27
Pelo menos um incidente de segurança reportado	27	37
Uso de cartão de crédito ou débito fraudulento	2	3
Perda de docs., fotos ou outros tipos de dados devido a vírus ou outra infeção informática	4	4
Má utilização de inform. pessoal na internet resultando em e.g. discriminação, assédio, bullying	1	2
Rede social ou email foi alvo de hacking e conteúdo publicado ou enviado sem conhecimento	2	3
Roubo de identidade online	1	1
Receber mensagens fraudulentas (phishing)	18	28
Ser redirecionado para websites falsos que solicitam informação pessoal (pharming)	15	13
Experienciou perda financeira em resultado de roubo de identidade, phishing ou pharming	1	1
Crianças a aceder a websites inapropriados	1	3

* Indivíduos que usaram a *internet* no último ano.

Tabela 7 | Eurostat 2020b

Aspetos sociodemográficos relevantes Portugal 2019

Género	Sem diferenças relevantes entre géneros.
Idade	Indivíduos com idades compreendidas entre os 25 e os 34 anos tendem a reconhecer mais ter sofrido incidentes (35%) do que os indivíduos com idades entre os 65 e os 74 anos (18%).
Educação	Em geral, indivíduos entre os 25 e os 64 anos, com uma educação formal superior, tendem a identificar mais incidentes (40%) do que aqueles que, na mesma faixa etária, têm uma educação formal inferior (17%).

Indivíduos que experienciaram incidentes de segurança no uso da *internet* para fins privados, por tipo de incidente, 2019 (%)

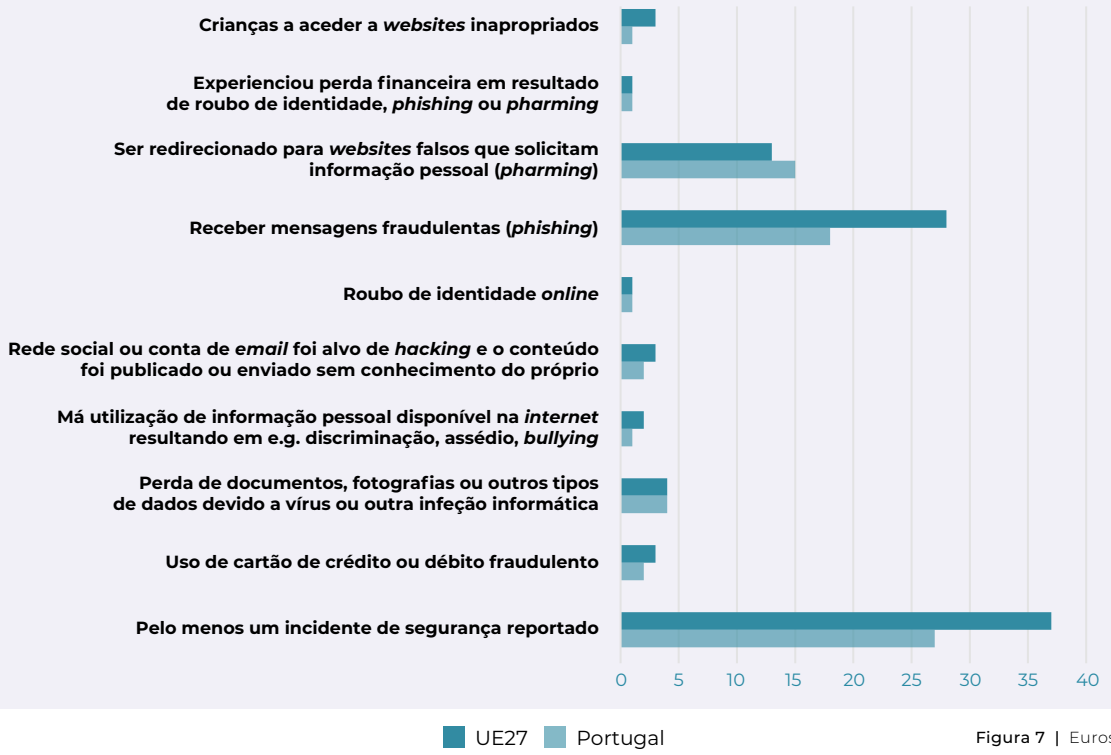


Figura 7 | Eurostat 2020b

DESTAQUES

Em Portugal, quase um terço dos inquiridos (27%) reconhece ter experienciado pelo menos um dos incidentes de segurança mencionados no uso da *internet* para fins privados, enquanto na UE mais de um terço o reconhecem (37%).

Os tipos de incidentes de segurança mais identificados pelos indivíduos no uso da *internet* para fins privados em Portugal são o *phishing* (18%) e o *pharming* (15%), tal como na UE (28% e 13%, respetivamente).

Indivíduos com idades entre os 25 e os 34 anos (35%) e indivíduos com estudos superiores (40%) tendem a reconhecer mais que sofreram incidentes de segurança no uso da *internet* para fins privados do que aqueles que têm entre 65 e 74 anos (18%) e aqueles que não têm estudos superiores (17%).

Síntese do Subcapítulo Empresas e Indivíduos

Em inquéritos realizados a empresas e indivíduos, em Portugal é relatado um menor número de incidentes de cibersegurança experienciados do que a média da UE.

Tendencialmente, é entre as grandes empresas e as de telecomunicações (embora estas apenas de indisponibilidade de serviço) que mais se relata terem sido experienciados incidentes de indisponibilidade de serviço (com maior número do que os restantes), destruição ou corrupção de dados e desocultação de dados confidenciais.

Existem menos empresas em Portugal com seguro contra incidentes de segurança em TIC do que a média da UE.

Ao nível dos indivíduos, quase um terço dos portugueses inquiridos já experienciou pelo menos um tipo de incidente de segurança no uso da *internet* para fins privados.

Os tipos de incidentes de segurança mais experienciados no uso da *internet* para fins privados são o *phishing* e o *pharming*.

Portugueses entre os 25 e os 34 anos e portugueses com estudos superiores reconhecem mais do que outros que experienciaram incidentes de segurança no uso da *internet* para fins privados.

CIBERESPAÇO DE INTERESSE NACIONAL

De acordo com a ENSC 2019-2023[3], o 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". Deste ponto de vista, o ciberespaço não se reduz à esfera dita virtual das atividades na *internet*, embora esse seja o seu campo privilegiado. Ele inclui todas as "interações entre redes, pessoas e sistemas de informação". Assim, a atividade digital num dispositivo não conectado tem implicações no ciberespaço; as instituições que estão presentes na rede são atores do ciberespaço; as estratégias governamentais atravessam o ciberespaço; e os indivíduos, em geral, mesmo que não queiram, têm atividades, pelo menos registadas, no ciberespaço. Acresce que, devido ao caráter não-territorial das redes do ciberespaço, este, ainda que tenha condicionamentos territoriais fruto da soberania nacional, é demasiado permeável para que o possamos reduzir apenas a um território nacional. Por essa razão, quando se faz referência ao ciberespaço nacional, e também de acordo com a ENSC 2019-2023, é mais adequado designar o "ciberespaço de interesse nacional", na medida em que este se refere a entidades não necessariamente confinadas ao território português, mas que nele têm implicações.

O objetivo deste subcapítulo é analisar os incidentes e outros eventos relevantes que ocorreram no ciberespaço de interesse nacional, em 2019 e anos anteriores. Para o efeito, utilizam-se indicadores sobretudo do CERT.PT e da RNCSIRT, além de alguma informação disponibilizada pela CNPD. Os dados que se apresentam são representativos do ciberespaço de interesse nacional na medida em que são recolhidos pelo CNCS, no qual se incluem os serviços do CERT.PT, e por uma rede de instituições-chave no país (RNCSIRT)[4]. Tratando-se de uma representação, não corresponde à totalidade do ciberespaço de interesse nacional, mas, ainda assim, apresenta indicadores muito fortes dos incidentes predominantes nesta esfera.

3 ENSC 2019-2023: https://dre.pt/home/-/dre/122498962/details/maximized

4 Para uma consulta aos membros da RNCSIRT, visitar: https://www.redecsirt.pt

8. Incidentes por tipo registados pelo CERT.PT, 2018 e 2019 – *ranking* top 10*

2018				2019				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta	Lugar RK
1º	*Phishing*	176	29	1º	*Phishing*	236	31	+	=
2º	Infeção *(malware)*	132	22	2º	Infeção *(malware)*	123**	16	-	=
3º	Distribuição *(malware)*	71	12	3º	Compromisso de Conta	95	13	+	+
4º	*Scan*	54	9	4º	Exp. de vuln. (intrusão)	58	8	+	+
5º	Exp. de vuln. (intrusão)	40	7	5º	Distribuição *(malware)*	55	7	-	-
6º	Tentativa de *login*	25	4	6º	Tentativa de *login*	30	4	+	=
7º	Compromisso de Conta	21	4	7º	*Scan*	28	4	-	-
8º	Exp. de vuln. (tentativa de intrusão)	19	3	8º	DoS/DDoS	27	4	+	+
9º	SPAM	15	3	9º	Utilização ilegítima de nome de terceiros	19	3	+	+
10º	*Blacklist*	12	2	10º	Exp. de vuln. (tentativa de intrusão)	18	2	-	-

* Para uma leitura completa de todos os tipos e classes de incidentes, consultar Anexo.
** dos quais, 24 são de *ransomware*.

Tabela 8 | CERT.PT

Incidentes por tipo registados pelo CERT.PT, 2019 – *ranking* top 10. Por mês.

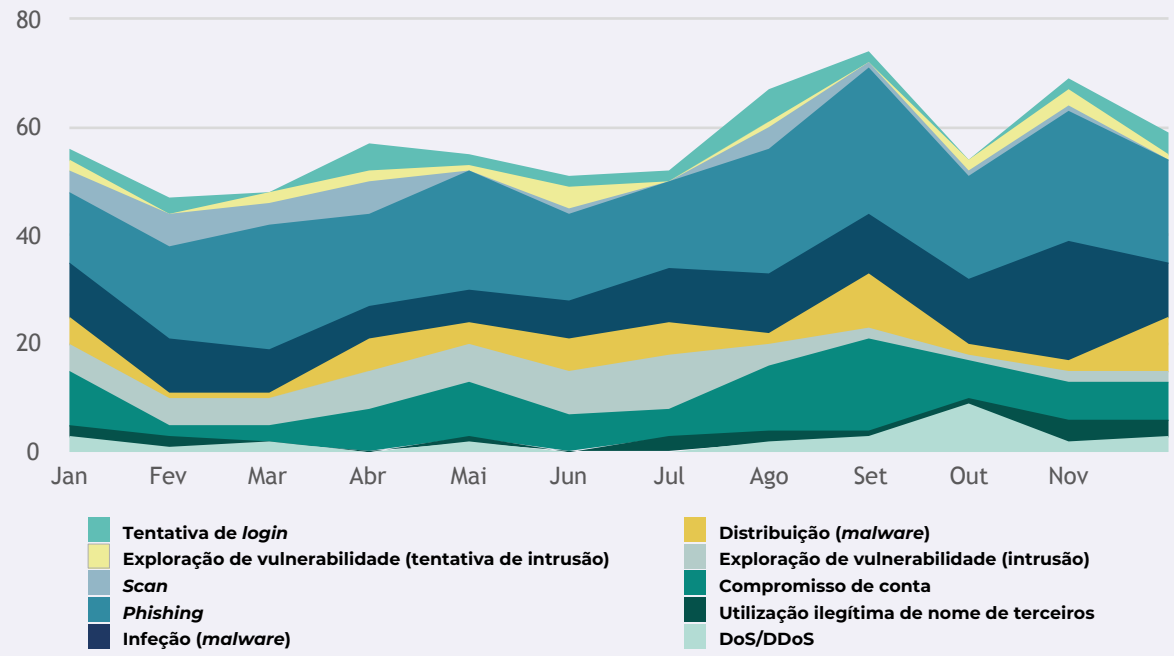


Figura 8 | CERT.PT

Incidentes por tipo registados pelo CERT.PT, 2019 – TOTAL. Percentagem de cada mês no total.

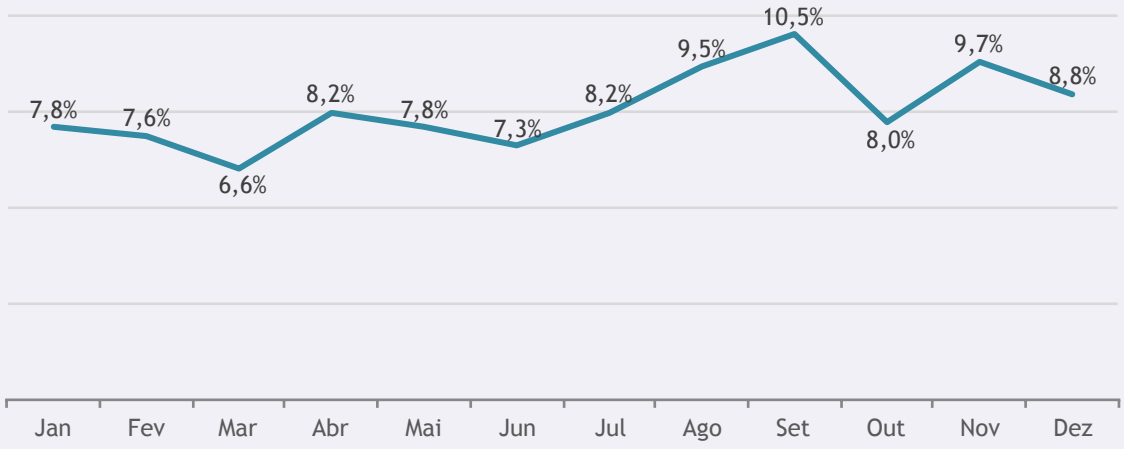


Figura 9 | CERT.PT

Incidentes regitados pelo CERT.PT por trimestre e semestre, 2019

Trimestre	1º tri.	2º tri.	3º tri.	4º tri.
Nº por trimestre	166	176	213	199
Nº por semestre	342		412	

Tabela 9 | CERT.PT

DESTAQUES

O *phishing*, a infeção por *malware* (dos quais 24 são *ransomware*) e o compromisso de conta são os tipos de incidentes registados pelo CERT.PT mais frequentes em 2019, correspondendo a 31%, 16% e 13% do total, respetivamente. Em relação ao ano anterior, esta ordenação corresponde a uma manutenção dos dois primeiros tipos de incidentes nos mesmos lugares no *ranking* e a uma subida do compromisso de conta do sétimo (4%) para o terceiro lugar (13%).

Há uma descida no número de casos de distribuição de *malware* e de *scans*, passando de terceiro e quarto para quinto e sétimo lugares, respetivamente.

Os meses com o maior número de incidentes registados são os de setembro e novembro. O terceiro trimestre e o segundo semestre são, por sua vez, os períodos que apresentam mais incidentes registados.

9. Incidentes por setor e área governativa, registados pelo CERT.PT, 2019 - *ranking* top 15*/**

RK	Setor e Área Governativa[5]	Nº	%
1º	Outros	251	28
2º	Infraestruturas Digitais	170	19
3º	Prestadores de Serviços de Internet	167	18
4º	Educação, Ciência, Tecnologia e Ensino Superior	81	9
5º	Banca	69	8
6º	Transportes	30	3
7º	Serviços de Computação em Nuvem	26	3
8º	Administração Local	18	2
9º	Saúde	11	1
10º	Infraestruturas do Mercado Financeiro	11	1
11º	Energia	9	1
12º	Defesa Nacional	9	1
13º	Órgãos de Soberania	9	1
14º	Presidência do Conselho de Ministros	9	1
15º	Agricultura	7	0,8

* Para uma leitura completa de todos os incidentes por setor e área governativa, consultar Anexo.
** 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.

Tabela 10 | CERT.PT

DESTAQUES

"Outros" setores e áreas governativas variados, que não os da tipologia adotada, são aqueles que sofreram mais incidentes entre os registados pelo CERT.PT em 2019, com 28% do total. As Infraestruturas Digitais (19%), os Prestadores de Serviços de Internet (18%), as entidades ligadas à Educação, Ciência, Tecnologia e Ensino Superior (9%) e a Banca (8%) ocupam os restantes lugares no *ranking* dos setores e áreas governativas.

A prevalência das Infraestruturas Digitais e dos Prestadores de Serviços de Internet tem relação com o facto dos mesmos prestarem serviços a clientes (organizações e particulares), eles próprios vítimas, independentemente das ações das infraestruturas ou dos prestadores em causa.

5 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 46/2018. Nos termos do artigo 31 da Lei 46/2018 de 13 de agosto que estabelece o regime jurídico da segurança do ciberespaço, os requisitos de notificação de incidentes previstos nos artigos 15 (1), 17 (1) e 19 (1) são definidos em legislação própria, não tendo havido ainda publicação oficial deste normativo. Assim, os dados apresentados neste Relatório baseiam-se, maioritariamente, no estabelecido no artigo 20 da referida Lei, 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. Para consultar a Lei 46/2018: https://dre.pt/web/guest/pesquisa/-/search/116029384/details/maximized.

10. Total de incidentes registados pelo CERT.PT, entre 2015 e 2019, e mês, trimestre e semestre com mais registos

	Total	Tend.	M. mais	T. mais	S. 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	+18%	Mar. (57)	4º (143)	2º (255)
2018	599	+16%	Out. (68)	2º (169)	1º (301)
2019	754	+26%	Set. (79)	3º (213)	2º (412)

Tabela 11 | CERT.PT

Total de incidentes registados pelo CERT.PT, entre 2015 e 2019

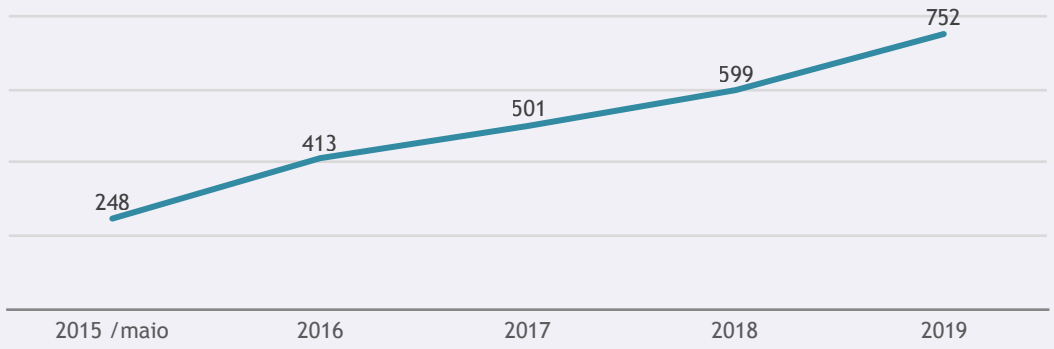


Figura 10 | CERT.PT

DESTAQUES

Desde 2015 (maio), o número de incidentes registados anualmente pelo CERT.PT tem aumentado de forma consistente, tendo em 2019 crescido 26% em relação ao ano anterior, passando de 599 registos em 2018 para 754 em 2019 – este aumento poderá estar ligado a um efetivo incremento no número de incidentes, mas também deve ser lido considerando a crescente visibilidade do CERT.PT sobre o ciberespaço de interesse nacional e um crescimento no número de incidentes comunicados voluntariamente, fruto em parte de um melhor conhecimento do CERT.PT por parte da comunidade.

Existe alguma variação quanto aos trimestres e semestres mais predominantes em termos do número de incidentes registados. Contudo, nos últimos dois anos, os meses com mais incidentes encontram-se no segundo semestre, setembro (2019) e outubro (2018).

11. Total de vulnerabilidades registadas pelo CERT.PT, entre 2015 e 2019, e mês, trimestre e semestre com mais registos

	Total	Tend.	M. mais	T. mais	S. mais
2015 (desde maio)	3	N/A	N/A	N/A	N/A
2016	12	N/A	Jan. e Fev. (3)	1º (6)	1º (7)
2017	38	+217%	Mar. e Abr. (10)	1º (15)	1º (28)
2018	33	-16%	Ago. (7)	4º (12)	2º (22)
2019	79	+139%	Ago. (12)	3º (28)	2º (43)

Tabela 12 | CERT.PT

Total de vulnerabilidades registadas pelo CERT.PT, entre 2015 e 2019

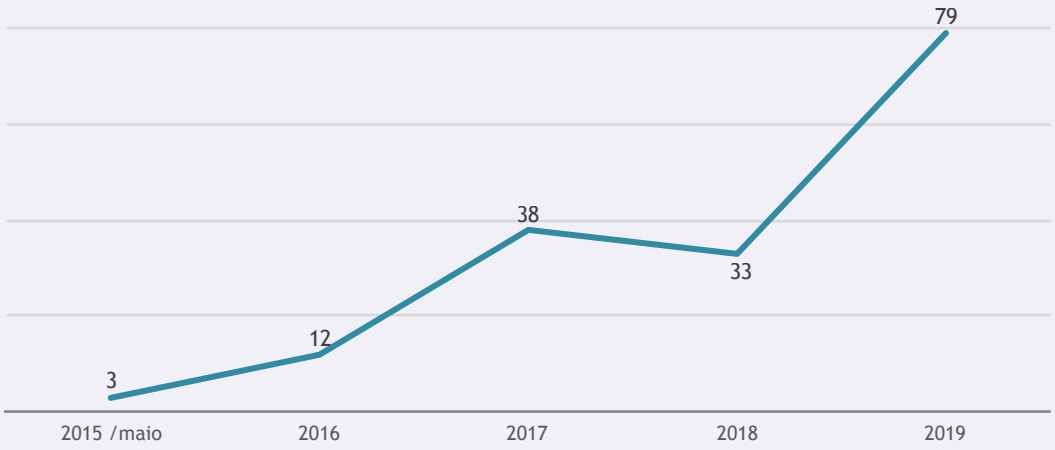


Figura 11 | CERT.PT

DESTAQUES

Desde 2015 (maio), o número de vulnerabilidades registadas pelo CERT.PT tem aumentado consistentemente, tendo em 2019 aumentado 139% em relação ao ano anterior, passando de 33 registos em 2018 para 79 em 2019; entre 2017 e 2018, excecionalmente, há uma ligeira diminuição, em 16%.

Nos últimos dois anos, o mês de agosto é aquele que apresenta mais registos de vulnerabilidades. Também nos últimos dois anos o segundo semestre foi aquele que apresentou mais vulnerabilidades registadas, havendo uma coincidência entre esta tendência e a dos incidentes de 2019.

12. Observáveis por tipo registados pelo CERT.PT, 2018 e 2019 - *ranking* top 10*

2018				2019				Ordenação	
RK	Tipo	Nº	%	RK	Tipo	Nº	%	Tendência absoluta	Lugar RK
1º	Serviço vulnerável	51072898	92	1º	Serviço vulnerável	50932870	93	-	=
2º	*Blacklist*	2885642	5	2º	*Blacklist*	2530931	5	-	=
3º	*Botnet drone*	1030717	2	3º	*Botnet dronet*	887418	2	-	=
4º	*Malware*	405866	0,7	4º	*Malware*	290463	1	-	=
5º	*Scan*	68748	0,1	5º	Força-bruta	103199	0,1	+	+
6º	*Phishing*	58142	0,1	6º	*Scan*	43530	0,07	-	-
7º	Força-bruta	47331	0,08	7º	Outro	38695	0,07	+	+
8º	C&C	21626	0,03	8º	*Phishing*	31625	0,05	-	-
9º	Comprom.	7937	0,01	9º	Nulos	31363	0,05	+	+
10º	Alerta IDS	7830	0,01	10º	Alerta IDS	17494	0,03	+	=

* Para uma leitura completa dos Observáveis por tipo registados pelo CERT.PT, consultar Anexo.

Tabela 13 | CERT.PT

Observáveis por tipo registados pelo CERT.PT, 2018 e 2019 - *ranking* top 10.
Nº de observáveis por mês.

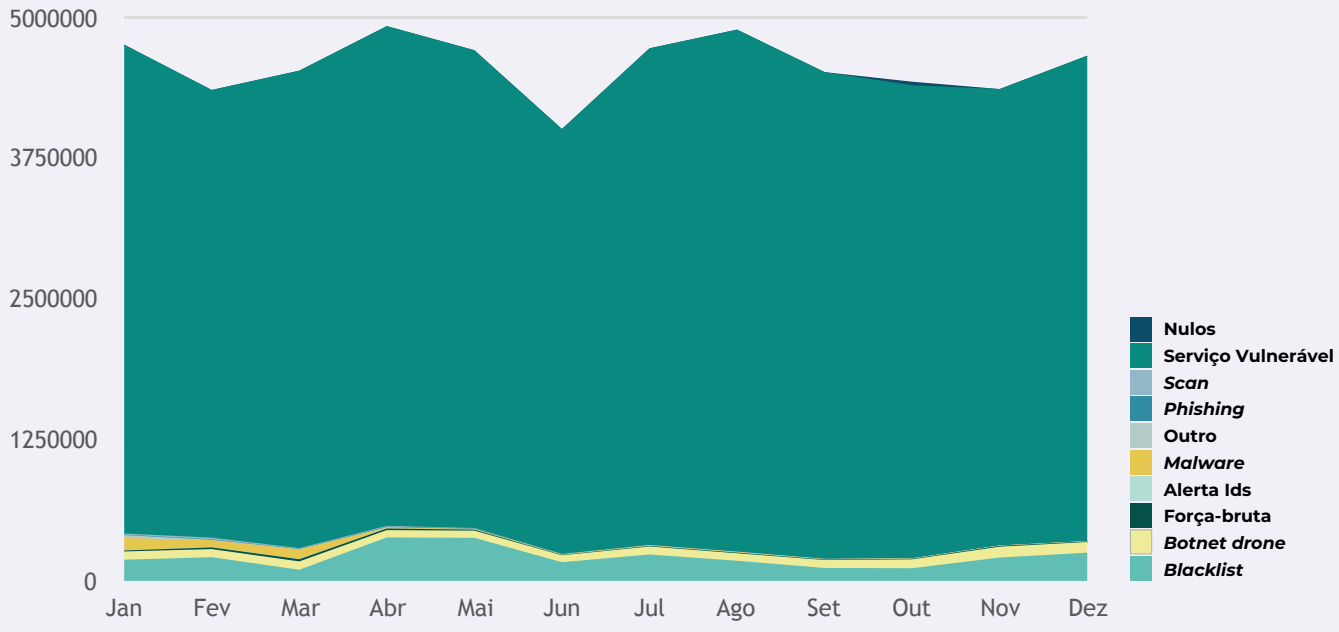


Figura 12 | CERT.PT

Observáveis por tipo registados pelo CERT.PT, 2019 - Total. Percentagem de cada mês no total.

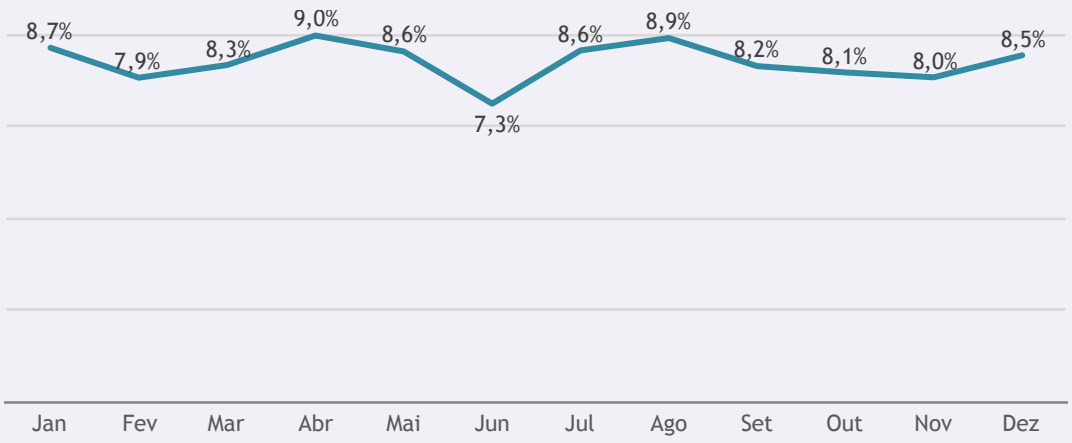


Figura 13 | CERT.PT

Observáveis registados pelo CERT.PT por trimestre e semestre, 2019

Trimestre	**1º tri.**	**2º tri.**	**3º tri.**	**4º tri.**
Nº por trimestre	13660254	13657588	14142871	13464653
Nº por semestre	27317842		27607524	

Tabela 14 | CERT.PT

DESTAQUES

Com grande destaque, em 2018 e 2019, o tipo de observável mais registado é o serviço vulnerável (mais de 90% dos registos nos dois anos), seguido de *blacklist* (5% em 2019) e de *botnet drone* (2% em 2019).

Entre 2018 e 2019, destacam-se ainda a diminuição dos observáveis relativos a *phishing* e o aumento dos respeitantes a força-bruta.

Em termos de incidentes observáveis, deve assinalar-se um menor peso do *phishing* comparando com o *malware* – possivelmente, essa diferença tem a ver com a natureza social desta ameaça, o que promove a identificação social e menos a automatizada.

Os meses de abril e agosto são os meses com mais observáveis registados pelo CERT.PT. O mês de junho apresentou uma diminuição assinalável.

O terceiro trimestre e o segundo semestre apresentam o maior número de registos, o que coincide com os dados relativos aos incidentes.

13. Observáveis por setor e área governativa registados pelo CERT.PT, 2019 - *ranking* top 15*

RK	Setor e Área Governativa	Nº	%
1º	Prestadores de Serviços de Internet	31248303	57
2º	Infraestruturas Digitais	10610563	19
3º	Nulos	8181627	15
4º	Educação, Ciência, Tecnologia e Ensino Superior	1398687	3
5º	Outros	1375993	3
6º	Nenhum	1350890	2
7º	Serviços de Computação em Nuvem	394906	0,7
8º	Administração Pública	320816	0,5
9º	Energia	12886	0,02
10º	Transportes	12225	0,02
11º	Administração Central	5733	0,01
12º	Órgãos de Soberania	2320	0,004
13º	Presidência do Conselho de Ministros	1750	0,003
14º	Prestadores de Serviços Digitais	1640	0,002
15º	Administração Local	1584	0,002

* Para uma leitura completa dos observáveis por setor e área governativa registados pelo CERT.PT, consultar Anexo.

Tabela 15 | CERT.PT

DESTAQUES

Os setores e áreas governativas nos quais se identifica o maior número de observáveis registados são os Prestadores de Serviços de Internet (57%) e as Infraestruturas Digitais (19%), bem como a Educação, Ciência, Tecnologia e Ensino Superior (3%) (não considerando os nulos). Também neste caso, a prevalência dos dois primeiros setores tem relação com o facto de muitos destes registos se referirem a clientes destas entidades, tal como explicado no indicador 9.

14. Total de observáveis registados pelo CERT.PT, entre 2015 e 2019

	Nº de Observáveis	Tend.
***2015** (desde maio)*	4117875	N/A
2016	2931767	N/A
2017	42956624	+1365%
2018	55607704	+29%
2019	54925366	-1%

Tabela 16 | CERT.PT

Total de observáveis registados pelo CERT.PT, entre 2015 e 2019

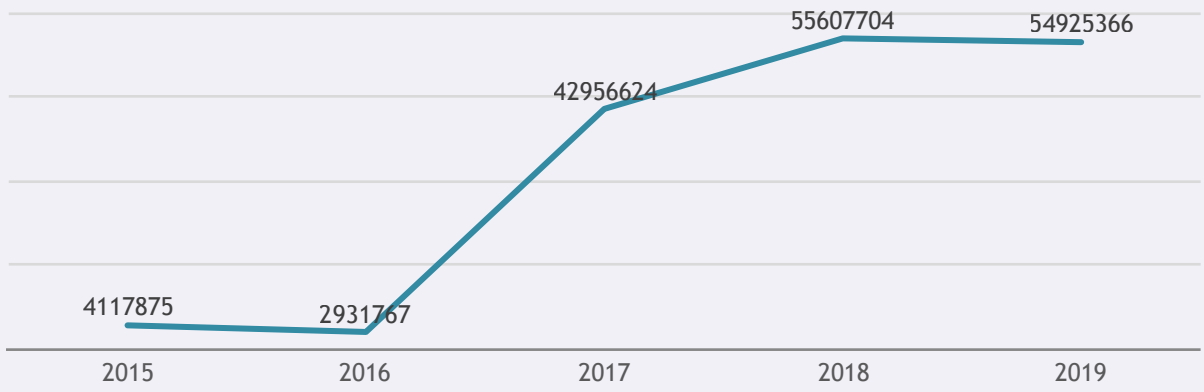


Figura 14 | CERT.PT

DESTAQUES

Entre 2018 e 2019 o número de observáveis manteve-se estável, com ligeira descida de 1%. As variações dos anos anteriores prendem-se com alterações nos tipos e quantidades de fontes.

15. Incidentes registados pelo CERT.PT vs. RNCSIRT, 2019 - *ranking* top 10*

2019 CERT.PT				2019 RNCSIRT (inclui CERT.PT)				
RK	Tipo	Nº	%	RK	Tipo	Nº	%	RNCSIRT em relação a CERT.PT no *Ranking*
1º	*Phishing*	236	31	1º	Infeção (*malware*)	2026	13	+
2º	Infeção (*malware*)	123	16	2º	*Phishing*	1946	13	-
3º	Compromisso de Conta	95	13	3º	Utilização ind./não aut. de recursos	1822	12	+
4º	Exp. de vuln. (intrusão)	58	8	4º	Outra	1813	12	N/A
5º	Distribuição (*malware*)	55	7	5º	*Scan*	1062	7	+
6º	Tentativa de *login*	30	4	6º	SPAM	985	6	+
7º	*Scan*	28	4	7º	Tentativa de *login*	953	6	-
8º	DoS/DDoS	27	4	8º	Utilização ilegítima de nome de terceiros	873	6	+
9º	Utilização ilegítima de nome de terceiros	19	3	9º	Indeterminado (*malware*)	842	6	+
10º	Exp. de vuln. (tentativa de intrusão)	18	2	10º	Acesso não autorizado	546	4	+

* Para uma leitura completa dos tipos de incidentes registados pela RNCSIRT, consultar Anexo.

Tabela 17 | CERT.PT e RNCSIRT

Incidentes registados pela RNCSIRT, 2019 - *ranking* top 10.
Nº de incidentes por mês.

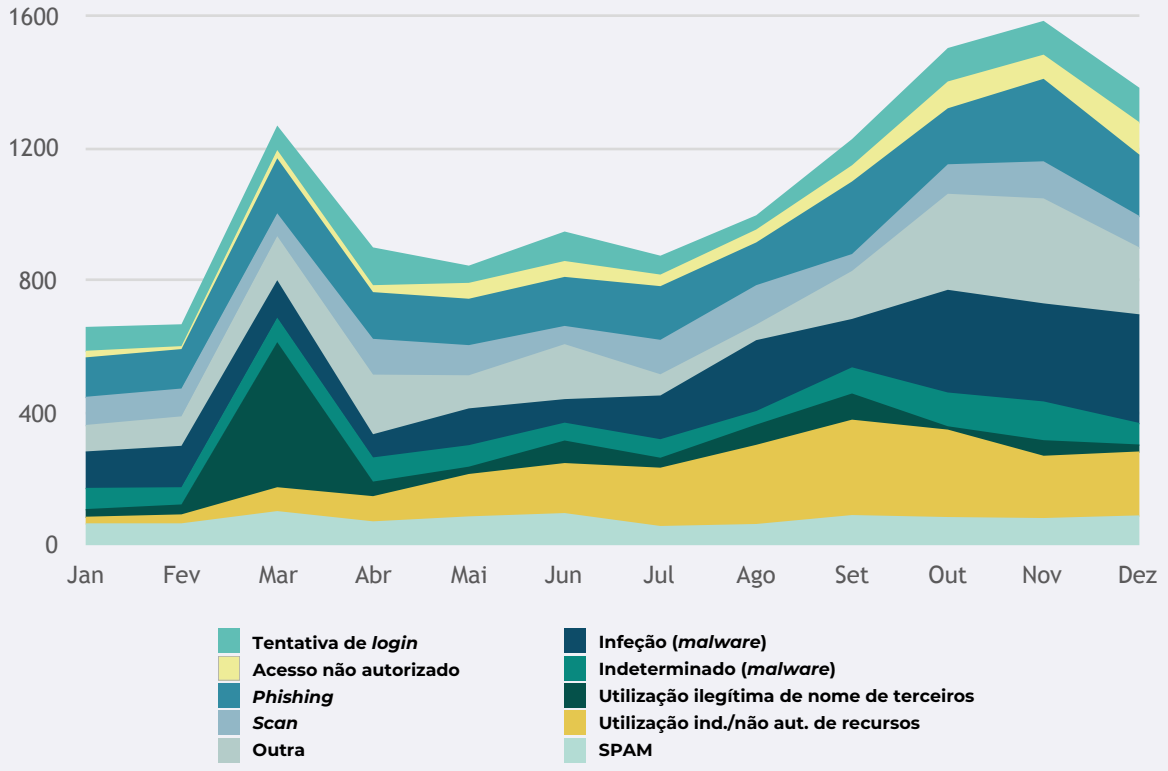


Figura 15 | RNCSIRT

Incidentes registados pela RNCSIRT, 2019 - Todos.
Percentagem de cada mês no total.

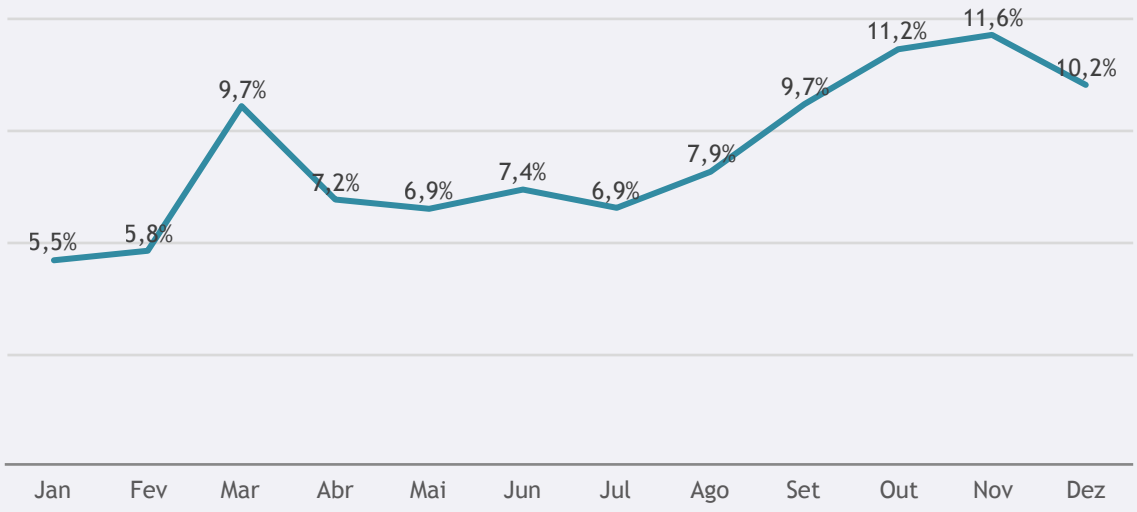


Figura 16 | RNCSIRT

Incidentes registados pela RNCSIRT por trimestre e semestre, 2019

Trimestre	1º tri.	2º tri.	3º tri.	4º tri.
Nº por trimestre	3194	3273	3741	5031
Nº por semestre	6467		8772	

Tabela 18 | RNCSIRT

DESTAQUES

Os tipos de incidentes mais frequentemente registados pela RNCSIRT, em Portugal, são a infeção por *malware* (13%) e o *phishing* (13%), à semelhança do CERT.PT, cujos dados estão incluídos nos dados da RNCSIRT.

Em termos de diferenças entre o CERT.PT e a RNCSIRT, destacam-se a maior importância relativa do *phishing* e do compromisso de conta entre os incidentes registados pelo CERT.PT e uma relevância maior da utilização indevida ou não autorizada de recursos entre os incidentes registados no âmbito da RNCSIRT – esta diferença também está relacionada com a natureza diversa das funções do CERT.PT e da RNCSIRT.

Ao longo do ano de 2019, os meses de outubro e novembro foram os que registaram mais incidentes no âmbito da RNCSIRT, reforçando a importância do segundo semestre, tal como no CERT.PT. Contudo, a RNCSIRT regista mais incidentes no quarto do que no terceiro trimestre.

16. Notificações à CNPD de violações (de segurança) de dados pessoais, 2018 e 2019

	Nº
***2018** (desde maio)*	160
2019	240

Tabela 19 | CNPD

DESTAQUES

Entre 2018 e 2019, ponderando os meses em falta de 2019, não existem grandes oscilações entre os dois anos no número de notificações à CNPD por violações de segurança de dados pessoais. Serão necessárias séries temporais mais longas para possibilitar uma leitura mais pertinente.

Síntese do Subcapítulo Ciberespaço de Interesse Nacional

O *phishing* e a infeção por *malware* são os tipos de incidentes mais registados pelo CERT.PT em 2018 e 2019. Em 2019, estes dois tipos de incidentes também são os mais registados pela RNCSIRT.

O mês de setembro, o terceiro trimestre e o segundo semestre foram os períodos nos quais o CERT.PT registou mais incidentes durante 2019 (ao contrário de 2018, em que o mês de outubro, o segundo trimestre e o primeiro semestre foram os que mais registos apresentaram). Também foi no terceiro trimestre e no segundo semestre de 2019 que se registaram mais vulnerabilidades e observáveis, no CERT.PT. Neste mesmo ano, a RNCSIRT também apresentou mais registos de incidentes no segundo semestre, embora com maior incidência no quarto trimestre do que no terceiro.

As Infraestruturas Digitais, os Prestadores de Serviços de Internet, a Educação, Ciência, Tecnologia e Ensino Superior, bem como a Banca são os setores e áreas governativas mais afetados por incidentes e com mais observáveis, entre os registados pelo CERT.PT, durante 2019 (com exceção da Banca em relação aos observáveis).

Entre 2018 e 2019 houve um aumento de 26% no número de incidentes e de 139% no número de vulnerabilidades registados pelo CERT.PT.

O tipo de observável mais registado pelo CERT.PT durante 2019 foi o serviço vulnerável, com grande destaque, seguido de *blacklist* e de *botnet drone*.

Enquanto observável, o *phishing* tem menos importância relativa se compararmos com os incidentes registados, no CERT.PT.

CIBERCRIME

A criminalidade que ocorre na esfera digital é uma realidade emergente que acompanha a crescente digitalização da sociedade. Este desenvolvimento torna mais problemática a distinção entre o crime que é específico do ciberespaço e aquele que o não é. A "transformação digital" é tão hegemónica que cada vez mais qualquer tipo de crime tem uma expressão digital. Não obstante, é possível seguir uma distinção que pelo menos sinaliza dois graus de integração de uma dada criminalidade na esfera digital: **1)** existem crimes ciberdependentes, os quais resultam das características específicas da informática – o *ransomware* é um vetor deste tipo de cibercrime (Europol 2019b); e **2)** os outros cibercrimes, aqueles que ocorrem no ciberespaço, mas apenas fazendo da informática um meio para a sua concretização – por exemplo, a burla por meio informático.

O cibercrime em Portugal é legislado através da Lei do Cibercrime[6], mas encontra-se noutro tipo de legislação a tipificação de crimes que utilizam meios informáticos para a sua concretização, como é o caso da devassa por meio informático (artigo 193° do Código Penal) ou a burla informática e nas comunicações (artigo 227° do Código Penal), ambos crimes que são considerados na análise a efetuar.

Os dados apresentados quanto a crimes efetivos registados pelas autoridades, desde 2009, são fornecidos pela DGPJ e a tipologia disponibilizada é a proposta por esta entidade. Estes dados têm duas limitações: apenas são registados os crimes mais graves, ficando por enumerar outros que também foram praticados nos mesmos casos; e não representam todo o espectro de crimes que ocorrem no ciberespaço, tais como aqueles que acompanham a violência doméstica ou a exploração sexual de menores. A informação fornecida pela APAV, com base nos processos abertos através da Linha Internet Segura[7], já contempla este tipo de crimes, mas tem as limitações próprias de um registo realizado com base nas chamadas telefónicas e contactos *online*. Neste subcapítulo, também são consideradas as queixas registadas pelo Gabinete de Cibercrime do Ministério Público.

De seguida apresentam-se os dados fornecidos pela DGPJ. A tipologia selecionada indica os crimes registados pelas autoridades policiais, o número de condenados e os arguidos.

6 Lei 109/2009: https://dre.pt/pesquisa/-/search/489693/details/maximized

7 Esta linha é um dos serviços disponibilizados no âmbito do projeto Centro Internet Segura - https://www.internetsegura.pt/lis/sobre-a-lis

Distingue-se entre crimes informáticos, do âmbito da Lei do Cibercrime, e alguns entre os que têm uma relação com a informática (que incluem os informáticos), nomeadamente, tal como referido, a devassa por meio informático e a burla informática e nas comunicações.

17. Crimes registados pelas autoridades policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, 2017 e 2018 – top 5*

2017				2018				Ordenação	
RK	Crime	Nº	%	RK	Crime	Nº	%	Tendência absoluta	Lugar RK
1º	Burla informática/ comunicações (contra património)	8149	85	1º	Burla informática/ comunicações (contra património)	9783	88	+	=
2º	Devassa p/meio informático (contra pessoa)	499	5	2º	Devassa p/meio informático (contra pessoa)	456	4	-	=
3º	Acesso/interceção ilegítimos	470	5	3º	Acesso/interceção ilegítimos	395	4	-	=
4º	Sabotagem informática	249	3	4º	Sabotagem informática	226	2	-	=
5º	Falsidade informática	196	2	5º	Falsidade informática	220	1	+	=

* Para uma leitura completa dos crimes, consultar Anexo.

Tabela 20 | DGPJ

Crimes registados pelas autoridades policiais, por crimes informáticos, entre 2009 e 2018 - Total. Evolução por crime.

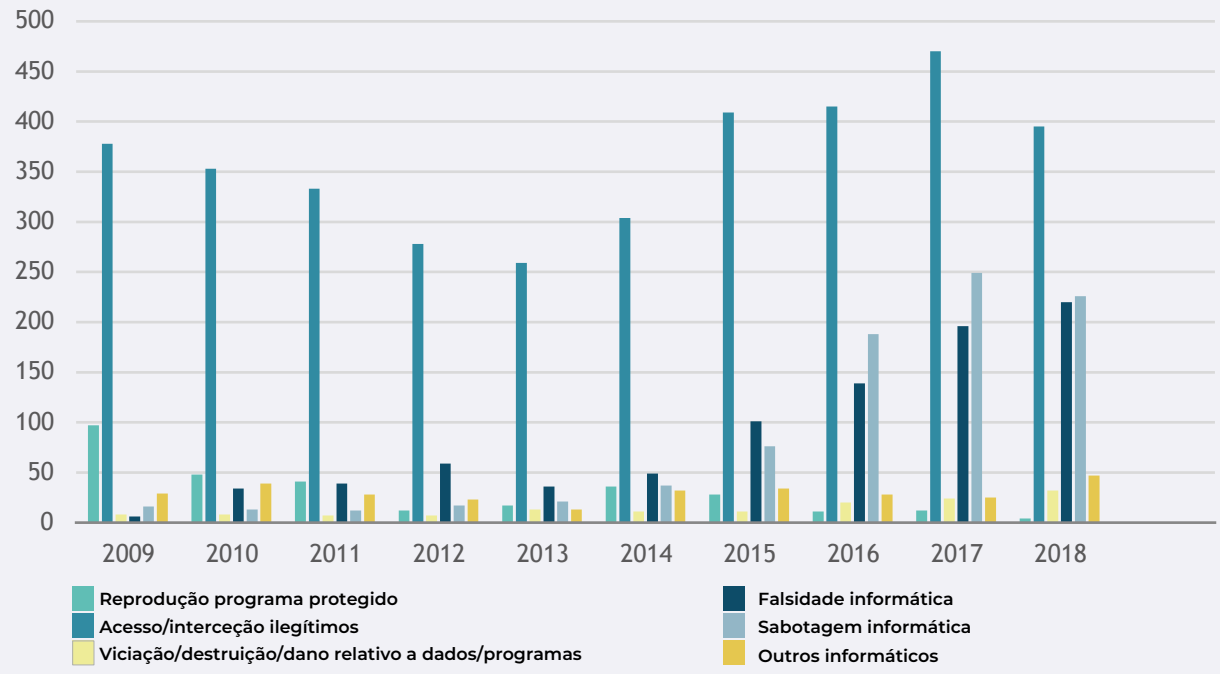


Figura 17 | DGPJ

Crimes registados pelas autoridades policiais, por crimes de devassa por meio informático e burla informática/comunicações, entre 2009 e 2018 - Total. Evolução por crime.

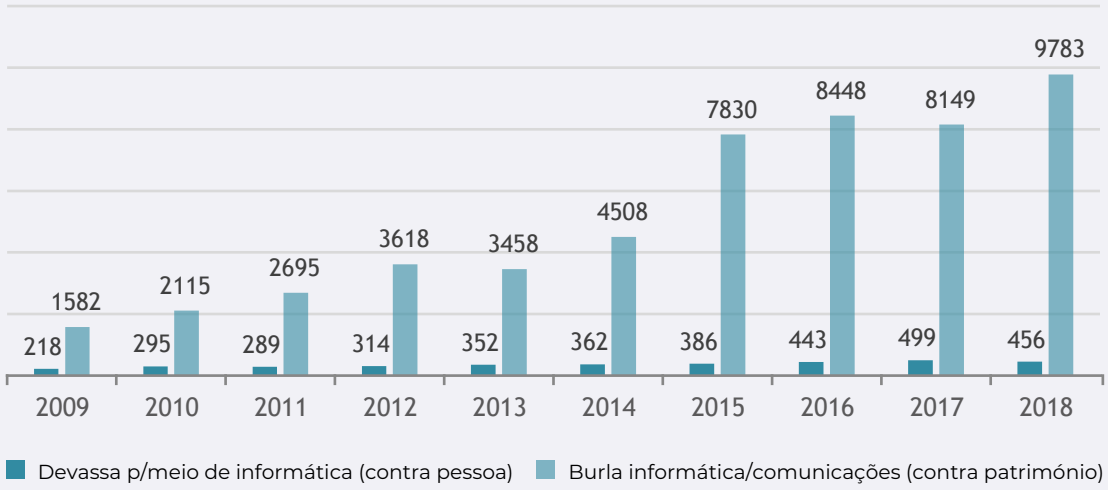


Figura 18 | DGPJ

Crimes registados pelas autoridades policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, entre 2009 a 2018. Total relacionados a informática/ informáticos (incluídos no total)

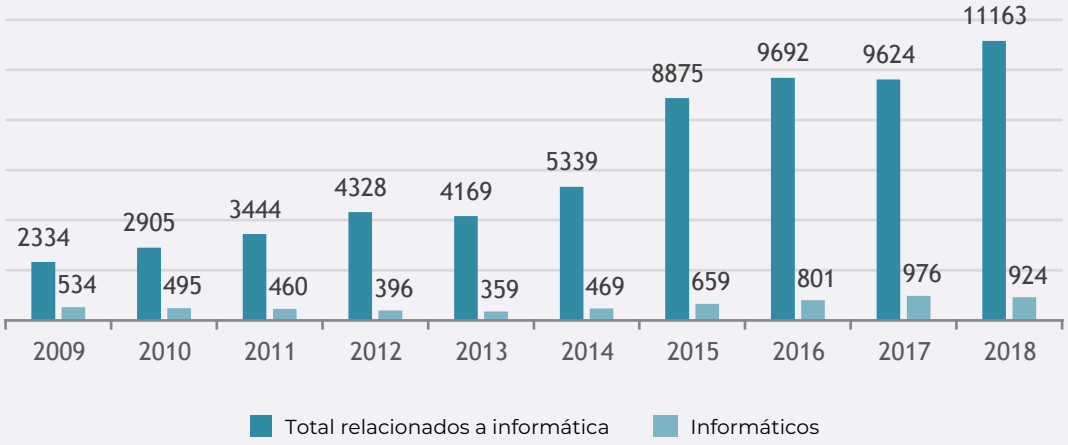


Figura 19 | DGPJ

Crimes registados pelas autoridades policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, entre 2009 a 2018, tendência (%)

	2010	2011	2012	2013	2014	2015	2016	2017	2018
T/Total	+24	+19	+25	-4	+28	+66	+9	-1	+16
T/Informáticos	-1	-7	-14	-9	+31	+41	+22	+22	-5

Tabela 21 | DGPJ

Crimes registados pelas autoridades policiais, por crimes informáticos,
devassa por meio informático e burla informática/comunicações, entre 2009 e 2018.
Evolução de total todos os crimes/total relacionados a informática.

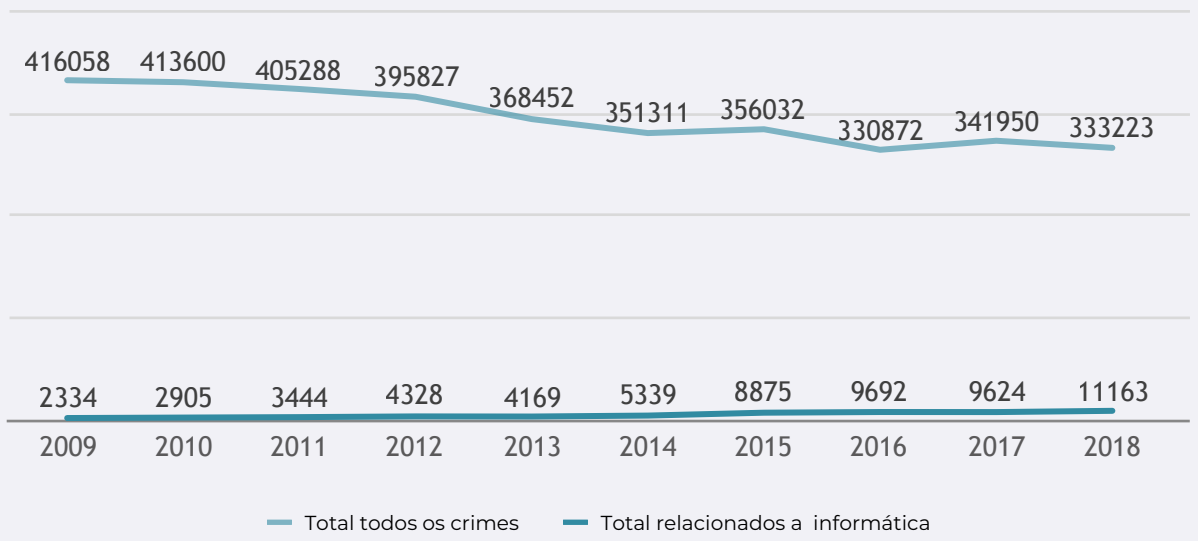


Figura 20 | DGPJ

Crimes registados pelas autoridades policiais, por crimes informáticos,
de devassa por meio informático e de burla informática/comunicações, entre 2009 e 2018.
Percentagem de evolução de total de crimes/total relacionados a informática.

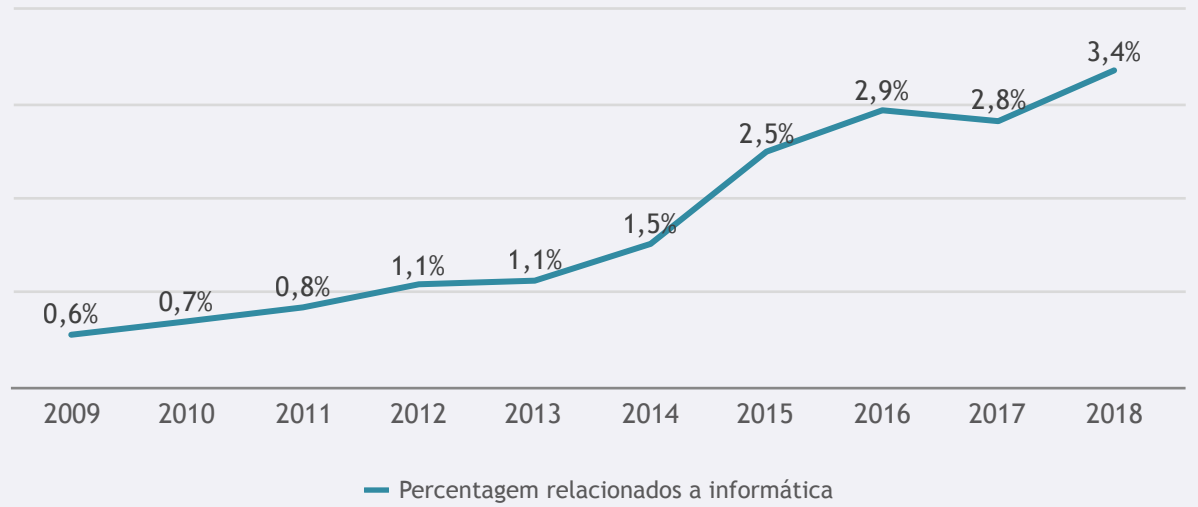


Figura 21 | DGPJ

Destaques

Entre 2017 e 2018, a burla informática/comunicações é o crime mais registado entre os relacionados a informática, representando 88% dos casos em 2018, tendo aumentado em relação ao ano anterior, de 8149 para 9783 registos. O acesso/interceção ilegítimos e a sabotagem informática são os crimes informáticos mais frequentes nesses dois anos, correspondendo, em 2018, a 4% dos casos cada, embora de 2017 para 2018 se assista a um ligeiro decréscimo nos números de ambos os tipos de crime. A predominância da burla informática/comunicações e do acesso/interceção ilegítimos mantém-se desde 2009.

Desde 2009 verifica-se um aumento constante no número total de crimes relacionados a informática (que inclui informáticos), com exceção do ano 2013 e do ano 2017, nos quais ocorreram ligeiros decréscimos. Quanto aos crimes informáticos, entre 2009 e 2013 ocorreu um decréscimo persistente de ano para ano. Contudo, entre 2013 e 2017, verificaram-se todos os anos aumentos entre os 20% e os 40%, aproximadamente. Em 2018, estes crimes diminuíram 5%.

2015 foi um ano em que o total de crimes relacionados a informática e os crimes estritamente informáticos aumentaram muito, 66% e 41%, respetivamente.

Apesar de haver um decréscimo de crimes informáticos em 2018 (-5%), há um aumento do total relacionados a informática (+16%).

A percentagem de crimes relacionados a informática, entre todos os crimes registados pelas autoridades, aumentaram todos os anos entre 2009 e 2018.

18. Condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, devassa por meio informático e burla informática/comunicações, 2017 e 2018 – top 5*/**

2017				2018				Ordenação	
RK	Crime	Nº	%	RK	Setor	Nº	%	Tendência absoluta	Lugar RK
1º	Burla informática/ comunicações (contra património)	179	85	1º	Burla informática/ comunicações (contra património)	123	74	-	=
2º	Falsidade Informática	19	9	2º	Falsidade Informática	23	14	+	=
3º	Acesso ilegítimo	5	2	3º	Reprodução ileg. prog. protegido	6	4	+	+
4º	Reprodução ileg. prog. protegido	3	1	4º	Dano rel. dados/ programas	5	3	+	+
5º	...	...	...	5º	Acesso ilegítimo	4	2	-	-

* Para uma leitura completa dos condenados, consultar Anexo.
** As percentagens correspondem aos totais e não a todos os crimes identificados, visto em alguns casos a informação de que se dispõe ser apenas total e não do tipo de crime, devido a segredo estatístico.

Tabela 22 | DGPJ

Aspetos sociodemográficos relevantes Portugal 2018

Género	Verifica-se a existência de um maior número de homens (65%) do que de mulheres (35%) a serem condenados por este tipo de crime.
Idade	Grande parte dos condenados encontram-se nas faixas etárias entre os 21 e os 29 anos (27%), entre os 30 e os 39 anos (31%) e entre os 40 e os 49 anos (24%).

Condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática/comunicações, entre 2009 e 2018. Total rel. informática/ Informáticos (incluídos no total)

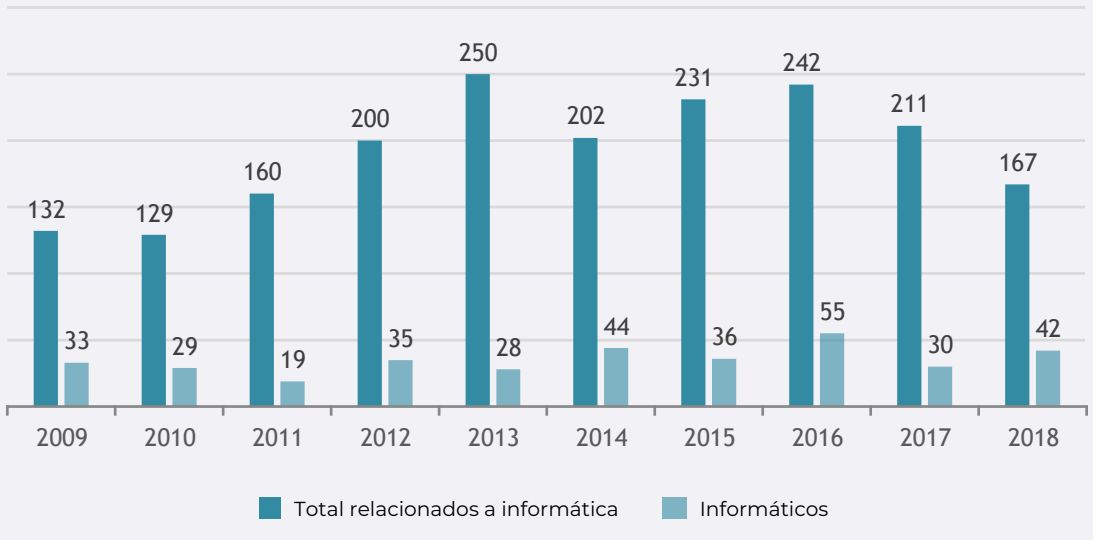


Figura 22 | DGPJ

Destaques

Entre os crimes relacionados a informática, a burla informática/comunicações é o que apresenta mais condenados (74% em 2018), embora entre 2017 e 2018 o nº de condenados por este crime tenha decrescido de 179 para 123.

O crime informático que apresenta um maior número de condenados é o de falsidade informática, tendo aumentado de 19 para 23 condenados, entre 2017 e 2018.

Desde 2009 que se assiste a algumas oscilações no número de condenados, sendo que entre 2016 e 2018 ocorreu uma descida constante nesses úmeros, exceto no que diz respeito aos condenados por crimes informáticos, que entre 2017 e 2018 aumentaram de 30 para 42.

Em termos de perfil, em 2018, os condenados são maioritariamente homens (65%) e quase um terço (31%) têm idades compreendidas entre os 30 e os 39 anos. .

19. Arguidos vs condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática/comunicações, entre 2009 e 2018, tendência

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Arguidos	284	269	331	422	530	444	469	502	484	401
Tendência %	N/A	-5	+23	+27	+26	-16	+6	+7	-6	-17
Condenados	132	129	160	200	250	202	231	242	211	167
Tendência %	N/A	-2	+24	+25	+25	-24	+14	+5	-13	-21

Tabela 23 | DGPJ

Arguidos vs condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática/comunicações, entre 2009 a 2018

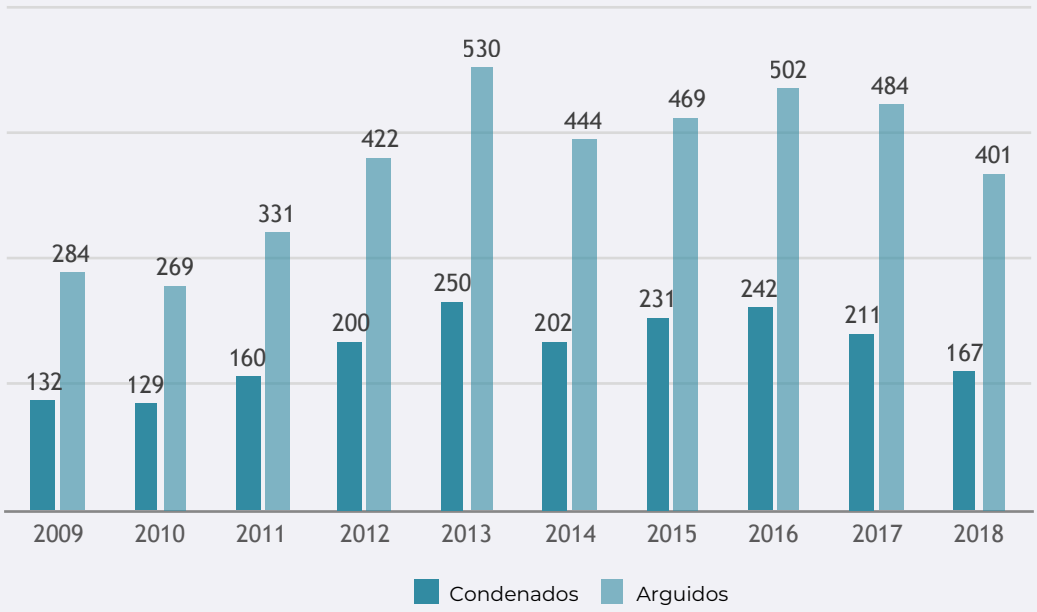


Figura 23 | DGPJ

Destaques

Os aumentos e os decréscimos nos números de condenados e arguidos por estes tipos de crimes foram relativamente paralelos desde 2009 até 2018.

Um indicador complementar sobre os níveis de cibercriminalidade é aquele que nos é fornecido pelo Gabinete de Cibercrime do Ministério Público, em documento publicado (MP, 2020) que menciona o número de denúncias recebidas por este organismo quanto a crimes cometidos *online*.

20. Denúncias recebidas pelo Gabinete de Cibecrime do MP, entre 2016 e 2019

	Denúncias	Variação anual	Encaminhadas p/ inquérito	Variação anual
2016 (fevereiro)	108	N/A	20	N/A
2017	155	+44%	59 (20)*	+195%
2018	160	+3%	50 (13)*	-15%
2019	193	+21%	67	+34%

* O número entre parêntesis corresponde a encaminhamentos para inquéritos já existentes.

Tabela 24 | MP2020

Denúncias recebidas pelo gabinete de cibecrime do MP entre 2016 e 2019

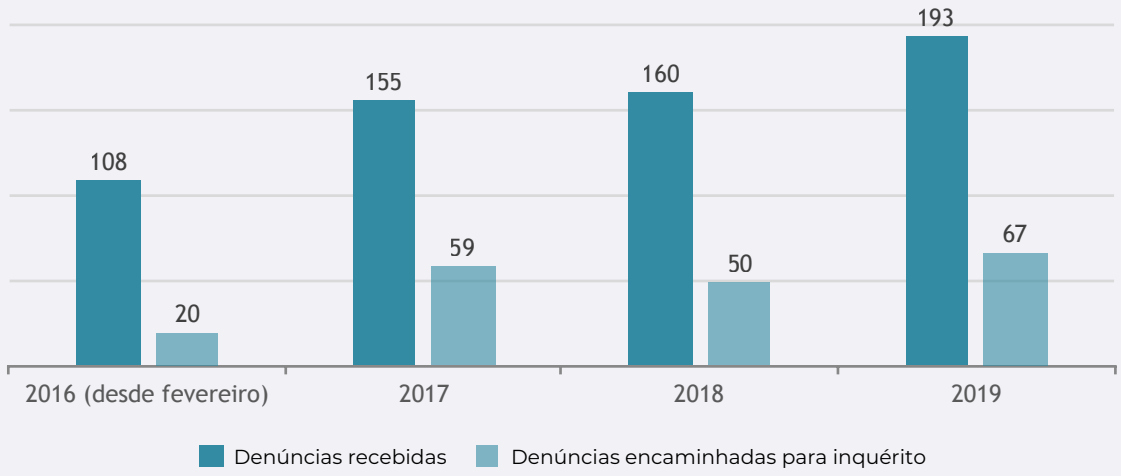


Figura 24 | MP2020

DESTAQUES

Verifica-se um aumento constante, desde 2016, no número de denúncias ao Gabinete de Cibercrime do Ministério Público – entre 2018 e 2019, este aumento foi de 21%.

Ainda entre 2018 e 2019, em conformidade com o aumento de denúncias, também se identifica um acréscimo de 34% no número de denúncias encaminhadas para inquérito.

Para complementar estes dados, é oportuno recorrer aos números da APAV respeitantes às atividades da Linha Internet Segura em 2019, na medida em que permitem completar a informação sobre cibercrime com a caracterização das vítimas e de alguns casos da esfera criminal não abrangidos na análise precedente. Esta linha presta apoio de duas formas: aceitando denúncias de conteúdos ilegais na *internet* (Hotline) e respondendo a questões do âmbito do uso das tecnologias ou apoiando vítimas de cibercrime (Helpline).

21. Processos de atendimento e apoio na Linha Internet Segura, APAV, 2019*

Meses	Jan.	Fev.	Mar.	Abr.	Mai.	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	Total
Processos	61	62	58	62	74	68	60	64	98	94	71	55	
	181			204			222			220			827
	385						442						

* Nas suas duas vertentes: atendimento e denúncia.

Tabela 25 | APAV

Processos de atendimento e apoio na Linha Internet Segura, APAV, 2019.
Percentagem de cada mês no total

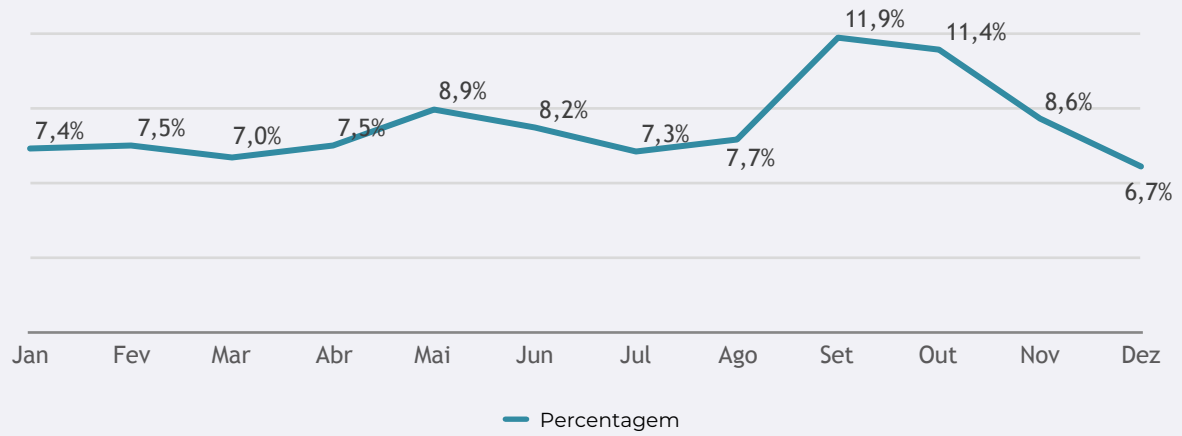


Figura 25 | APAV

DESTAQUES

Em setembro, assistiu-se a um aumento de processos de atendimento e apoio na Linha Internet Segura, da APAV, de 64 em agosto (7,7%) para 98 em setembro (11,9%).

Entre outubro e novembro, ocorreu uma descida de 94 (11,4%) para 71 (8,6%), respetivamente.

O terceiro trimestre e o segundo semestre são os períodos que têm mais processos. Esta conclusão coincide com os dados de 2019 sobre os incidentes e os observáveis registados pelo CERT.PT e os incidentes registados pela RNCSIRT (quanto à RNCSIRT, dá-se a exceção de esta registar mais incidentes no quarto trimestre).

22. Crimes e outras formas de violência registados pela Helpline, APAV, 2019

Crimes e outras formas de violência	Nº	Crimes e outras formas de violência	Nº
Burla	20	Ameaça	2
Furto de Identidade	12	Crimes sexuais	2
Phishing	9	Dano informático	2
Devassa da vida privada	8	Denúncia redes sociais	2
Sextortion	8	Gravação de fotografias ilícitas	2
Acesso ilegítimo	7	Dependência de videojogos	1
Difamação/injúrias	7	Divulgação de imagens e vídeos	1
Violência doméstica	5	*Grooming*	1
Cyberbullying	4	Importunação sexual	1
Pornografia de menores	4	Tentativa de homicídio	1
Sexting	3	TOTAL	102

Tabela 26 | APAV

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

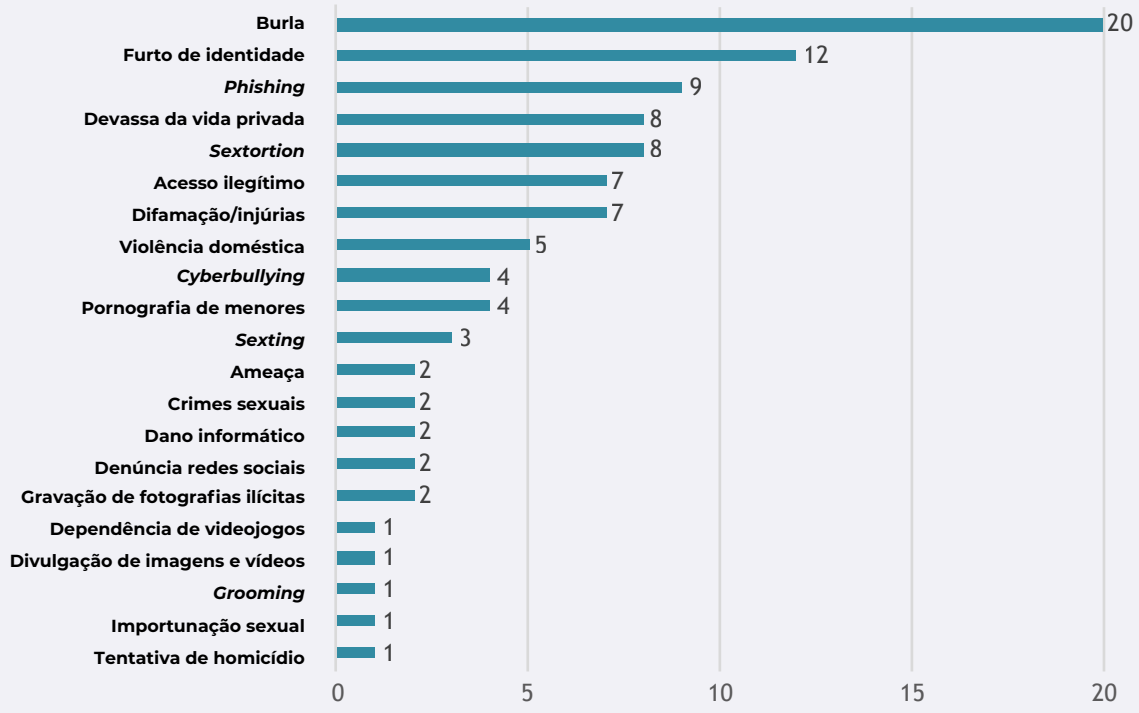


Figura 26 | APAV

DESTAQUES

Os crimes e outras formas de violência mais frequentemente registados pela Helpline da Linha Internet Segura, da APAV, são a burla (20), o furto de identidade (12) e o *phishing* (9).

23. Informações prestadas pela Helpline, APAV, 2019

	Nº	%
Segurança informática	20	83
Outras informações	4	17
TOTAL	24	100

Tabela 27 | APAV

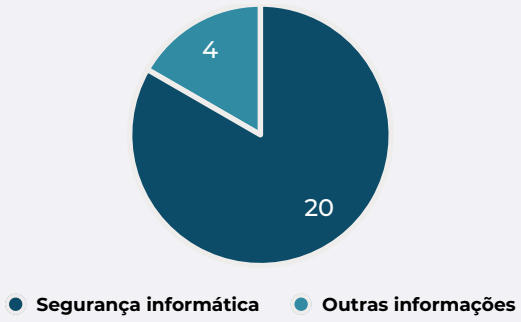


Figura 27 | APAV

DESTAQUES

A maioria das informações prestadas pela Helpline da Linha Internet Segura, da APAV, foram do âmbito da segurança informática, com 83% dos casos.

24. Denúncias de crimes registadas pela Hotline, APAV, 2019

	Nº	%
Pornografia infantil	676	96
Discriminação racial	24	3
Instigação pública a um crime	1	0,1
TOTAL	701	100

Tabela 28 | APAV

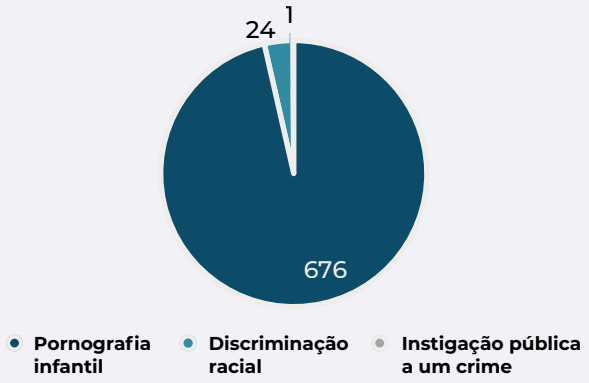


Figura 28 | APAV

DESTAQUES

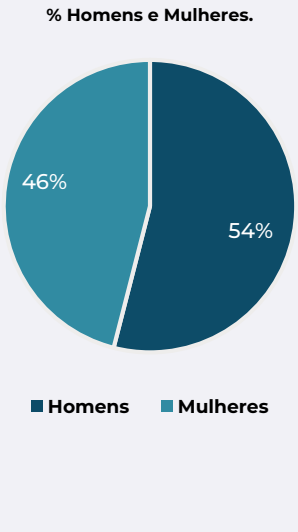
A grande maioria das denúncias de crimes registadas pela Hotline da Linha Internet Segura, da APAV, são de pornografia infantil, com 96% dos casos.

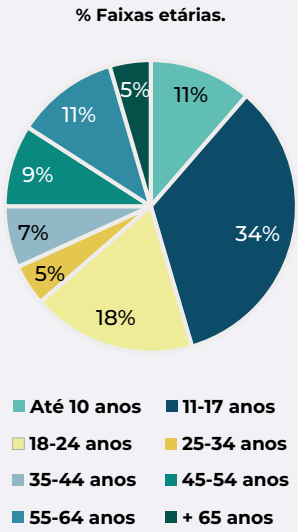
25. Perfil da vítima - informação recolhida na Helpline, APAV, 2019

	Nº	%
Homens	68	54%
Mulheres	58	46%
*Até 10 anos**	5	11%
11-17 anos	15	34%
18-24 anos	8	18%
25-34 anos	2	5%
35-44 anos	3	7%
45-54 anos	4	9%
55-64 anos	5	11%
+ 65 anos	2	5%

* 82 não respostas em relação a idade.
Percentagem calculada em relação aos restantes 44.

Tabela 29 | APAV





Figuras 29 e 30 | APAV

DESTAQUES

O perfil da vítima em contacto com a Helpline da Linha Internet Segura, da APAV, é relativamente equilibrado entre os dois géneros, mas com ligeira maioria para as pessoas do sexo masculino (54%). Quanto à faixa etária, são as pessoas com idades compreendidas entre os 11 e os 17 anos as que mais contactam esta linha (36%).

Síntese do Subcapítulo Cibercrime

A burla informática/comunicações é o crime mais registado entre os relacionados com informática entre 2009 e 2018 e o que apresenta mais condenados. No mesmo período, o acesso/interceção ilegítimos é o tipo de crime informático mais registado pelas autoridades. No entanto, não é aquele que resulta em mais condenados. Por exemplo, em 2018, houve 23 condenados por falsidade informática e apenas 4 por acesso ilegítimo.

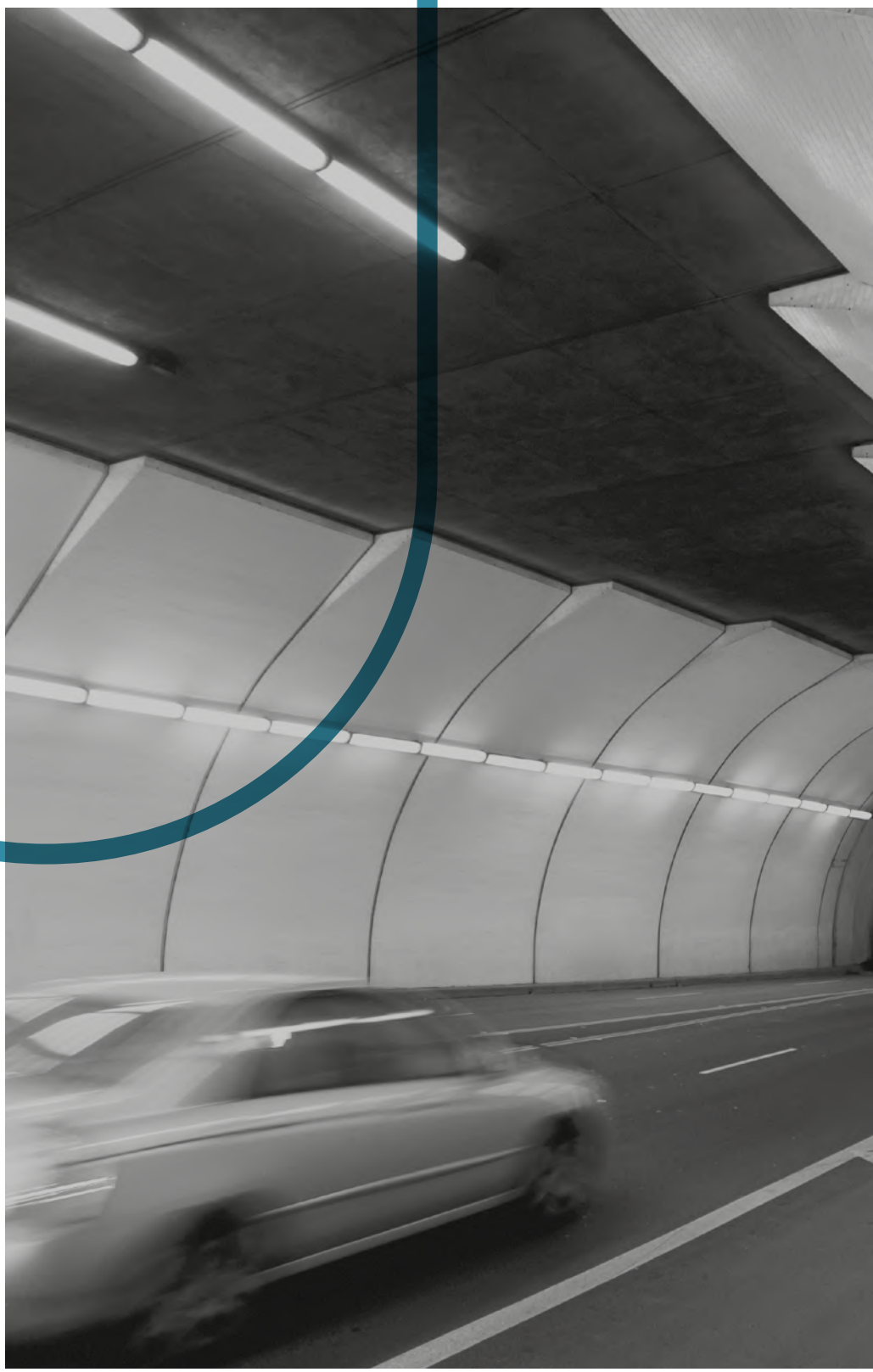
Genericamente, os crimes relacionados a informática aumentaram de forma consistente entre 2009 e 2018, sobretudo se considerarmos a sua percentagem no total de crimes registados pelas autoridades. Os crimes estritamente informáticos, incluídos naqueles, apresentaram algumas oscilações na sua evolução durante este período.

Verifica-se um aumento constante de denúncias ao Gabinete de Cibercrime do Ministério Público desde 2016 até 2019.

O mês de setembro, o terceiro trimestre e o segundo semestre são os períodos que registam mais processos de atendimento e apoio na Linha Internet Segura, da APAV. Estes resultados coincidem na generalidade com os dados do mesmo tipo apresentados relativamente aos incidentes registados pelo CERT.PT e pela RNCSIRT.

Os crimes mais frequentes registados pela Helpline da Linha Internet Segura, da APAV, são a burla, o furto de identidade e o *phishing*.

As pessoas que mais frequentemente entram em contacto com a Helpline da Linha Internet Segura, da APAV, são homens (diferença ligeira em relação a mulheres) e pessoas com idades compreendidas entre os 11 e os 17 anos (das que revelaram a idade).



CNCS
Centro Nacional de Cibersegurança PORTUGAL

AMEAÇAS E PROSPETIVAS

Observatório de Cibersegurança

Nas páginas anteriores, foi possível analisar dados sobre acontecimentos comprovados e categorizados enquanto incidentes e cibercrimes. Essa análise permitiu identificar processos materializados em efetivas ocorrências. Neste capítulo, o objetivo é, com base nos dados apresentados e em análises dos parceiros do CNCS, identificar as principais ameaças e prospetivas. Enquanto o primeiro capítulo incide sobre aquilo que já aconteceu, este foca-se sobretudo naquilo que pode acontecer. Em termos de formato, é menos quantitativo, mas apresenta um destaque no final de cada tópico e uma síntese no fim dos subcapítulos.

AMEAÇAS

Entende-se por ameaça uma "potencial causa de um incidente indesejado, que pode provocar danos a um sistema, indivíduo ou organização" (ISO/IEC 27032). Deste ponto de vista, uma ameaça é tudo aquilo que pode fomentar os acontecimentos descritos no primeiro capítulo: incidentes e cibercrimes. Estas ameaças podem **1)** ser responsabilidade de certos agentes e **2)** concretizarem-se através de táticas, técnicas e procedimentos (TTP) identificáveis - duas categorias em permanente correlação - os agentes são os promotores da ameaça e as TTP os meios utilizados para realizar um ataque. A ameaça é o processo que articula estas variáveis numa possível situação de agressão futura, considerando determinada vítima em potência.

Dos dados apresentados nos subcapítulos anteriores, é possível destacar um conjunto de TTP que se concretizaram em 2019 e que, por isso, têm maior probabilidade do que outras de continuarem a ser ameaças em 2020 e 2021. Do ponto de vista dos agentes, a atribuição de responsabilidade/culpa por determinado incidente/cibercrime é uma das maiores dificuldades no campo da cibersegurança. A este respeito, os dados mais certos de que dispomos são os relativos a condenados, mas esses incidem sobretudo sobre ameaças nacionais, excluindo um conjunto de agentes de ameaças muito alargado, e apresentam uma distância temporal em relação ao ato criminoso que não permite fazer leituras adequadas da atualidade. Portanto, no que se refere a agentes de ameaças, devemos remeter sobretudo para as conjeturas realizadas quanto à relação provável entre estes e determinados tipos de ataque. Estas correlações são feitas com base nas pesquisas efetuadas pela comunidade de informações nacional e euro-atlântica.

AGENTES DE AMEAÇAS

Uma das formas de tipificar os agentes de ameaças é através da identificação da sua relação com os Estados. Enquanto ator com muitos recursos e responsável pela soberania nacional, um Estado, ao relacionar-se com um tipo de ameaça, fornece a esta, em hipótese, os seus recursos e faz dessa ameaça parte da sua estratégia em termos das relações nacionais e internacionais. Esta conexão pode não ser completa, isto é, um grupo de cibercriminosos, por exemplo, pode não se integrar na estrutura de um Estado, mas ter o seu apoio. Nesse caso, estamos perante atores paraestatais.

Cabem no âmbito dos atores estatais entidades que atuam em nome de um órgão governamental, como, por exemplo, governos, representações oficiais, forças armadas ou serviços de informações. A quantidade e a qualidade dos recursos destes atores fazem com que se classifiquem muitos deles como "ameaças persistentes avançadas" (Advanced Persistent Threats – APT).

Numa esfera híbrida, os atores paraestatais são aqueles que são vinculados a Estados ou dirigidos por eles, mas que não pertencem formalmente a qualquer entidade governamental. Entre os agentes de ameaças incluídos neste tipo de ator estão os grupos de *hackers* que vendem os seus serviços (*hackers for hire*, isto é, cibercriminosos), podendo prestá-los, precisamente, a Estados, mas não só. Alguns destes grupos também podem tomar a forma de APT.

Os atores não estatais, por fim, distinguem-se por não serem unidades soberanas e incluírem organizações e indivíduos que não são afiliados, dirigidos ou financiados por um governo. São exemplos disso os cibercriminosos, os hacktivistas, alguns lobos solitários ou entidades do universo da cibersegurança, como empresas ou *freelancers*.

Considerando o tipo de agentes de ameaças proposto pela ENISA[8], podemos considerar a seguinte distribuição dos agentes quanto à sua relação com os Estados. A distribuição que se propõe deve ser lida à luz da noção de ideal-tipo, ou seja, por regra esta é a correlação que existe entre os agentes de ameaças e os Estados, mas existirão zonas cinzentas nas quais por vezes e em dadas circunstâncias esta configuração apresenta exceções.

8 Ver Termos e Abreviaturas para a definição de cada um dos agentes mencionados.

Quadro de Estados /Agentes de Ameaças

	Ciber criminosos	*Insiders*	Agentes Estatais	Empresas	Hacktivistas	Ciber terroristas	*Script kiddies*
Atores Estatais			■				
Atores Paraestatais	■	■	■			■	
Atores Não Estatais	■	■		■	■	■	■

Adaptado de *ENISA Threat Landscape Report 2018* (2019)

■ Correlação entre Estados e os Agentes de Ameaças.

Quadro 1 | adaptado de ENISA

À luz deste quadro, é possível destacar três agentes de ameaças que sobressaem em relação a outros no contexto português, seguindo a taxonomia proposta pela ENISA: os cibercriminosos, os agentes estatais e os hacktivistas. Como referido anteriormente, o destaque atribuído a estes agentes de ameaças ocorre com base nas pesquisas empreendidas pela comunidade de informações em relação a Portugal. Não obstante, qualquer um dos restantes agentes de ameaças é um potencial agressor e possível responsável por alguns dos incidentes e cibercrimes registados.

A atividade dos cibercriminosos, entidades que regem as suas ações com base em motivos sobretudo económicos, tem sido muito relevante em território nacional. Estes grupos ou indivíduos têm agido com os objetivos principais de extorquir, realizar fraudes e obter credenciais. Por vezes, misturam-se com atores estatais, que os patrocinam, ou agem de forma solitária.

Alguns agentes estatais também continuam a ser uma ameaça importante, através do patrocínio e contratação de grupos de cibercriminosos ou mediante o uso dos seus próprios serviços de informações. Neste contexto, as práticas de ciberespionagem são um meio importante, usualmente com o objetivo de exfiltrar informação (isto é, extrair dados de teor político, estratégico, militar, económico e operacional), apontando indivíduos e organizações como alvos, procurando recrutar colaboração ou sabotar e comprometer sistemas.

O terceiro tipo de agente de ameaças relevante para Portugal, os hacktivistas, tem como objetivo promover a desestabilização sistémica através de sabotagens, danos reputacionais em organizações e indivíduos, exibindo a capacidade de realizar um determinado ataque sem na realidade o concretizar na sua totalidade (*proof of concept*) ou promovendo a divulgação de *bugs* ou vulnerabilidades em sistemas, para se autopromover ou como veículo da sua mensagem ativista.

Em geral, o objetivo destas ações é protestar contra decisões ou fazer afirmações com cunho político-ideológico.

Vejamos no quadro que se segue o peso de uma possível correlação com Estados que cada um destes agentes adquire, indicador importante, como referido, para a compreensão do seu nível de recursos.

Quadro de Estados/Agentes de Ameaças – ameaças mais relevantes para Portugal

	Ciber criminosos	Insiders	Agentes Estatais	Empresas	Hacktivistas	Ciber terroristas	*Script kiddies*
Atores Estatais			■				
Atores Paraestatais	■	■	■			■	
Atores Não Estatais	■	■		■	■	■	■

Adaptado de *ENISA Threat Landscape Report 2018* (2019)

■ Correlação entre Estados e os Agentes de Ameaças.

■ Correlação entre Estados e Agentes de Ameaças mais relevantes para Portugal na atualidade.

Quadro 2 | adaptado de ENISA

Do ponto de vista da relação com os Estados e da quantidade e qualidade de recursos que cada um destes agentes de ameaças possui, logo, do nível de potencial impacto da ameaça, para lá da conclusão óbvia de que os agentes estatais são os que têm, potencialmente, mais recursos, verifica-se que os cibercriminosos, na medida em que por vezes são patrocinados por Estados, têm por regra acesso a mais recursos do tipo estatal do que os hacktivistas. Contudo, estes, comparando com alguns cibercriminosos não estatais, podem, em certos casos, obter mais recursos por via de uma maior capacidade de mobilização ideológica. Tendo objetivos mais correlacionados à provocação de danos reputacionais e à autopromoção do que à obtenção de ganhos económicos, conseguem com maior facilidade atingir os seus objetivos, que em geral requerem menos recursos.

As principais vítimas destes três tipos de agentes de ameaças são os organismos do Estado; algumas empresas-chave com dados sensíveis; e os sistemas de controlo industrial, devido ao seu caráter crítico. Muitas destas organizações são operadores de serviços essenciais ou infraestruturas críticas. Não obstante, os indivíduos e as PME continuam a ser alvos relevantes, como é possível verificar nos dados apresentados na primeira parte deste documento. Considerando esses dados e, portanto, ameaças concretizadas, as principais vítimas que se reconheceram como tal através de inquéritos foram as grandes empresas e as

empresas de telecomunicações. Este dado é coerente com os indicadores produzidos pelo CERT.PT, nos quais se identifica um pendor forte das Infraestruturas Digitais e dos Prestadores de Serviços de Internet enquanto alvos frequentes. Como referido, pela sua natureza de prestação de um serviço, estes incidentes têm muitas vezes por alvo os clientes destas entidades, no que se incluem as empresas e os indivíduos, também eles vítimas quando se identificam ações maliciosas nestes setores. Com base nos dados do primeiro capítulo, é possível ainda realçar a área de governação da Educação, Ciência, Tecnologia e Ensino Superior e o setor da Banca como alvos recorrentes em 2019.

Destaques

Três tipos de agentes de ameaças destacam-se no ciberespaço de interesse nacional português: cibercriminosos, agentes estatais e hacktivistas.

Os hacktivistas são aqueles que apresentam, potencialmente, uma ligação mais fraca a Estados, embora tenham capacidade de mobilização ideológica.

Os principais alvos destes agentes de ameaças são organismos do Estado, algumas empresas-chave e sistemas de controlo industrial. Muitas destas organizações são operadores de serviços essenciais ou infraestruturas críticas. As entidades ligadas aos serviços digitais e de *internet*, a Educação, Ciência, Tecnologia e Ensino Superior, bem como a Banca, são alvos importantes.

TÁTICAS, TÉCNICAS E PROCEDIMENTOS (TTP)

Os agentes de ameaças utilizam diversas TTP para atingirem os seus fins. Associados aos agentes, estes meios são a componente mais visível de uma ameaça, pois são aqueles que se constituem como instrumentos usados para atingir diretamente as vítimas.

Um dos aspetos mais importantes das TTP dominantes entre os agentes de ameaças referidos é a engenharia social, a qual explora as fragilidades do fator humano. O *phishing* é um dos vetores relevantes a este respeito (mas também o *spearphishing* - *phishing* direcionado e adaptado a um alvo específico), através de *emails* ou SMS (*smishing*), promovendo a infeção por *malware* mediante cliques em *links* e anexos ou a recolha de credenciais. É relevante considerar alguns casos de CEO *fraud* através de telefonemas direcionados a altos dirigentes, com potencial recurso a *deep fakes* de voz. Neste contexto, o compromisso de conta é outro dos objetivos comuns da engenharia social. Não obstante, também se concretiza com recurso a bases de dados de palavras-passe disponíveis *online* e/ou utilizando mecanismos de força-bruta. A exploração de vulnerabilidades nos sistemas é levada a cabo em vários casos, quer como intrusão, quer como tentativa de intrusão. O *ransomware*, no âmbito da infeção por *malware*, tem tido algum impacto mediático e capacidade de desestabilização em certas organizações. Em geral, a devolução ou não dos dados cifrados é o fator-chave no pedido de resgate, mas a possibilidade de os divulgar a terceiros também é um elemento que fortalece a chantagem.

Verifica-se ainda um crescimento na utilização de técnicas de *false flag* – grupos estatais que mimetizam outros grupos e vice-versa, promovendo a falsa atribuição. Por vezes, estes agentes de ameaças roubam infraestruturas de outros coletivos de modo a simular ainda melhor a sua atuação. Existem também APT estatais que recorrem a *outsourcing*, o que pode ter um efeito semelhante, visto os ataques passarem a ser realizados pelas entidades contratadas, trazendo consigo as técnicas pelas quais são reconhecidas. A este propósito, é possível identificar o crescimento da oferta de campanhas de *hacking* e de desinformação como serviços e produtos (cibercrime-como-serviço). Este tipo de ação dificulta a atribuição e facilita a anonimização.

Considerando os dados de 2019, esta leitura é coerente com as ameaças concretizadas em termos de incidentes, com grande relevância para o *phishing* e a infeção por *malware*. Houve também uma maior identificação de vulnerabilidades (embora em termos de observáveis estas apresentem uma certa estabilização) e de compromissos de conta. Acresce que o terceiro

trimestre e o segundo semestre são os períodos mais intensos no que diz respeito à concretização destas ameaças.

Observando de novo o quadro proposto pela ENISA, mas na articulação que estabelece entre os agentes e as ciberameaças, é possível, à luz da conjetura acerca dos principais agentes de ameaças em Portugal, identificar correlações.

Quadro de Ameaças: Ciberameaças/Agentes de ameaças[9]

	Ciber criminosos	*Insiders*	Agentes Estatais	Empresas	Hacktivistas	Ciber terroristas	*Script kiddies*
Malware	■	□	■	■	□	□	□
Web-based attacks[10]	■		■	■	■	■	□
Web application attacks	■		■	■	■	□	□
Denial of Service (DoS)	■		□	□	■	□	■
Botnets	■		■	■	□	■	□
Phishing	■	■	■	■	□		□
SPAM	□	■	□	□			
Ransomware	■	□	■	■			□
Ameaça interna	■		□	■		□	
Manipulação física	■	■	■	■	□	□	□
Exploit kits	■		■	■			
Data breaches	■	■	■	■	■	■	□
Roubo de identidade	■	■	■	■	■	□	□
Information leakage	■	□	■	■	□	□	□
Ciberespionagem		□	□	□			

Adaptado de *ENISA Threat Landscape Report 2018* (2019)

■ **Agentes de ameaças mais relevantes em Portugal durante 2019/2020.**
■ **Grupo primário para a ciberameaça, segundo ENISA (c/ adaptação).**
□ **Grupo secundário para a ciberameaça, segundo ENISA (c/ adaptação).**

■ **Ciberameaça de primeiro nível em Portugal durante 2019/2020.**
■ **Ciberameaça de segundo nível em Portugal durante 2019/2020.**
■ **Ciberameaça de terceiro nível em Portugal durante 2019/2020.**

Quadro 3 | adaptado de ENISA

9 A seleção das principais ciberameaças e agentes de ameaças fez-se com base na pesquisa anteriormente realizada, quer neste capítulo, quer no anterior. Para uma compreensão mais aprofundada do significado de cada uma destas ciberameaças, consultar Termos e Abreviaturas e o texto *ENISA Threat Landscape Report 2018*. Chamamos "ciberameaças de primeiro nível" àquelas que ocupam os lugares cimeiros nos rankings do CERT.PT e da RNCSIRT e são redundantes nessa importância em várias fontes; "ciberameaças de segundo nível", àquelas que ocupam lugares intermédios nesses *rankings* e/ou são referidas em análises qualitativas; e "ciberameaças de terceiro nível", a todas as outras. A componente analítica, nas "ciberameaças de segundo nível", para lá daquilo que os dados revelam, tem importância em particular se considerarmos ciberameaças como a ciberespionagem. A distinção entre grupos primários e secundários, utilizada pela ENISA, refere-se à utilização predominante (primários) ou complementar (secundários) dos meios envolvidos em cada uma das ciberameaças por parte dos agentes identificados.

10 As ciberameaças *Web-based attacks* e *Application-based attacks* referem-se, na taxonomia do CERT.PT, sobretudo a intrusão e tentativa de intrusão – ver Anexo, tabela A.

Tendo em conta os três tipos de agentes que constituem as principais ameaças em Portugal, considerando ainda as TTP mencionadas anteriormente, no que se incluem os tipos de incidentes e o *modus operandi* dominantes, é possível identificar as ciberameaças integráveis nas ações dos referidos agentes e verificar algumas correlações possíveis, prováveis ou improváveis. Estas ciberameaças podem ser operacionalizadas em simultâneo - por exemplo, um ciberataque pode utilizar, ao mesmo tempo, na sua cadeia de ataque o *phishing* e o *malware* para atingir os seus objetivos.

Os cibercriminosos são dos agentes que maior diversidade de ciberameaças utilizam, sendo apenas improvável o uso da ciberespionagem. Contudo, visto esta ser uma prática típica de agentes estatais, quando cibercriminosos são patrocinados por Estados, não podemos colocar de parte a hipótese de utilizarem esse meio. Sendo o *phishing* e o *malware* ciberameaças de primeiro nível, é provável que em parte sejam promovidas por cibercriminosos, com intenções económicas, correlação reforçada pelo facto do quadro de ameaças prever uma utilização primária destas ciberameaças por estes agentes. Todavia, é possível que recorram a qualquer uma das restantes ciberameaças.

Os agentes estatais, de modo ainda mais transversal, recorrem a todas as ciberameaças identificadas e, portanto, também às mais ameaçadoras no contexto português. Esta transversalidade expressa a quantidade e qualidade de recursos que possuem. Tendo em conta o quadro proposto pela ENISA, a ciberespionagem não é o meio mais frequentemente utilizado pelos agentes estatais. Não obstante, essa utilização existe e será mais comum em relação a determinados alvos, dependendo dos objetivos. Em rigor, devemos considerar que é possível os agentes estatais serem responsáveis por qualquer uma das ciberameaças. No que diz respeito às de primeiro nível (*malware* e *phishing*) e a algumas de segundo nível no país (*web-based attacks*, *web application attacks*, *botnets*, *ransomware* e *data breaches*), os agentes estatais utilizam-nas de modo primário, o que faz com que a correlação entre essas ciberameaças e alguns agentes estatais seja provável.

Quanto aos hacktivistas, comparando com os outros tipos de agentes mais relevantes em Portugal, verificamos que são os que, tradicionalmente, recorrem a uma menor variedade de ciberameaças para realizarem os seus objetivos, correspondendo também a uma menor quantidade e qualidade de recursos. Entre as ciberameaças de primeiro nível em Portugal, os hacktivistas não se apresentam como os agentes que mais recorrem às mesmas. Além disso, será improvável recorrerem, por exemplo, ao SPAM, ao r*ansomware* ou à ciberespionagem.

Contudo, algumas das ciberameaças de segundo nível têm uma utilização primária pelos hacktivistas, favorecendo a probabilidade de uma correlação: *web-based attacks*, *web application attacks*, DoS/DDoS e *data breaches*.

Destaques

No âmbito das ciberameaças mais frequentes identificadas no ciberespaço de interesse nacional, o *phishing* e o *malware* (inclui *ransomware*) surgem destacadas. Estas ciberameaças são frequentemente acompanhadas pela exploração do fator humano, através de engenharia social.

É importante considerar ainda como relevantes o compromisso de conta, a exploração de vulnerabilidades, os DoS/DDoS, as *botnets*, o *ransomware*, os *data breaches* e a ciberespionagem.

Os agentes de ameaças mais comuns recorrem a grande parte das ciberameaças destacadas no primeiro e segundo níveis de utilização, destacando-se uma coincidência entre as mais frequentes em Portugal (*phishing* e *malware*) e o *modus operandi* comum destes agentes, com exceção dos hacktivistas, que fazem deles uma utilização secundária.

Há uma crescente utilização de técnicas de *false flag* que dificultam a atribuição.

Verifica-se o aumento de práticas de cibercrime-como-serviço, com a venda de campanhas de *hacking* e de desinformação.

Síntese do Subcapítulo Ameaças

Os tipos de agentes que representam uma maior ameaça para Portugal são os cibercriminosos, os agentes estatais e os hacktivistas.

As ciberameaças a que estes agentes recorrem com mais frequência para atingirem os seus fins são o *phishing*, o *malware* (inclui *ransomware*), o compromisso de conta, a exploração de vulnerabilidades, o DoS/DDoS, as *botnets* e os *data breaches*, fazendo-se acompanhar frequentemente de ações de engenharia social e, cada vez mais, de técnicas de *false flag*, bem como, em alguns casos, ciberespionagem.

Muitas das ciberameaças estão disponíveis como serviços e produtos, no âmbito do cibercrime-como-serviço.

PROSPETIVAS

Neste subcapítulo apresentam-se algumas prospetivas que procuram identificar tendências e ajudar os agentes a gerir o futuro quanto ao risco de concretização de certas ameaças à cibersegurança. Estas análises realizam-se com base nos dados apresentados no primeiro capítulo e na identificação de algumas ameaças, dois aspetos avaliados à luz da previsibilidade aplicável à linha temporal que se avizinha. Reconhece-se, não obstante, a incerteza que estes exercícios sempre acarretam.

A este respeito, divide-se a análise em três tópicos: Tendências em Agentes e TTP, no qual se estima a continuidade ou não das ameaças já identificadas; Tendências Globais, em que se elencam algumas dinâmicas internacionais que podem interferir no nível nacional; e, por fim, em O Caso Covid-19, analisa-se a pandemia do ponto de vista da cibersegurança dando conta da sua interferência em todas as previsões.

TENDÊNCIAS EM AGENTES E TTP

Considerando as ameaças já identificadas, deve observar-se que existe uma elevada probabilidade de elas se manterem. Além disso, assiste-se a uma tendência de convergência cada vez mais acentuada entre tipos de atores estatais, paraestatais e não estatais na concretização de atividades hostis, reforçando-se o papel dos cibercriminosos, dos agentes estatais e dos hacktivistas, bem como a relação entre si. Por isso, a sua categorização e identificação clara tendem a tornar-se mais complexas de se realizar.

As TTP associadas ao universo destes agentes são cada vez mais fáceis de obter e de utilizar através de serviços e produtos de cibercrime vendidos *online*, como referido anteriormente, facto que, portanto, tende a intensificar-se. A multiplicação dos vetores de ataque contribuirá para o aumento de oportunidades e de hipóteses de sucesso, dificultando ainda mais a criação de perímetros de segurança.

É expectável que em 2020 e 2021 estes agentes de ameaças continuem a persecução dos seus objetivos táticos e estratégicos e que explorem novas vulnerabilidades nas dimensões digitais emergentes, como a Internet das Coisas, as redes 5G, a Inteligência Artificial e a criptomineração, o que representa um aumento da superfície de ataque.

Destaques

Tendência para a convergência entre atores estatais, paraestatais e não estatais, dificultando a atribuição, e para o reforço das atividades de cibercriminosos, agentes estatais e hacktivistas.

Tendência para maior facilidade na obtenção dos instrumentos envolvidos nas TTP dominantes e para o aumento dos vetores e superfícies de ataque.

TENDÊNCIAS GLOBAIS

Na transformação destas ameaças em incidentes e cibercrimes, é importante considerar algumas tendências globais, quer devido a fatores tecnológicos, quer comportamentais. Uma das consequências mais relevantes destas dinâmicas é o referido aumento da superfície de ataque, com efeito na multiplicação dos vetores. Tendo um cunho global, esta tendência afeta também Portugal, ainda que com ritmos específicos, considerando as características sociais e económicas do país. Vejamos algumas tecnologias cujo desenvolvimento aumenta as oportunidades para a realização de ataques, mas também para a criação de inovações nos modos através dos quais estes se realizam. Acrescentamos alguns dados fornecidos por fontes internacionais:

Aumento da quantidade de dispositivos em rede, no âmbito da Internet das Coisas, bem como a importância estabilizada dos *smartphones*:

> Há cerca de 21 mil milhões de dispositivos do tipo Internet das Coisas no mundo – perspetiva-se que em 2025 este número seja o dobro;
>
> Na primeira metade de 2019 os ciberataques a dispositivos da Internet das Coisas aumentaram 300%;
>
> A Internet das Coisas intensifica os efeitos cinéticos de um ciberataque e as vulnerabilidades em relação à proteção de dados.

(WEF, 2020)

Emergência do 5G, com desafios tecnológicos e comerciais:

> A implementação do 5G exige novos controlos de risco.

(NISCG, 2020)

Crescente aplicabilidade da Inteligência Artificial:

> A Inteligência Artificial é cada vez mais usada para *deep fakes*;
>
> Com a Inteligência Artificial, a atribuição no cibercrime é ainda mais difícil.

(ENISA, 2019)

Desenvolvimento da Computação Quântica:

> A computação quântica torna obsoletas antigas aplicações de cibersegurança.

(ENISA, 2019)

Uso crescente das Plataformas em Nuvem:

> Uso que ameaça mais a proteção de dados.

(WEF, 2020)

Digitalização de grande parte dos serviços essenciais:

> Os ciberataques aos serviços essenciais são um dos maiores riscos em 2020.

(WEF, 2020)

O *Global Risk Report 2020*, do World Economic Forum, coloca os ciberataques como o 7º risco mais provável no mundo e o 8º com mais potencial de impacto, reconhecendo que já no presente os ciberataques são cada vez mais frequentes contra organizações e indivíduos. Identificam-se dois aspetos, neste documento do World Economic Forum, que são importantes de destacar no que se refere ao contexto de governação do ciberespaço: **1)** o caráter fragmentado dos quadros normativos de regulação do setor das TIC, dentro de uma determinada área e mesmo de país para país, o que dificulta uma ação global e coordenada contra o cibercrime; e **2)** as consequências não intencionais, imprevisíveis, de certos desenvolvimentos tecnológicos, como é o caso da Inteligência Artificial. A dificuldade de coordenação e a imprevisibilidade da tecnologia tornam a governação da cibersegurança no mundo mais incerta (WEF, 2020).

Em termos de cibercrime, o Relatório da Europol *Internet Organized Crime Threat Assessment*, de 2019, identifica algumas ameaças à UE, que caracterizam 2019 e se estendem para 2020, que podem ser ameaças também para Portugal: o *ransomware* (apesar de existir menos em relação a anos anteriores, tem mais impacto); a fraude com cartões de crédito; a CEO *fraud*; o DoS/DDoS com extorsão; ataques à cadeia de fornecimento; a crescente digitalização do terrorismo; uma maior apetência para os ataques a dados; e o *phishing* e as criptomoedas a permanecerem como veículos transversais às ciberameaças. Também este documento, do ponto de vista da governação, tal como o *Global Risk Report* de 2020, aponta para a necessidade de haver articulação internacional para que o combate ao cibercrime funcione.

DESTAQUES

Tendências globais tecnológicas com implicações regionais no aumento da superfície de ataque: a Internet das Coisas, o 5G, a Inteligência Artificial, a Computação Quântica e as Plataformas em Nuvem.

Tendências que dificultam a governação da cibersegurança: fragmentação de *standards* e de regulamentações, bem como as consequências não intencionais.

Tendências globais no cibercrime: maior impacto do *ransomware*, crescimento da fraude, ameaças à cadeia de fornecimento e aos dados, digitalização do terrorismo, *phishing* e criptomoedas como ferramentas transversais.

O CASO COVID-19

A importância da pandemia de Covid-19 durante o ano de 2020, incidindo no mesmo período de publicação deste Relatório, exige uma análise às características e aos possíveis efeitos permanentes que este acontecimento tem e terá na cibersegurança nacional. Durante o período sujeito à pandemia, e que ainda vigora na data de publicação deste Relatório, assistiu-se, por parte de agentes maliciosos, à utilização da temática e do alarme relativos a esta doença por forma a tirarem partido da disposição dos indivíduos para reagirem ou procurarem soluções. As ameaças em termos de TTP mais identificadas foram:

> *Phishing/smishing* (através de *email*, SMS e redes sociais) a utilizar o nome de organizações ligadas à saúde, instituições internacionais como a UNICEF, a Organização Mundial de Saúde e laboratórios, procurando a captura de dados pessoais ou infetando os dispositivos com *malware*;
>
> *Malware*, algum dele *ransomware*, distribuído através de *emails* ou de redirecionamento de DNS (Sistema de Nomes de Domínio);
>
> Aplicações que oferecem funcionalidades no âmbito da pandemia de Covid-19, mas distribuem *malware*, em alguns casos *ransomware*;
>
> Fraudes digitais que recolhem donativos através de *crowdfunding* para a falsa compra de materiais médicos na ajuda à luta contra a doença;
>
> Páginas de *internet* falsas, ou ofertas fraudulentas, para venda de materiais médicos contra a doença;
>
> Venda na *darkweb* de Kits Covid-19, os quais permitem realizar ciberataques a indivíduos em teletrabalho;
>
> Campanhas de desinformação que culpabilizam pela pandemia grupos minoritários e Estados.

Durante o mês de março de 2020, que corresponde ao início da resposta nacional à pandemia, o CERT.PT registou 138 incidentes, o que corresponde a um aumento de 84% em relação a fevereiro, que havia registado 75 incidentes. Se compararmos com os mesmos meses do ano anterior, verificamos que em 2019 houve apenas 57 incidentes em fevereiro e 50 em março – portanto, o mês de março de 2020 teve mais 176% de incidentes do que o de 2019. Quanto ao *phishing*, em março de 2020 assiste-se a um aumento de 217% em relação a fevereiro do mesmo ano, passando-se de 18 incidentes para 57.

26. Incidentes (total e *phishing*) registados pelo CERT.PT em março de 2020, comparação com fevereiro e meses homólogos

Fev. 2019		Mar. 2019		Fev. 2020		Mar. 2020	
Phishing	**Total Inc.**	***Phishing***	**Total Inc.**	***Phishing***	**Total inc.**	***Phishing***	**Total Inc.**
17	57	23	50	18	75	57	138

Tabela 30 | CERT.PT

Incidentes (total) registados pelo CERT.PT, entre janeiro e março de 2020

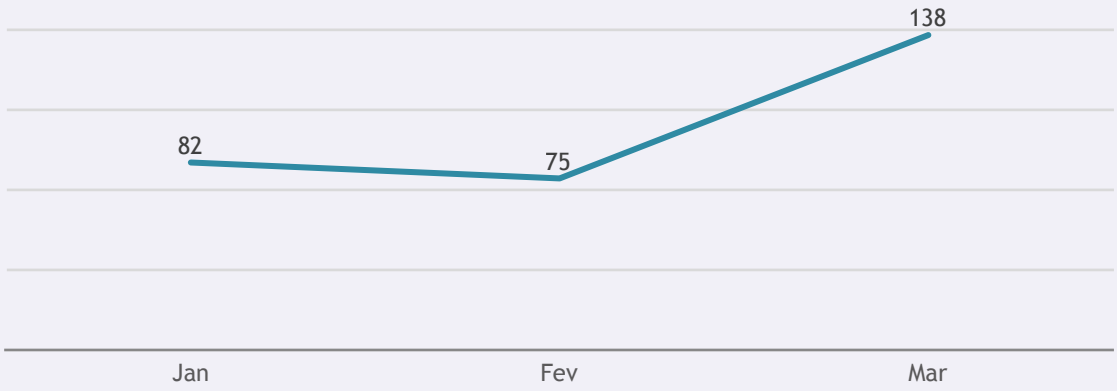


Figura 31 | CERT.PT

Incidentes registados pelo CERT.PT no mês de março, entre 2016 e 2020

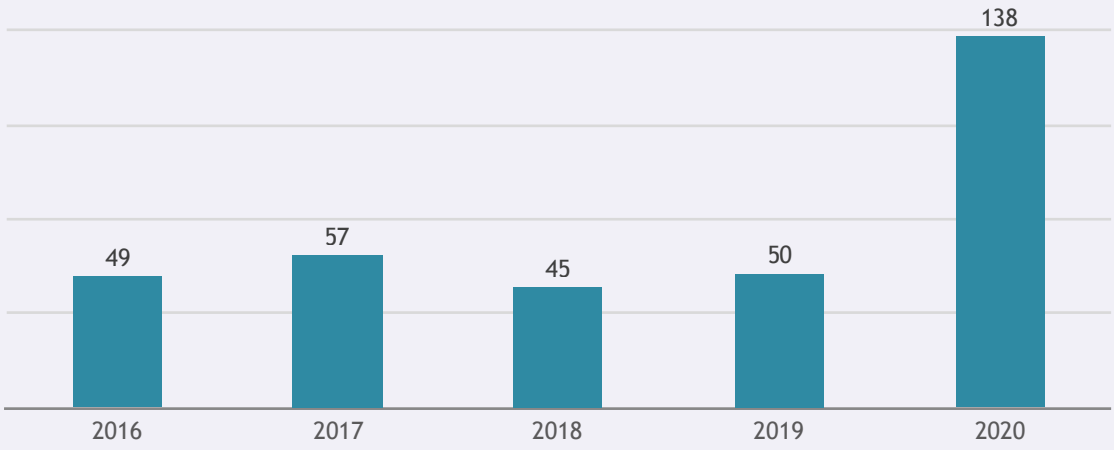


Figura 32 | CERT.PT

Em consonância com estes registos, em documento do Gabinete de Cibercrime do Ministério Público, *Nota Informativa COVID 19: cibercrime em tempo de pandemia,* já referenciado, é possível identificar um aumento das denúncias recebidas no mesmo período. Enquanto no ano de 2019 houve, no total, 193 denúncias, em 2020, até 16 de abril, já se registavam 162, quase tantas como no ano anterior. Entre fevereiro e março de 2020 ocorreu um aumento em mais do dobro, de 20 denúncias para 46, respetivamente, um aumento de 130%. Os crimes mais reportados foram as fraudes na utilização da aplicação de pagamentos MB WAY, mensagens de *email* e SMS com *malware*, campanhas de *phishing* e extorsão via *email* (MP, 2020).

Em muitos destes casos, tal como em 2019, a engenharia social é uma ferramenta de ataque muito importante na medida em que utiliza a preocupação e a informação sobre uma situação hegemónica a nível social para conduzir os indivíduos a agirem contra os seus próprios interesses, beneficiando agentes maliciosos. É um exercício conjetural realizar prospetivas quanto a este acontecimento e ao nível de interferência que pode vir a ter na cibersegurança nacional, contudo, a natureza preponderante do mesmo a isso obriga. A este respeito, devem considerar-se, por um lado, a interferência deste evento em tendências já identificadas; e, por outro, as novas tendências que ele pode promover.

Quanto à interferência nas tendências globais já identificadas:

> O esperado desaceleramento, e mesmo recessão, a nível económico poderá ter como efeito atrasar a implementação de algumas das tecnologias que colocam desafios à cibersegurança, como é o caso do 5G;
>
> Não obstante, a relevância acrescida que adquiriu a utilização dos dados pessoais dos cidadãos no combate à doença pode tornar mais relevantes as tecnologias que os utilizam de forma mais central, como a Internet das Coisas, a Inteligência Artificial e a Computação em Nuvem;
>
> Um aumento da pressão sobre os organismos internacionais no sentido de melhorarem a cooperação internacional no campo da cibersegurança, mas também a possibilidade de a componente restritiva da pandemia reforçar o fechamento nacional;
>
> Intensificação dos veículos identificados de cibercrime que utilizam as fragilidades do fator humano: *phishing*, *ransomware*, fraude, com aproveitamento da crescente utilização dos dados.

Quanto ao desenvolvimento de tendências específicas fruto da pandemia de Covid-19:

> Continuidade no aproveitamento da temática da Covid-19 para ações de engenharia social, através de *phishing* e *malware*, eventualmente utilizando *emails*, SMS e aplicações;

Desafio para os Estados democráticos quanto ao dilema que opõe segurança e privacidade. A utilização dos dados dos cidadãos com a justificação de necessidade de controlo da pandemia tem conduzido à aceitação social desta utilização. Existe o risco de, no mundo pós-pandemia, algumas destas medidas não serem revertidas, algo que pode facilitar o uso abusivo dos dados pessoais;

Aproveitamento por parte de cibercriminosos das fragilidades sociais e económicas, ligadas ao desemprego, por exemplo, para realizarem fraudes, reproduzindo as TTP relacionadas com a pandemia de Covid-19 em temas do âmbito de uma crise económica;

Aumento dos ataques a serviços essenciais e a infraestruturas críticas, aproveitando a maior dependência do digital;

A desestabilização social pode aumentar a atividade dos hacktivistas através de ações que procurem provocar impacto mediático e danos reputacionais, como sejam DDoS, *data breaches* ou compromissos de contas;

A crise económica e a desestabilização social podem ser vistas por alguns Estados como oportunidades para campanhas de desinformação e de ciberataques que comprometam a soberania de outros Estados.

DESTAQUES

A pandemia de Covid-19 foi uma oportunidade para agentes maliciosos realizarem ciberataques oportunistas, utilizando esta temática, através de *phishing*, *smishing*, *ransomware*, fraudes e desinformação.

Registou-se um aumento de 85% no número de incidentes reportados ao CERT.PT entre fevereiro e março de 2020 e de 176% comparando o mês de março de 2020 com o mês homólogo de 2019 - também os crimes *online* denunciados ao Ministério Público aumentaram para mais do dobro (130%), entre fevereiro e março.

Este acontecimento hegemónico interfere nas tendências globais e nacionais perspetivadas: possível desaceleramento do desenvolvimento de algumas tecnologias críticas para a cibersegurança, como o 5G; aprofundamento dos fatores de risco associados à segurança dos dados pessoais; desafios à coordenação internacional para a cibersegurança; aumento dos ciberataques de cibercriminosos que utilizam engenharia social oportunista em relação a uma previsível crise económica e social; crise económica e social que pode também favorecer ciberataques com motivos políticos.

Síntese do Subcapítulo Prospetivas

Tendência para maior articulação entre ameaças estatais e não estatais, com reforço dos cibercriminosos, dos agentes estatais e dos hacktivistas, além de maior superfície e mais vetores de ataque, acesso a ciberameaças facilitado e crescente dificuldade na atribuição.

Tendências globais relevantes: tecnologias emergentes (Internet das Coisas, 5G, Inteligência Artificial, Computação Quântica e Plataformas em Nuvem) que aumentam a superfície e os vetores de ataque; fragmentação e imprevisibilidade da governabilidade da cibersegurança a nível internacional; importância de certas ciberameaças, como *ransomware*, fraude, *phishing* e ataques à cadeia de fornecimento.

A pandemia de Covid-19 vem trazer um potencial de interferência em todas as previsões, ameaçando alterar umas e intensificar outras, e trazendo consigo novas tendências: possível desaceleramento de algumas tecnologias; ameaça à proteção dos dados pessoais; aumento dos ciberataques que usam a engenharia social oportunista; ameaça a serviços essenciais e infraestruturas críticas; e possível uso político da crise económica e social por agentes de desinformação ou de desestabilização sociopolítica.

G. NOTAS CONCLUSIVAS

Espera-se que os dados e as análises apresentados sejam úteis para as partes interessadas, em particular para todos aqueles que têm um papel na segurança do ciberespaço de interesse nacional. O objetivo é que possam agir com mais informação sobre as principais ameaças e as suas tendências.

As ciberameaças dominantes mostram a necessidade de existirem investimentos das organizações em cibersegurança, quer do ponto de vista técnico (contra a ameaça tão presente da infeção por *malware,* por exemplo), quer em termos humanos (a melhor forma de combater o *phishing* é educando o utilizador). Mostra também como alguns períodos do ano são mais críticos, como o segundo semestre, mas nem sempre (2020 revela já um primeiro semestre acima da média devido à pandemia de Covid-19). Mas também evidencia a hegemonia de alguns agentes de ameaças, como os cibercriminosos e os agentes estatais, muitas vezes agindo em colaboração estreita. Quanto ao futuro, mapeia as novas tecnologias que colocam desafios à cibersegurança e tornam esta mais crítica e complexa. Considerando o acontecimento tão presente da pandemia de Covid-19, este Relatório também faz notar a forma como os agentes de ameaças são oportunistas em relação às crises, utilizando a engenharia social para atacarem cidadãos fragilizados e serviços essenciais. Precisamente por isso, é importante estar preparado para o mesmo tipo de ameaça no que se refere às consequências da pandemia, bem como em relação às mudanças que ela produz nas previsões que se faziam antes do seu surgimento.

Pretende-se manter a regularidade na publicação deste documento, estabilizando os indicadores apresentados, produzindo novos e procurando melhorar a comparabilidade internacional de alguns dos dados. Desse modo, será possível manter as linhas temporais da análise, bem como uma avaliação mais relativa da posição de Portugal nestas matérias, comparando com outros países.

H. NOTAS METODOLÓGICAS

O *Relatório Cibersegurança em Portugal – Linha de Observação Riscos & Conflitos* utiliza fontes diversas na sua natureza e nas metodologias aplicadas na recolha dos dados. Recorre-se a fontes abertas que fornecem resultados de inquéritos, como as do Eurostat, mas também a dados disponibilizados por algumas organizações diretamente, como os relativos ao cibercrime, da DGPJ. Não obstante, uma parte muito importante deste Relatório resulta de dados produzidos pelo próprio CNCS, nomeadamente pelo CERT.PT, ou que são obtidos junto da RNCSIRT.

O inquérito do Eurostat *Security incidents and consequences* corresponde a uma parcela de dados recolhida pelas instituições de estatísticas nacionais de cada país da UE (INE, em Portugal), numa base anual, no âmbito dos questionários ao uso das TIC e do comércio eletrónico nas empresas. O questionário, em Portugal, foi respondido por via eletrónica ou postal, por 7203 empresas, entre fevereiro e julho de 2019. O inquérito, também do Eurostat, *Security related problems experienced through using the internet for private purposes* enquadra-se no âmbito dos dados recolhidos pelo Eurostat referentes ao uso das TIC por parte dos indivíduos, também através do INE, em Portugal. O respetivo questionário é aplicado por via eletrónica, postal e presencial. Em Portugal, foi respondido por 6624 pessoas, o que corresponde a um igual número de agregados domésticos, entre abril e julho de 2019. Para mais detalhe sobre a metodologia destes inquéritos do Eurostat, consultar as fontes.

Os dados do CERT.PT têm duas origens principais. Por um lado, as notificações realizadas pela comunidade que são convertidas em incidentes confirmados. Por outro, observáveis recolhidos de forma automatizada num conjunto de 84 fornecedores de observáveis e eventos de segurança, selecionados por critérios de confiança na fonte, relevo da tipologia de observações e pertinência da informação para o contexto de atuação do CNCS. Os números de incidentes e de observáveis registados estão sujeitos a variações na motivação social para realizar notificações de incidentes e à instabilidade na quantidade e no tipo de algumas das fontes dos observáveis.

O inquérito à RNCSIRT foi realizado pela própria RNCSIRT, e inclui os dados do CERT.PT, enquanto membro da referida rede, em articulação com o Observatório de Cibersegurança.

O questionário foi respondido por via eletrónica, registando-se 28 respostas, das quais 21 foram consideradas válidas para este Relatório, num universo de 42 membros, entre janeiro e fevereiro de 2020.

Os dados da CNPD foram fornecidos diretamente pela organização em causa, resultando da sua própria atividade durante 2018 e 2019.

No que diz respeito ao cibercrime, grande parte da informação é fornecida pela DGPJ, a qual faz o seu próprio trabalho de recolha junto das diversas organizações de Justiça e de Segurança no país que são responsáveis pelos registos criminais. Os dados do Ministério Público foram publicados pelo próprio em comunicado à imprensa e correspondem ao número de queixas recebidas pelo seu Gabinete de Cibercrime. A APAV também fornece alguns dados neste contexto, embora mais no âmbito das vítimas do que da Justiça. A informação partilhada é pública e corresponde à sua própria atividade durante 2019 no que à Linha Internet Segura diz respeito.

Por fim, a análise qualitativa efetuada no capítulo Ameaças e Prospetivas resulta dos dados apresentados no capítulo Atores e Incidentes, mas também em parte da colaboração dos parceiros deste Relatório, nomeadamente a comunidade de informações, na avaliação do presente e do futuro quanto aos riscos que o ciberespaço enfrenta. Estes dados e estas análises são acompanhados pela consideração de alguns estudos de referência aí identificados.

I. ENTIDADES PARCEIRAS

Associação Portuguesa de Apoio à Vítima

Centro de Ciberdefesa

Comissão Nacional de Proteção de Dados

Direção-Geral de Política de Defesa Nacional

Direção-Geral de Estatísticas da Educação e Ciência

Direção-Geral de Políticas de Justiça

Rede Nacional CSIRT

Serviço de Informações de Segurança

Serviço de Informações Estratégicas de Defesa

J. CONSELHO CONSULTIVO

Alexandre Sousa Pinheiro
(Professor Universitário em Direito)

António Brandão Moniz
(Faculdade de Ciências e Tecnologia – Universidade Nova de Lisboa)

José Luís Garcia
(Instituto de Ciências Sociais – Universidade de Lisboa)

Luís Antunes
(Faculdade de Ciências – Universidade do Porto)

Manuel Mira Godinho
(Instituto Superior de Economia e Gestão – Universidade de Lisboa)

Maria Eduarda Gonçalves
(ISCTE – Instituto Universitário de Lisboa)

Paulo Esteves-Veríssimo
(Universidade do Luxemburgo)

Pedro Miguel Alves Ribeiro Correia
(Instituto Superior de Ciências Sociais e Políticas
– Universidade de Lisboa)

Sandro Miguel Ferreira Mendonça
(ISCTE – Instituto Universitário de Lisboa)

K. REFERÊNCIAS PRINCIPAIS

RELATÓRIOS

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

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

Europol (2019a) *CEO/Business Email Compromise (BEC) fraud*, Europol EC3.

Europol (2019b) *Europol Internet Organized Crime Thread Assessmen*t, Europol EC3.

MP (2020) *Nota Informativa COVID 19: cibercrime em tempo de pandemia,* Ministério Público, Procuradoria-Geral da República, Gabinete de Cibercrime.

NISCG (2020) *Cybersecurity of 5G Networks: EU toolbox of risk mitigating measures*, NIS Cooperation Group.

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

WEF (2020) *Global Risks Report 2020*, World Economic Forum.

INQUÉRITOS

Eurostat (2020a) *Security incidents and consequences*. Code: isoc_cisce_ic.

Eurostat (2020b) *Security related problems experienced through using the internet for private purposes*. Code: isoc_cisci_pb.

OUTROS DOCUMENTOS

Eurostat (2019) *Newsrelease ICT usage in households and by individuals in 2019*, Eurostat.

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

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

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

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

RNCSIRT (2012) *Taxonomia Comum para a Rede Nacional de CSIRT*, CERT.PT e Fundação para a Computação Científica Nacional.

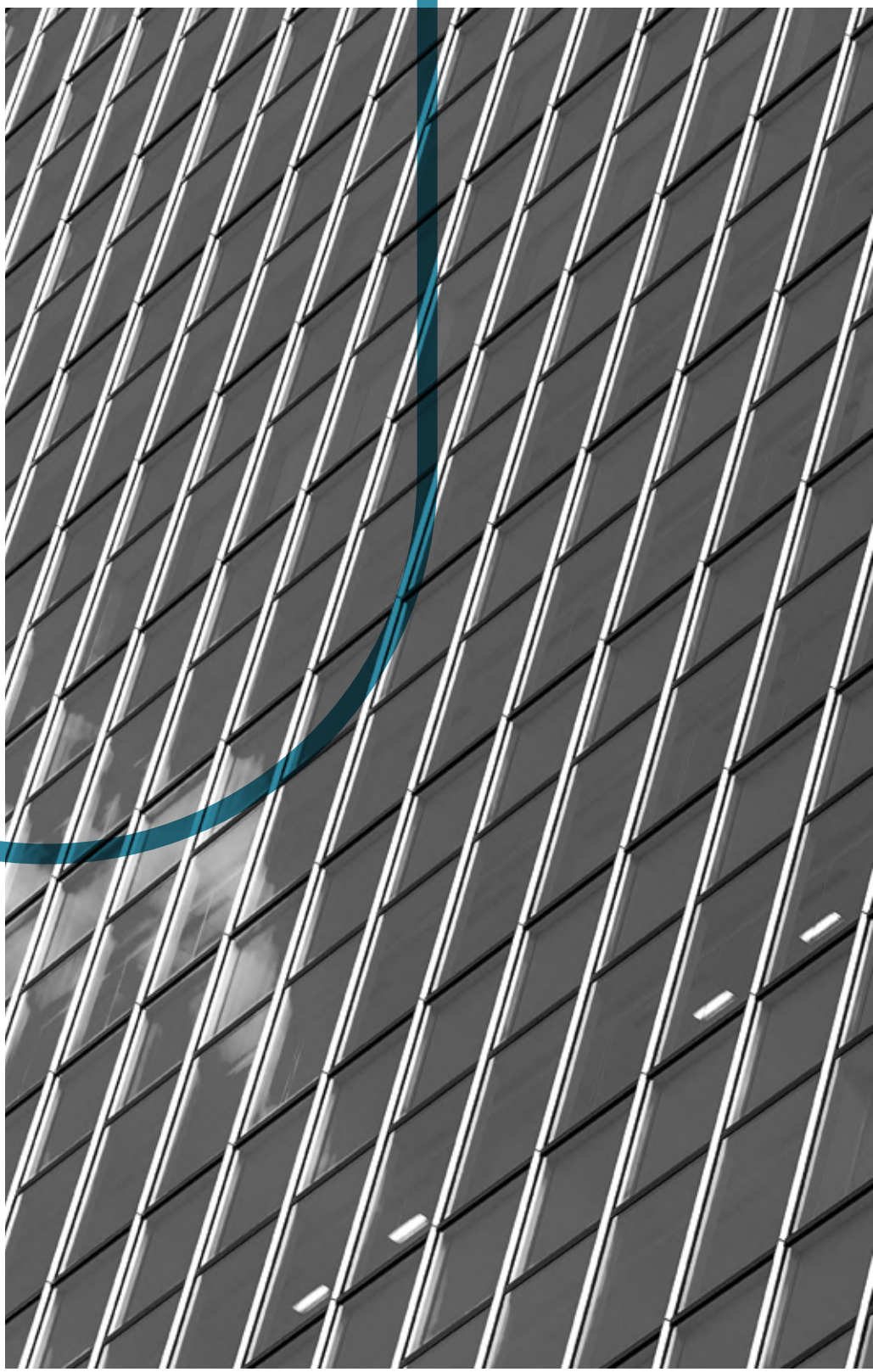
WEBSITES

https://csrc.nist.gov/glossary

https://stixproject.github.io

https://www.kb.cert.org

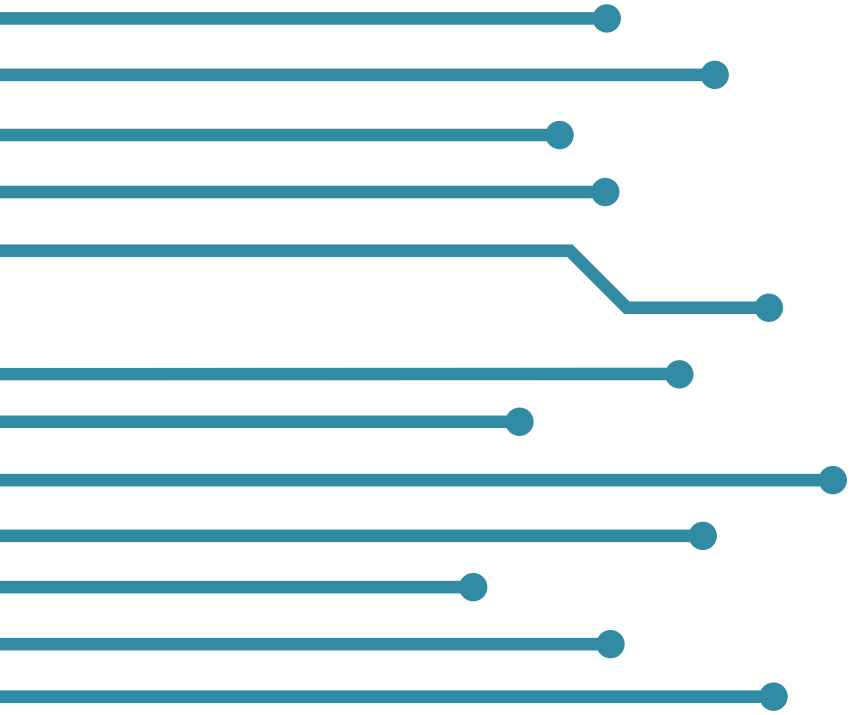
https://www.redecsirt.pt



CNCS
Centro Nacional de Cibersegurança PORTUGAL

ANEXO
TABELAS DETALHADAS

Observatório de **Cibersegurança**



A. (8) Incidentes por classe e tipo registados pelo CERT.PT, 2019 – TOTAL

Classe	Tipo	Jan.	Fev.	Mar.	Abr.	Mai.	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	TOTAL
Conteúdo Abusivo	Direitos de Autor	1	2	0	0	0	0	0	0	0	0	0	0	3
	SPAM	1	2	0	4	2	2	1	0	0	1	0	4	17
Disponibilidade	DoS/DDoS	3	1	2	0	2	0	0	2	3	9	2	3	27
	Sabotagem	0	0	0	0	0	0	1	1	1	0	0	0	3
Fraude	Utilização Ilegítima de nome de terceiros	2	2	0	0	1	0	3	2	1	1	4	3	19
	Utilização indevida ou não autorizada de recursos	0	0	0	0	0	1	3	1	1	1	0	0	7
Intrusão	Compromisso de Conta	10	2	3	8	10	7	5	12	17	7	7	7	95
	Exploração de Vulnerabilidade	5	5	5	7	7	8	10	4	2	1	2	2	58
Malware	Distribuição	5	1	1	6	4	6	6	2	10	2	2	10	55
	Indeterminado	0	1	0	0	0	0	0	0	0	0	0	0	1
	Infeção	10	10	8	6	6	7	10	11	11	12	22	10	123
Outro	*Blacklist*	1	1	1	1	1	0	2	1	0	0	2	0	10
	Indeterminado	0	4	1	0	1	0	2	1	2	4	2	0	17
Recolha de Informação	*Phishing*	13	17	23	17	22	16	16	23	27	19	24	19	236
	Scan	4	6	4	6	0	1	0	4	1	1	1	0	28
Segurança da Informação	Acesso não autorizado	0	0	0	0	0	1	1	0	1	0	0	3	6
	Modificação / Remoção não autorizada	0	0	0	0	0	0	0	1	0	0	0	0	1
Tentativa de Intrusão	Exploração de Vulnerabilidade	2	0	2	2	1	4	0	1	0	2	3	1	18
	Tentativa de *login*	2	3	0	5	2	2	2	6	2	0	2	4	30
Total		59	57	50	62	59	55	62	72	79	60	73	66	754
Vulnerabilidade	Serviço vulnerável	7	7	4	2	11	5	10	12	6	3	4	8	79
Total		66	64	54	64	70	60	72	84	85	63	77	74	833

Tabela A | CERT.PT

B. (9) Incidentes por setor e área governativa registados pelo CERT.PT, 2019 - *RANKING* TOTAL

	Setor e Área Governativa	Nº	%
1º	Outros	251	27,6
2º	Infraestruturas Digitais	170	18,7
3º	Prestador de Serviços de Internet	167	18,4
4º	Educação, Ciência, Tecnologia e Ensino Superior	81	8,9
5º	Banca	69	7,6
6º	Transportes	30	3,3
7º	Serviços de Computação em Nuvem	26	2,9
8º	Administração Local	18	2,0
9º	Saúde	11	1,2
10º	Infraestruturas do Mercado Financeiro	11	1,2
11º	Energia	9	1
12º	Defesa Nacional	9	1
13º	Órgãos de Soberania	9	1
14º	Presidência do Conselho de Ministros	9	1
15º	Agricultura	7	0,8
16º	Administração Regional	5	0,6
17º	Cultura e Turismo	4	0,4
18º	Setor das Águas	4	0,4
19º	Administração Interna	4	0,4
20º	Trabalho, Solidariedade e S.S.	4	0,4
21º	Economia	4	0,4
22º	Negócios Estrangeiros	3	0,3
23º	Ambiente	3	0,3
24º	Serviços de Motor de Pesquisa em Linha	1	0,1
25º	Infraestruturas e Planeamento	1	0,1
26º	Serviço de Mercado em Linha	1	0,1
27º	Justiça	1	0,1

Tabela B | CERT.PT

C. (12) Observáveis por tipo registados pelo CERT.PT, 2019 - *RANKING* TOTAL

RK	Tipo	Nº	%
1º	Serviço vulnerável	50932870	92,7
2º	*Blacklist*	2530931	4,6
3º	*Botnet drone*	887418	1,6
4º	*Malware*	290463	0,5
5º	Força-bruta	103199	0,1
6º	*Scan*	43530	0,07
7º	Outro	38695	0,07
8º	*Phishing*	31625	0,05
9º	Nulos	31363	0,05
10º	Alerta IDS	17494	0,03
11º	C&C	10093	0,01
12º	Compromisso	2942	0,005
13º	Distribuição	2875	0,005
14º	Tentativa de *login*	1491	0,003
15º	SPAM	377	0,001

Tabela C | CERT.PT

D. (13) Observáveis por setor e área governativa registados CERT.PT, 2019 – *RANKING* TOTAL

RK	Setor e Área Governativa	Nº	%
1º	Prestadores de Serviços de Internet	31248303	56,8
2º	Infraestruturas Digitais	10610563	19,3
3º	Nulos	8181627	14,8
4º	Educação, C. T. e Ensino Superior	1398687	2,5
5º	Outros	1375993	2,5
6º	Nenhum	1350890	2,4
7º	Serviços de Computação em Nuvem	394906	0,7
8º	Administração Pública	320816	0,5
9º	Energia	12886	0,02
10º	Transportes	12225	0,02
11º	Administração Central	5733	0,01
12º	Órgãos de Soberania	2320	0,004
13º	Presidência de Conselho de Ministros	1750	0,003
14º	Prestador de Serviços Digitais	1640	0,002
15º	Administração Local	1584	0,002
16º	Infraestruturas do Mercado Financeiro	1203	0,002
17º	Cultura e Turismo	1182	0,002
18º	Ambiente	1100	0,002
19º	Trabalho, Solidariedade e S.S.	905	0,001
20º	Administração Regional	322	0,0005
21º	Negócios Estrangeiros	292	0,0005
22º	Agricultura	122	0,0002
23º	Saúde	90	0,0001
24º	Banca	89	0,0001
25º	Administração Interna	59	0,0001
26º	Justiça	51	0,00009
27º	Regulador/Autoridade	26	0,00004
28º	Setor das Águas	2	0,000004

Tabela D | CERT.PT

E. (15) Incidentes por classe e tipo registados pela RNCSIRT, 2019 – TOTAL

Classe	Tipo	Jan.	Fev.	Mar.	Abr.	Mai.	Jun.	Jul.	Ago.	Set.	Out.	Nov.	Dez.	TOTAL
Conteúdo Abusivo	Direitos de Autor	14	13	12	15	8	26	12	20	24	18	5	11	178
	Porn. infantil, rac. e apol. violência	18	23	5	6	9	21	21	9	23	14	5	13	167
	SPAM	68	68	105	74	89	99	60	66	93	87	84	92	985
Disponibilidade	DoS/DDoS	15	17	14	15	20	13	13	23	27	43	38	27	265
	Sabotagem	6	5	4	3	2	4	6	7	8	8	9	0	62
Fraude	Utilização Ilegítima de nome de terceiros	23	30	438	44	22	68	30	61	79	10	47	21	873
	Utilização indevida ou não autorizada de recursos	20	27	72	76	128	151	176	239	288	264	188	193	1822
Intrusão	Compromisso de Conta	35	34	35	49	52	37	32	50	52	31	35	31	473
	Exploração de Vulnerabilidade	28	35	41	38	51	25	38	37	41	26	23	27	410
Malware	C&C	0	0	42	1	0	0	1	2	3	0	0	0	49
	Distribuição	19	14	9	21	14	15	12	14	24	26	22	31	221
	Indeterminado	64	52	74	73	65	54	56	41	79	102	117	65	842
	Infeção	110	125	113	70	111	71	132	214	146	310	296	328	2026
Outra	Outro	80	89	133	180	100	166	64	47	145	290	317	202	1813
Recolha de Informação	*Phishing*	119	119	166	141	140	148	162	129	219	169	249	185	1946
	Sniffing	5	6	8	2	4	8	6	2	8	4	4	5	62
	Scan	85	84	69	108	91	55	104	119	51	89	112	95	1062
Segurança da Informação	Acesso não autorizado	20	9	25	21	48	48	35	39	49	81	73	98	546
	Modificação / Remoção não autorizada	14	11	4	1	3	2	6	11	1	7	5	9	74
Tentativa de Intrusão	Exploração de Vulnerabilidade	26	53	30	38	43	31	33	31	42	26	34	23	410
	Tentativa de *login*	72	66	74	114	52	89	57	43	79	101	102	104	953
Total		841	880	1473	1090	1052	1131	1056	1204	1481	1706	1765	1560	15239

F. (17) Crimes registados pelas autoridades policiais, por crimes informáticos, devassa por meio informático e burla informática/comunicações, entre 2009 e 2018

Tipo de crime	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009	2009 a 2018
Devassa p/meio de informática (contra pessoa)	456	499	443	386	362	352	314	289	295	218	3 614
Burla informática/ comunicações (contra património)	9783	8149	8448	7830	4508	3458	3618	2695	2115	1582	52 186
Reprodução programa protegido	4	12	11	28	36	17	12	41	48	97	306
Acesso/interceção ilegítimos	395	470	415	409	304	259	278	333	353	378	3 594
Viciação/destruição/ dano relativo a dados/ programas	32	24	20	11	11	13	7	7	8	8	141
Falsidade informática	220	196	139	101	49	36	59	39	34	6	879
Sabotagem informática	226	249	188	76	37	21	17	12	13	16	855
Outros informáticos	47	25	28	34	32	13	23	28	39	29	298
Informáticos Total	924	976	801	659	469	359	396	460	495	534	6 073
Total geral	11163	9624	9692	8875	5339	4169	4328	3444	2905	2334	61 873

Tabela F | DGPJ

G. (18) condenados em processos crime em fase de julgamento findos nos tribunais de 1ª instância, por crimes da lei da criminalidade informática, de devassa por meio informático e de burla informática/comunicações, entre 2009 e 2018*

Tipo de crime	2018	2017	2016	2015	2014	2013	2012	2011	2010	2009	2009 a 2018
Devassa p/meio de informática (contra pessoa)	..	..	..	..	3	6	5	..	..	4	27
Burla informática/ comunicações (contra património)	123	179	185	195	155	216	160	139	99	95	1 546
Falsidade informática	23	19	24	15	20	8	12	3	7	..	132
Dano rel. dados/ programas	5	..	..	3	..	..	..	..	..	..	13
Dano rel. dados/ programas TENT	..	..	..	..	..	..	..	..	..	..	..
Dano rel. dados/ programas agrav	..	..	..	..	..	..	..	..	..	..	..
Sabotagem informática	..	..	3	..	..	..	..	5	..	..	17
Acesso ilegítimo	4	5	7	4	6	10	8	3	..	..	51
Acesso ilegítimo TENT	..	..	..	..	..	..	..	..	..	..	..
Acesso ilegítimo agravado	..	..	3	..	..	..	..	..	..	..	5
Reprodução ileg. prog. protegido	6	3	16	12	15	7	12	7	20	24	122
Reprod. ileg.prog.proteg. TENT	..	..	..	..	..	..	..	..	..	..	..
Outros inform./ informáticos ne	..	..	..	..	..	..	..	..	..	3	6
Informáticos Total	42	30	55	36	44	28	35	19	29	33	351
Total geral	167	211	242	231	202	250	200	160	129	132	1 924

* .. Resultado nulo/protegido pelo segredo estatístico.

Tabela G | DGPJ

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**