BRANDEFENSE COUNTRY REPORT · PORTUGAL 2026

Brandefense Panorama de Ciberameaças em Portugal 2026

Perturbação no setor público, exposição na cadeia de fornecimento e fraude de identidade móvel nos serviços digitais de Portugal

Odin by Brandefense
Janela de investigação: 1 jan a 26 nov 2026 (UTC; recente: 12 a 26 nov)
Versão 1.0 · Edição pública de investigação · TLP:CLEAR · 27 nov 2026

83 de 247
domínios avaliados apresentavam uma credencial à venda na verificação

20
incidentes públicos oficialmente confirmados e amplamente noticiados (14 dossiês)

36
registos de ransomware com etiqueta Portugal em 17 etiquetas (face a 21 em 2025)

51
incidentes TIC graves ao abrigo do DORA reportados ao Banco de Portugal em 2025 (+16 homólogo)

ÍNDICE

Índice

Translated with AI

Esta edição em português europeu foi traduzida com IA a partir do original em inglês. Em caso de divergência, prevalece a edição em inglês.

01	Síntese executiva e prioridades defensivas	05
	Mapa do relatório	09
02	Perfil digital nacional e panorama de 2026	10
03	Exposição nacional e observações sobre domínios selecionados	17
04	Alegações e casos clandestinos	28
05	Incidentes públicos confirmados e divulgações	41
06	Perturbação, hacktivismo e alegação face à realidade	53
07	Ransomware, registos de extorsão e perfis de ameaça	57
08	Fraude, abuso de identidade e dano secundário	68
09	Banca, pagamentos e resiliência da identidade digital	72
10	Regulação, prazos de notificação e resposta nacional	76
11	Perspetivas e cenários condicionais de planeamento	80
12	Plano de ação e evidências de conclusão	84
A	Apêndice A. Método, âmbito e exclusões	90
B	Apêndice B. Registo de evidências	93
C	Apêndice C. Fontes	94
D	Apêndice D. Glossário	100
	Sobre este relatório	102

Administração e direção executiva	01 02 10 11
CISO e operações de segurança	03 05 07 12
Fraude, banca e identidade digital	04 08 09
Setor público e resiliência OT	05 06 12
Jurídico, privacidade e conformidade	05 10 A

Sobre esta edição

Traduzido com IA. Esta edição em português europeu foi traduzida a partir do original em inglês (Brandefense Portugal Cyber Threat Landscape Report 2026). Em caso de divergência de redação, prevalece a edição em inglês.

51/100

Indicador nacional Atlas nos 247 domínios portugueses avaliados (retrato de 27 de novembro de 2026)

744 809

Publicações clandestinas com etiqueta Portugal (1 de janeiro a 26 de novembro de 2026; 97,7% em jan-fev)

36

Registos de ransomware com etiqueta Portugal (1 de janeiro a 26 de novembro de 2026; 21 em todo o ano de 2025)

EUR 5,3M

Perdas em fraude de pagamentos eletrónicos no 1.º semestre de 2025 (-40,4% homólogo; 51 incidentes DORA graves em 2025)

Índice e percursos de leitura

Capítulo	Questão respondida
1 Síntese executiva	Que conclusões e decisões exigem ação imediata da liderança?
2 Perfil nacional	Como interagem a adoção digital, os indicadores oficiais e o volume bruto?
3 Exposição nacional	Que sinais de credenciais, dispositivos e correio eletrónico exigem validação?
4 Alegações clandestinas	O que mostram os anúncios em fóruns, pedidos de compra e arquivos reciclados?
5 Incidentes públicos	Que eventos confirmados em 2026 e no final de novembro afetaram serviços em Portugal?
6 Perturbação e hacktivismo	Como se comparam as alegações com os registos oficiais e o impacto real?
7 Ransomware e grupos	Que etiquetas de extorsão visam Portugal e como se comparam os pares regionais?
8 Fraude e dano secundário	Como impulsionam os dados expostos, o malware móvel e o spoofing a fraude nacional?
9 Banca e pagamentos	Como visam os atacantes a banca de retalho, o Multibanco, o MB WAY e a CMD?
10 Regulação e prazos	Que autoridades, portais e prazos legais regem a resposta a incidentes em Portugal?
11 Cenários de planeamento	Que sinais operacionais devem alterar a postura defensiva após 26 de novembro de 2026?
12 Plano de ação	Quem atua, perante que sinal e que evidência de conclusão demonstra eficácia?
Apêndices A-D	Âmbito e exclusões, registo de evidências, fontes verificadas e glossário

CAPÍTULO 01

Síntese executiva e prioridades defensivas

01

ESTE CAPÍTULO RESPONDE

Que sinais de 2026 exigem ação imediata dos defensores em Portugal?

5

conclusões principais assentes em populações de evidência distintas

1.1 Cinco conclusões para a liderança 06

1.2 Quatro decisões executivas imediatas 07

1.3 Âmbito e fronteiras deste relatório 07

CAPÍTULO 01

Síntese executiva e prioridades defensivas

EM RESUMO

O panorama cibernético português em 2026 centra-se em paragens municipais e públicas, exposição de fornecedores, fraude móvel e fugas de credenciais. Nos 247 domínios avaliados, 83 (33,6%) tinham credenciais à venda na verificação. O indicador nacional Atlas é de 51/100. Os registos de ransomware subiram para 36 (vs 21 em 2025), com 20 incidentes confirmados e seis no final de novembro. Isole portais externos e controladores OT, exija MFA em acessos clínicos e municipais e feche os 87 domínios sem DMARC restritivo.

1.1 Cinco conclusões para a liderança

- **Anúncios ativos de credenciais atingem um terço dos domínios portugueses avaliados.** Na verificação de 27 de novembro de 2026, **83 de 247 domínios portugueses avaliados (33,6%)** apresentavam uma credencial associada à venda, e o **indicador nacional Atlas da carteira é de 51/100** [S4]. Os sinais históricos acumulados abrangem **235 domínios** com associações a dispositivos infetados e **238 domínios** com registos históricos de credenciais, enquanto **87 de 250 domínios selecionados (34,8%)** ainda não aplicam DMARC restritivo [S3][S4].
- **Autarquias e organismos públicos sofreram perturbações repetidas em 2026.** Ataques atingiram **Câmara Municipal da Guarda** (fevereiro), **Câmara Municipal de Serpa** (maio), **Câmara Municipal de Ovar** (outubro) e **Câmara Municipal de Santa Maria da Feira** (novembro) [S34-S36][S43-S45][S60-S61][S66-S67]. Registos nacionais foram expostos no **SNS 24 / SPMS** (>100 000 utentes) e na **ANEPC** (~60 000 bombeiros) [S39-S42] [S62-S63]. Entre **11 e 26 de novembro**, uma vaga atingiu **Worten**, **SMAS de Sintra**, **IMT**, **ASAE**, **Câmara Municipal do Porto** e **ADENE**, com confirmação ou avisos desde 12 de novembro [S68-S78].
- **Fornecedores externos e operadores OT remotos converteram falhas externas em impacto local.** Em maio, a falha global na **Instructure Canvas** afetou utilizadores universitários portugueses [S37][S38]. Em outubro, um servidor de testes de um subcontratado web expôs registos não classificados de sítios públicos do **SIRP** [S58] [S59]. Em novembro, um ataque pan-europeu a controladores de refrigeração atingiu sete lojas **Intermarché Portugal** [S64][S65].
- **Os registos em portais de extorsão subiram acentuadamente, liderados por The Gentlemen e Qilin.** A **Ransompedia** registou **36 entradas com etiqueta Portugal** entre 1 de janeiro e 26 de novembro de 2026, superando as **21** de todo o ano de 2025 [S2]. Uma duplicação no mesmo dia limita as entradas a no máximo **35 entidades distintas alegadas** [S2]. Trinta entradas surgiram entre junho e novembro, e duas coincidiram com ataques confirmados na **Santa Casa da Misericórdia de Santo Tirso** (Qilin) e na **Metro Mondego** (The Gentlemen) [S2][S46-S50].

- **As perdas em pagamentos eletrónicos caíram com os controlos do Banco de Portugal, mas a engenharia social e o malware móvel adaptaram-se.** Os dados oficiais do **Banco de Portugal** mostram uma queda homóloga de **40,4%** nas perdas do 1.º semestre de 2025, para **EUR 5,3 milhões**, apoiada pela confirmação de beneficiário e pelo **SPIN** [S12][S13]. Em paralelo, a **ANACOM** viu duplicar as queixas de spoofing telefónico e SMS até meados de julho de 2025, e o **CERT.PT** registou forte subida no phishing e no trojan Android `Toxic-Panda` [S5][S15]. Investigação de fevereiro de 2026 expôs ainda o trojan **Massiv** dirigido à **Chave Móvel Digital** [S81].

1.2 Quatro decisões executivas imediatas

1. **Separe ambientes de desenvolvimento externo, SaaS e manutenção remota dos sistemas centrais.** Exija garantias escritas de que agências web externas nunca copiam submissões reais de cidadãos para servidores de testes, e retire da Internet pública controladores OT de frio, edifícios e serviços públicos.
2. **Imponha MFA resistente a phishing e limites de consulta em portais públicos, clínicos e de acesso remoto.** Restrinja pesquisas e exportações em massa nos registos nacionais, exija MFA resistente a phishing em VPN e correio corporativo, e reforce a deteção de infostealers nos postos de trabalho.
3. **Feche a lacuna de 87 domínios sem DMARC restritivo e audite formulários públicos.** Migre os **68** domínios em monitorização (`p=none`) e os **19** sem registo válido para políticas DMARC `quarantine` ou `reject` , e proteja formulários que recolhem **NIF** e **IBAN**.
4. **Ensaie os prazos regulatórios de 2026 antes de ocorrer um incidente.** O **Regime Jurídico da Cibersegurança** (Decreto-Lei n.º 125/2025, de 4 de dezembro, em vigor desde 3 de abril de 2026) e o **MyCiber** (Regulamento n.º 756/2026) regem a cibersegurança [S22-S24]. Coexistem com o **DORA** (Lei n.º 73/2025) e o **RGPD** (Lei n.º 58/2019), cada um com prazos e autoridades próprios [S25-S27].

1.3 Âmbito e fronteiras deste relatório

Este relatório cobre a janela de atividade de **1 de janeiro a 26 de novembro de 2026 (UTC)**, com uma secção dedicada à atividade recente de **12 a 26 de novembro de 2026** [S1][S2]. As observações de exposição e configuração passiva refletem um retrato de **27 de novembro de 2026** em **250 domínios portugueses selecionados** [S3][S4]. A exposição externa avalia **247 domínios**, permanecendo **3** domínios por avaliar como desconhecidos e nunca como zero [S4]. As menções clandestinas a 365 dias decorrem de **27 de novembro de 2025 a 26 de novembro de 2026** [S4].

Quatro populações de evidência mantêm-se estritamente separadas ao longo do texto. Primeiro surgem as publicações retidas em fóruns, Telegram, sites de texto e Discord [S1]. Segundo surgem os registos de sites de extorsão na **Ransompedia** [S2]. Terceiro surgem a exposição externa e a configuração passiva nos 250 domínios selecionados [S3][S4]. Quarto surgem as fontes oficiais portuguesas, europeias e jornalísticas verificadas a 27 de novembro de 2026 [S5-S93]. Alegações clandestinas e entradas não confirmadas nunca são tratadas como intrusões confirmadas. Uma organização afetada só é nomeada quando existem simultaneamente confirmação oficial e ampla cobertura mediática, conforme `public_names.json` .

PRINCIPAIS CONCLUSÕES

01

Anúncios ativos de credenciais atingem 83 de 247 domínios portugueses avaliados, enquanto 87 de 250 não aplicam DMARC restritivo.

02

Paragens municipais, registos nacionais e fornecedores externos dominaram os incidentes confirmados em 2026.

03

Separe alegações de fóruns e fugas históricas recicladas antes de acionar notificações legais.

Mapa do relatório

Doze capítulos, cinco percursos de leitura. Siga a decisão que corresponde à sua função preservando sempre a fronteira entre registos verificados e alegações clandestinas.

Administração e direção executiva	Dimensionar a exposição nacional, o aumento do ransomware e a urgência regulatória	01 02 10 11
CISO e operações de segurança	Priorizar validação de credenciais, aplicação de DMARC, isolamento de fornecedores e correções	03 05 07 12
Fraude, banca e identidade digital	Combater spoofing SMS/voz, malware CMD, mulas KYC e abuso de referências Multibanco	04 08 09
Setor público e resiliência OT	Separar paragens reais de alegações e proteger TI municipais e controladores OT remotos	05 06 12
Jurídico, privacidade e conformidade	Alinhar prazos e evidências de MyCiber (NIS2), DORA, CNPD (RGPD) e CRA	05 10 A

CAPÍTULO 02

Perfil digital nacional e panorama de 2026

02

ESTE CAPÍTULO RESPONDE

Como moldam a pegada digital, os dados oficiais e o volume bruto o risco de Portugal em 2026?

89,0%

penetração da Internet numa população de 10,4 milhões à entrada de 2026

2.1 Elevada adoção digital e infraestruturas nacionais partilhadas 11

2.2 Ritmo oficial das ameaças em Portugal de 2024 a 2026 11

2.3 Interpretar o volume clandestino associado a Portugal 13

CAPÍTULO 02

Perfil digital nacional e panorama de 2026

EM RESUMO

Portugal entrou em 2026 com 9,26 milhões de utilizadores de Internet (89,0%) e serviços nacionais partilhados como a Chave Móvel Digital, o SNS 24 e a rede SIBS. No RASI 2025, incidentes não automáticos no CERT.PT subiram 40% para 3 864 (61 798 no total). O ransomware cresceu 71% para 60 e a exploração de falhas subiu 162%. As publicações somaram 744 809 até 26 de novembro, das quais 97,7% em janeiro-fevereiro, sobretudo spam em turco. Separe ruído massivo da atividade de março a novembro antes de alocar analistas.

2.1 Elevada adoção digital e infraestruturas nacionais partilhadas

O relatório Digital 2026: Portugal da DataReportal contabiliza **9,26 milhões de utilizadores de Internet** no final de 2025 [S20]. Este valor equivale a **89,0%** de penetração numa população estimada de **10,4 milhões** em outubro de 2025 [S20]. As ligações móveis celulares ativas atingiram **13,9 milhões** (equivalente a **133%** da população) e as identidades em redes sociais somaram **7,59 milhões** (**72,9%**) em outubro de 2025 [S20].

A economia quotidiana em Portugal depende de infraestruturas digitais fortemente partilhadas. Os cidadãos autenticam-se em serviços públicos e privados através da **Chave Móvel Digital (CMD)** e interagem com portais fiscais (`Portal das Finanças`), de saúde (`SNS 24`), mobilidade (`IMT`) e autarquias [S39][S74][S81]. Os pagamentos de retalho e faturas assentam na rede doméstica **SIBS**, incluindo referências **Multibanco** e transferências instantâneas **MB WAY**, a par da confirmação de beneficiário e do serviço **SPIN** do **Banco de Portugal** [S12][S13].

Esta concentração traz conveniência e forte segurança nos pagamentos de retalho, mas amplia dependências sistémicas. Quando falha uma plataforma nacional partilhada, uma solução municipal comum ou um único subcontratado externo, a perturbação e o phishing secundário atingem rapidamente dezenas de milhares de residentes [S39][S58][S62]. A interligação elétrica com Espanha evidenciou também a interdependência física durante o apagão ibérico de **28 de abril de 2025** [S16][S17]. O relatório técnico da **ENTSO-E**, validado pela **ACER** e apresentado a 20 de março de 2026, atribui o apagão a múltiplos fatores técnicos, incluindo controlo de tensão insuficiente, com início no sistema espanhol [S16][S17]. As fontes oficiais citadas não identificam causa cibernética [S16][S17].

2.2 Ritmo oficial das ameaças em Portugal de 2024 a 2026

Os relatórios oficiais portugueses documentam uma subida sustentada no volume e na sofisticação técnica dos incidentes à entrada de 2026. Na 6.ª edição de Riscos & Conflitos do CNCS (sobre 2024), o **CERT.PT** validou **2 758 incidentes** (**+36%** homólogo; **11 163** com deteções automáticas), sendo **78%** no setor privado [S6][S7].

O **Relatório Anual de Segurança Interna (RASI) 2025**, publicado pelo Governo de Portugal em 2026, evidencia nova escalada transversal nas entidades oficiais [S5]. A base de 2024 implícita no RASI (**2 761**) difere ligeiramente do valor do Riscos & Conflitos (**2 758**) [S5][S6]:

Indicador oficial português (2025 face a 2024)	Valor oficial 2025	Tendência homóloga	Fonte
Total de incidentes no CERT.PT (incl. feeds automáticos)	61 798	+50 635 (impulsionado por feeds automáticos de infostealers)	RASI 2025 / CNCS [S5]
Incidentes não automáticos no CERT.PT (de 8 891 notificações)	3 864	+40% (+1 103 incidentes; notificações +75%)	RASI 2025 / CNCS [S5]
Incidentes de ransomware no CERT.PT	60	+71% (incl. Akira, MAKOP, Qilin, INC Ransom)	RASI 2025 / CNCS [S5]
Exploração de vulnerabilidades no CERT.PT	118 (46 CVE)	+162% (CVSS mediano Crítico; SharePoint e DNN no topo)	RASI 2025 / CNCS [S5]
Crescimento de phishing e DDoS não automáticos no CERT.PT	Phishing +93% / DDoS +36%	Energia juntou-se a Banca, ISP, Saúde e Admin. Pública	RASI 2025 / CNCS [S5]
Crimes informáticos registados pela DGPJ (`participações`)	2 826	+13,4% (+334; falsidade informática +29,1%; acesso ilegítimo +8,4%)	RASI 2025 / DGPJ [S5]
Suspeitos constituídos / detidos pela Polícia Judiciária	2 559 / 83	Suspeitos +28,5% / detidos +88,6%	RASI 2025 / PJ [S5]
Denúncias por correio eletrónico ao Gabinete de Cibercrime	Total anual	+13,16% homólogo (subida contínua desde 2016)	MP [S8]
Processos de violação de dados pessoais abertos na CNPD	472	+42% (face a 332 em 2024; 375 entidades privadas e 115 públicas reportadas nos 472 processos; 27% erro humano)	CNPD [S9][S10][S11]

Os infostealers dominaram as deteções automáticas do CERT.PT em 2025, com o furto de contas não privilegiadas a atingir **47 953 incidentes** (**78%** dos 61 798 casos registados) [S5]. O **Lumma** isoladamente correspondeu a **25 430 incidentes** (**59%** dos casos ligados a malware), a par do emergente **Acreed** (**6%**) e das ameaças Android **BadBox2.0** e **ToxicPanda** [S5].

Excluindo feeds automáticos, os reportes de terceiros foram liderados por engenharia social (**1 054** casos), código malicioso (**931**, subida de **224%**) e fraude (**806**, **82%** phishing) [S5]. Na engenharia social, o CERT.PT registou **192** casos de Fraude ao CEO, **118** falsas ofertas de emprego, **99** burlas "Olá Pai / Olá Mãe" e **85** casos de vishing [S5].

No início de 2026, as instituições portuguesas reforçaram também a monitorização de integridade informativa antes das **eleições presidenciais de janeiro-fevereiro de 2026**. A **Comissão Nacional de Eleições (CNE)** abriu um canal público de denúncia de desinformação [S18]. Um estudo conjunto da **ERC** e do **LabCom-UBI**, abrangendo o período de 17 de novembro de 2025 a 8 de fevereiro de 2026, analisou **8 047** publicações oficiais de candidaturas nas redes sociais [S19]. O estudo registou **26** casos de desinformação (**7** com material gerado ou alterado por IA) e estimou mais de **12,8 milhões** de visualizações; a **ERC** abriu **8** processos regulatórios [S19].

2.3 Interpretar o volume clandestino associado a Portugal

Entre **1 de janeiro e 26 de novembro de 2026**, a Odin by Brandefense registou **744 809 publicações clandestinas com etiqueta Portugal** [S1]. Ler este total bruto sem contexto mensal e linguístico distorceria gravemente a avaliação de risco nacional.

Publicações clandestinas mensais com etiqueta Portugal de janeiro a novembro de 2026

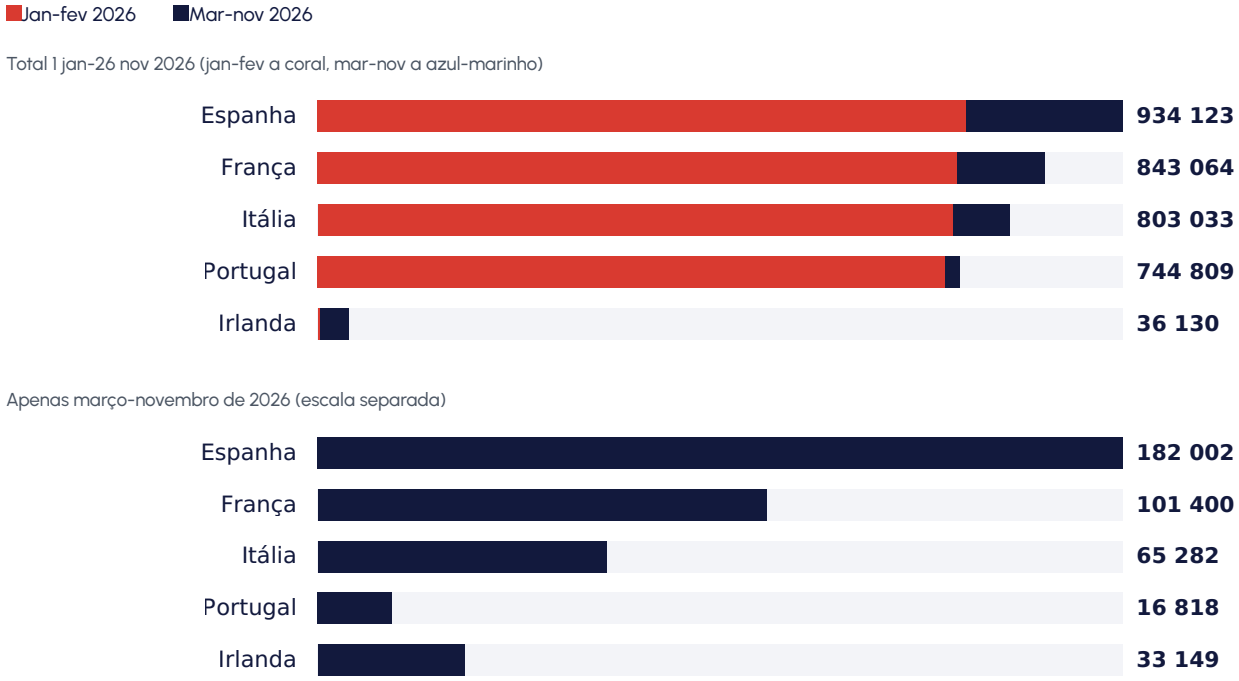


Fonte: Odin by Brandefense, publicações clandestinas com etiqueta Portugal, 1 de janeiro-26 de novembro de 2026; novembro parcial [S1]. As publicações não são incidentes confirmados; as etiquetas de idioma podem sobrepor-se.

Mês (2026)	Publicações com etiqueta Portugal	Peso na janela	Padrão operacional
Janeiro	411 861	55,3%	Vaga multipaís de bots promocionais em turco no Telegram (409 800 TR)
Fevereiro	316 130	42,4%	Continuação da mesma vaga promocional em turco no Telegram (314 145 TR)
Março	2 068	0,3%	Regresso à base; carding, contas financeiras e 25 tópicos de fórum
Abril	2 269	0,3%	Pico de fóruns (26 tópicos); anúncios-modelo de retalho e combolists
Maio	1 484	0,2%	Anúncio alegado de Domain Admin; extratos stealer; 7 tópicos de fórum
Junho	1 664	0,2%	Publicação alegada de VPN autárquica; atualizações de lotes de cartões
Julho	1 780	0,2%	Subida estival de ransomware; anúncios de carding e KYC/documentos
Agosto	1 558	0,2%	Subida de tráfego no Telegram em espanhol (204) e em russo (194)
Setembro	1 637	0,2%	Republicações repetidas de dados aéreos; crescimento de contas OTC
Outubro	2 625	0,4%	Pico pós-fevereiro impulsionado por canais OTC em russo (960 RU)
Novembro (até 26 nov)	1 733	0,2%	715 publicações na janela recente de 12-26 nov; 785 RU; 7 fóruns
Total (1 jan-26 nov)	**744 809**	**100,0%**	**727 991 (97,7%) em jan-fev; 16 818 (2,3%) em mar-nov**

Das **727 991** publicações de janeiro e fevereiro, **723 945** (**99,4%**) estavam em turco, o que é compatível com bots promocionais automáticos em grupos multipaís [S1]. O mesmo pico de janeiro-fevereiro surge em **Espanha** (`424 494` jan; `327 627` fev), **França** (`419 017` ; `322 647`) e **Itália** (`415 967` ; `321 784`) [S1]. Já a **Irlanda** (`1 531` ; `1 450`) ficou fora dessa vaga de bots [S1].

Volume mensal clandestino comparando Portugal com Espanha, França, Itália e Irlanda

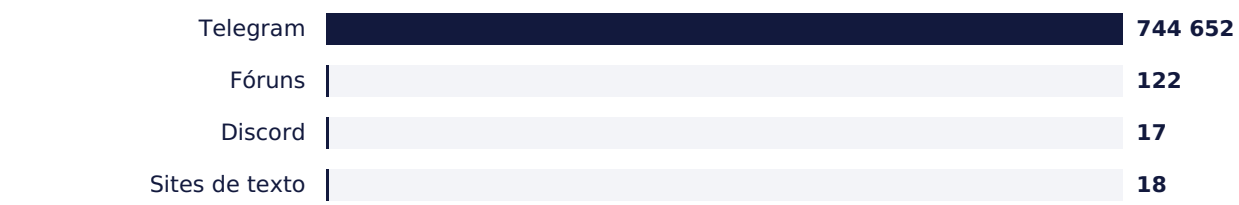


Publicações brutas com etiqueta de país nos canais monitorizados; não ajustadas à população nem à cobertura de fontes. Fonte: Odin by Brandefense, publicações clandestinas com etiqueta Portugal, 1 de janeiro-26 de novembro de 2026; novembro parcial [S1]. As publicações não são incidentes confirmados; as etiquetas de idioma podem sobrepor-se.

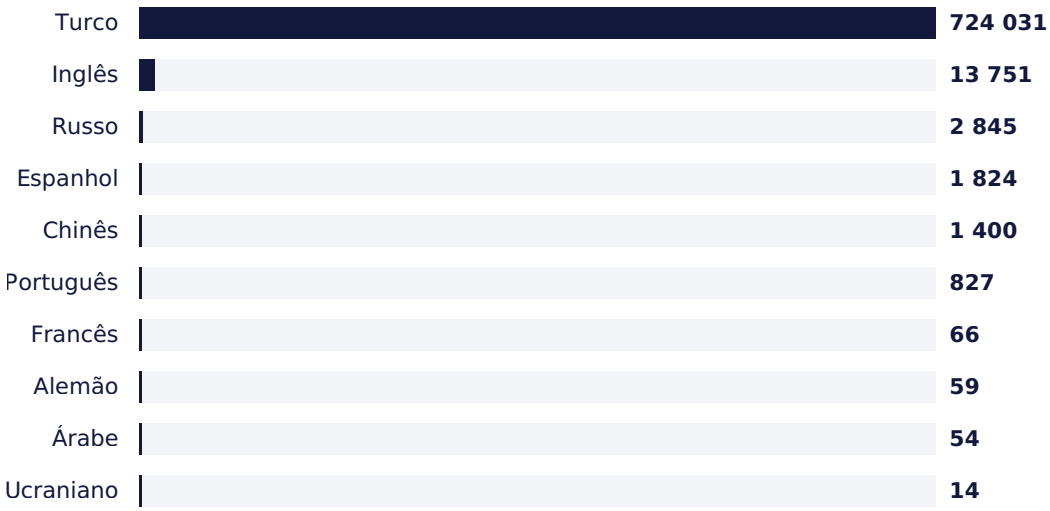
Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

Na base de **março a novembro** (`16 818` publicações), o volume mensal de Portugal correspondeu a cerca de metade da **Irlanda** (`33 149`) e a um quarto de **Itália** (`65 282`) [S1]. Situou-se igualmente em cerca de um sexto de **França** (`101 400`) e abaixo de um décimo de **Espanha** (`182 002`) [S1]. Em toda a janela, o **Telegram** concentrou **744 652** publicações (`99,98%`), os **fóruns 122**, os **sites de texto 18** e o **Discord 17** (`0` na rede Tor) [S1]. Excluindo a vaga massiva em turco, lideraram o **inglês** (`13 751`), o **russo** (`2 845`), o **espanhol** (`1 824`), o **chinês** (`1 400`) e o **português** (`827`) [S1].

Distribuição por plataforma e idioma das publicações clandestinas com etiqueta Portugal



Idioma



Fonte: Odin by Brandefense, publicações clandestinas com etiqueta Portugal, 1 de janeiro-26 de novembro de 2026; novembro parcial [S1]. As publicações não são incidentes confirmados; as etiquetas de idioma podem sobrepor-se.

Uma alteração outonal merece atenção operacional: o tráfego em língua russa com etiqueta Portugal saltou de `90-194` publicações mensais entre janeiro e setembro para **960** em outubro e **785** em novembro até dia 26 [S1]. As publicações analisadas nessa subida provinham sobretudo de canais OTC em russo no Telegram que anunciam contas financeiras europeias e portuguesas, mulas KYC e reposições de lojas de cartões [S1].

PRINCIPAIS CONCLUSÕES

01

A elevada dependência de infraestruturas nacionais partilhadas (CMD, SNS 24, Multibanco, MB WAY) amplia incidentes de fornecedores e credenciais em Portugal.

02

Os incidentes não automáticos no CERT.PT subiram 40% em 2025, com o ransomware a subir 71% e a exploração de falhas 162%.

03

Janeiro e fevereiro representaram 97,7% do volume bruto, sobretudo bots promocionais multipaís no Telegram; março a novembro revela o ritmo operacional real.

CAPÍTULO 03

Exposição nacional e observações sobre domínios selecionados

ESTE CAPÍTULO RESPONDE

Que sinais de exposição e lacunas de configuração exigem validação em 250 domínios portugueses?

83 de 247

domínios avaliados apresentavam uma credencial à venda na verificação

3.1 Ficha da carteira e limites de avaliação 18

3.2 Indicador nacional Atlas e anúncios ativos de credenciais 19

3.3 Associações a dispositivos infetados e registos históricos de credenciais 21

3.4 Documentos, nomes de domínio semelhantes e menções a 365 dias 24

3.5 Autenticação de correio, DNSSEC, TLS e HSTS nos 250 domínios portugueses 24

3.6 Converter sinais de exposição em filas separadas de validação 27

CAPÍTULO 03

Exposição nacional e observações sobre domínios selecionados

EM RESUMO

Em 27 de novembro de 2026, 83 de 247 domínios portugueses avaliados (33,6%) tinham credenciais à venda na verificação. O indicador nacional Atlas é de 51/100. Os sinais históricos abrangem 235 domínios com dispositivos (pelo menos 523 733 no total; 38 013 de colaboradores) e 238 com 13 777 936 registos de credenciais. Nos 250 domínios, 163 (65,2%) aplicam DMARC restritivo e 87 (34,8%) não. Valide primeiro os 83 anúncios ativos, imponha DMARC nos 87 domínios restantes e corrija 20 falhas TLS.

3.1 Ficha da carteira e limites de avaliação

Reunimos uma carteira intencional de **250 domínios portugueses verificados em DNS**, distribuídos por dez células setoriais iguais de 25 domínios cada [S3][S4]. As identidades individuais dos domínios permanecem privadas para evitar expor observações não confirmadas.

Elemento	Âmbito
Datas de referência	Janela de atividade de 1 de janeiro a 26 de novembro de 2026; menções de 365 dias de 27 de novembro de 2025 a 26 de novembro de 2026; retratos de exposição e configuração em 27 de novembro de 2026; fontes externas verificadas em 27 de novembro de 2026
Carteira	250 domínios portugueses selecionados em 10 células iguais de 25 domínios (130 privados, 63 empresas públicas ou administração central, 57 autarquias, saúde e ensino público)
Seleção	Carteira intencional englobando ministérios, agências, municípios, universidades, hospitais, bancos supervisionados, seguradoras, energia, telecomunicações, transportes, indústria e retalho; não constitui censo nacional
Unidade	Um domínio principal por organização; todos os 250 resolviam em DNS em 27 de novembro de 2026 [S3]
Retrato de exposição	247 de 250 domínios avaliados em 27 de novembro de 2026; 3 domínios permanecem desconhecidos (1 em energia e serviços públicos, 1 em indústria e manufatura, 1 em transportes, marítimo e logística) [S4]
Sinais de exposição	Associações acumuladas de dispositivos infetados e de colaboradores, registos históricos de credenciais, anúncios ativos de credenciais, histórico de anúncios, documentos expostos e nomes semelhantes a 30 dias [S4]

Elemento	Âmbito
Contexto de menções	Menções clandestinas a 365 dias em chats e fontes da dark web nos 250 domínios (27 de novembro de 2025 a 26 de novembro de 2026), com o subconjunto de 1 de janeiro a 26 de novembro de 2026 separado [S4]
Retrato passivo	Observações públicas de DNS, DMARC, SPF, DKIM, DNSSEC, CAA, TLS e HSTS nos 250 domínios em 27 de novembro de 2026 [S3]
Limite de publicação	Apenas o indicador nacional Atlas (51/100); não são publicadas classificações setoriais, por grupo ou por organização [S4]
Limite de inferência	Os sinais podem sobrepor-se entre domínios e indivíduos; observações em falta nunca são tratadas como zero e nenhuma contagem isolada estabelece uma intrusão confirmada

As observações de exposição e as configurações passivas medem riscos distintos. Os registos históricos de credenciais refletem frequentemente contas de consumidores ou antigos estudantes, e não uma intrusão interna. Por sua vez, uma política DMARC restritiva reduz a falsificação direta de domínio sem impedir a reutilização de sessões furtadas. Mantenha cada métrica ligada ao respetivo denominador (**247** domínios avaliados na exposição; **250** domínios na configuração e nas menções).

3.2 Indicador nacional Atlas e anúncios ativos de credenciais

Na verificação de 27 de novembro de 2026, **83 de 247 domínios portugueses avaliados (33,6%)** apresentavam uma credencial associada à venda [S4]. Todos os 83 apresentam também histórico anterior, totalizando **2 621 registos históricos de anúncios** na carteira avaliada [S4].

O indicador nacional Atlas da carteira avaliada é de 51/100 [S4]. Valores mais elevados na escala de 0 a 100 refletem maior exposição externa observada nos domínios avaliados. Apenas este valor nacional único é publicado. Não constam neste relatório classificações por setor, por grupo nem pontuações individuais de organizações.

Este valor nacional apoia a priorização global da carteira. Não representa uma taxa de intrusão, uma probabilidade de ataque futuro nem um censo da economia portuguesa. Os três domínios não avaliados permanecem desconhecidos e nunca zero.

Anúncios ativos de credenciais e sinais de exposição nos 247 domínios portugueses avaliados

	Anúncios ativos	Com dispositivos	Disp. de colaboradores	Com credenciais	Com documentos	Nomes sem. (30 dias)
Administração pública	7/25	23/25	17/25	24/25	14/25	21/25
Administração regional e local	2/25	25/25	21/25	24/25	16/25	25/25
Banca e finanças	13/25	24/25	21/25	25/25	15/25	23/25
Energia e serviços públicos	6/24	22/24	17/24	23/24	8/24	15/24
Telecomunicações e serviços digitais	9/25	24/25	21/25	25/25	13/25	19/25
Indústria e manufatura	2/24	21/24	21/24	24/24	14/24	13/24
Transportes, marítimo e logística	8/24	23/24	20/24	23/24	12/24	15/24
Saúde e ciências da vida	5/25	24/25	16/25	20/25	8/25	16/25
Educação e investigação	12/25	25/25	25/25	25/25	21/25	20/25
Retalho, media e serviços ao consumidor	19/25	24/25	23/25	25/25	16/25	24/25

Anúncios ativos de credenciais por setor (coral). Cada célula mostra domínios observados / domínios avaliados (24 ou 25); os sinais podem sobrepor-se. Fonte: observações de exposição da Brandefense para 247 domínios avaliados de 250 domínios portugueses selecionados, retrato de 27 de novembro de 2026 (3 domínios permanecem desconhecidos) [S4]. As associações acumuladas podem sobrepor-se; não representam pessoas únicas nem intrusões confirmadas.

Célula setorial	Avaliados (de 25)	Anúncios ativos	Com dispositivos	Com dispositivos de colaboradores	Com credenciais	Com documentos	Com nomes semelhantes (30d)
Administração pública	25	7	23	17	24	14	21
Administração regional e local	25	2	25	21	24	16	25
Banca e finanças	25	13	24	21	25	15	23
Energia e serviços públicos	24	6	22	17	23	8	15
Telecomunicações e serviços digitais	25	9	24	21	25	13	19
Indústria e manufatura	24	2	21	21	24	14	13

Célula setorial	Avaliados (de 25)	Anúncios ativos	Com dispositivos	Com dispositivos de colaboradores	Com credenciais	Com documentos	Com nomes semelhantes (30d)
Transportes, marítimo e logística	24	8	23	20	23	12	15
Saúde e ciências da vida	25	5	24	16	20	8	16
Educação e investigação	25	12	25	25	25	21	20
Retalho, media e serviços ao consumidor	25	19	24	23	25	16	24
Total avaliado	**247**	**83**	**235**	**202**	**238**	**137**	**191**

Os anúncios ativos de credenciais concentram-se nas células de retalho, banca e ensino superior. **Retalho, media e serviços ao consumidor** registou **19** domínios com anúncios ativos, **Banca e finanças 13**, **Educação e investigação 12**, **Telecomunicações e serviços digitais 9** e **Transportes, marítimo e logística 8** [S4]. **Administração pública (7)**, **Energia e serviços públicos (6)** e **Saúde e ciências da vida (5)** mostram igualmente exposição ativa [S4]. **Administração regional e local (2)** e **Indústria e manufatura (2)** registam menos anúncios ativos apesar da ampla presença histórica [S4].

3.3 Associações a dispositivos infetados e registos históricos de credenciais

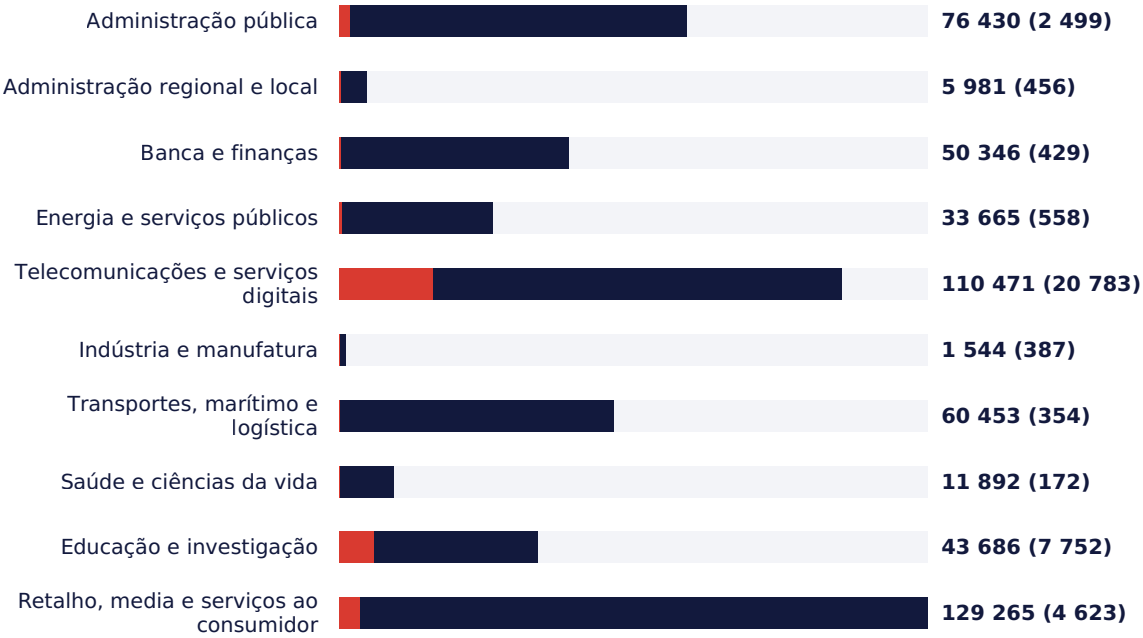
Nos **247 domínios avaliados**, **235 domínios (95,1%)** apresentaram associações acumuladas a dispositivos infetados, totalizando **pelo menos 523 733** registos [S4]. Os totais de dispositivos são valores mínimos e não totais exatos [S4]. Dentro desse total, **202 domínios (81,8%)** apresentaram **38 013 associações a dispositivos de colaboradores**, enquanto **485 720** refletiram outros dispositivos ou equipamentos de clientes [S4].

Associações históricas de credenciais surgiram em **238 de 247 domínios avaliados (96,4%)**, somando **13 777 936 registos** [S4]. Este total divide-se em **6 414 548** combolists, **4 898 461** bases de fugas e **2 464 927** registos de infostealers [S4]. A exposição concentra-se fortemente em portais de correio web, telecomunicações e retalho de massas. **Telecomunicações e serviços digitais** representa **10 154 007** registos **(73,7%)** e **Retalho, media e serviços ao consumidor 2 050 002 (14,9%)** [S4]. Os dois maiores domínios isoladamente concentram **86,7%** de todos os registos de credenciais observados [S4].

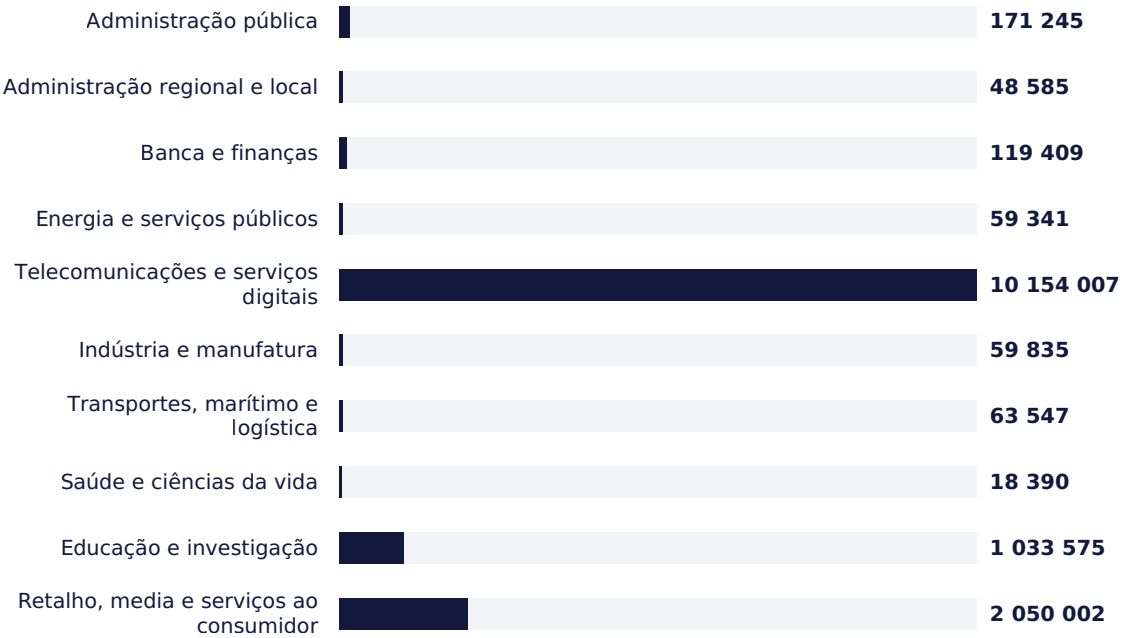
Observações acumuladas de dispositivos, credenciais, documentos e nomes semelhantes por setor nos 247 domínios avaliados

Associações de dispositivos de colaboradores Outras associações de dispositivos

Associações de dispositivos, mínimo (colaboradores entre parênteses)



Associações de registos de credenciais (escala separada)



Fonte: observações de exposição da Brandefense para 247 domínios avaliados de 250 domínios portugueses selecionados, retrato de 27 de novembro de 2026 (3 domínios permanecem desconhecidos) [S4]. As associações acumuladas podem sobrepor-se; não representam pessoas únicas nem intrusões confirmadas.

Célula setorial	Avaliados	Dispositivos (mín.)	Dispositivos de colaboradores	Total credenciais	Bases de fugas	Stealer	Combolist	Documentos	Nomes semelhantes (30d)
Administração pública	25	76 430	2 499	171 245	28 296	61 028	81 921	93	5 032

Célula setorial	Avaliados	Dispositivos (mín.)	Dispositivos de colaboradores	Total credenciais	Bases de fugas	Stealer	Combolist	Documentos	Nomes semelhantes (30d)
Administração regional e local	25	5 981	456	48 585	12 333	15 347	20 905	29	13 935
Banca e finanças	25	50 346	429	119 409	63 836	9 294	46 279	53	2 374
Energia e serviços públicos	24	33 665	558	59 341	24 926	9 986	24 429	34	772
Telecomunicações e serviços digitais	25	110 471	20 783	10 154 007	3 518 551	1 821 600	4 813 856	314	8 363
Indústria e manufatura	24	1 544	387	59 835	31 660	6 850	21 325	29	66
Transportes, marítimo e logística	24	60 453	354	63 547	26 291	11 669	25 587	48	2 467
Saúde e ciências da vida	25	11 892	172	18 390	8 995	3 624	5 771	12	886
Educação e investigação	25	43 686	7 752	1 033 575	103 535	430 052	499 988	98	4 092
Retalho, media e serviços ao consumidor	25	129 265	4 623	2 050 002	1 080 038	95 477	874 487	91	2 073
Total avaliado	**247**	**523 733**	**38 013**	**13 777 936**	**4 898 461**	**2 464 927**	**6 414 548**	**801**	**40 060**

A coluna de dispositivos de colaboradores merece prioridade imediata. Todos os 25 domínios universitários e de investigação avaliados apresentaram dispositivos de colaboradores (**7 752**) e **430 052** registos de infostealers, o que é compatível com redes académicas abertas de equipamento próprio [S4]. A Administração pública registou **2 499** associações de dispositivos de colaboradores em **17** domínios e **61 028** registos de infostealers, reforçando a conclusão do CERT.PT de que os infostealers lideram as deteções nacionais [S4][S5].

3.4 Documentos, nomes de domínio semelhantes e menções a 365 dias

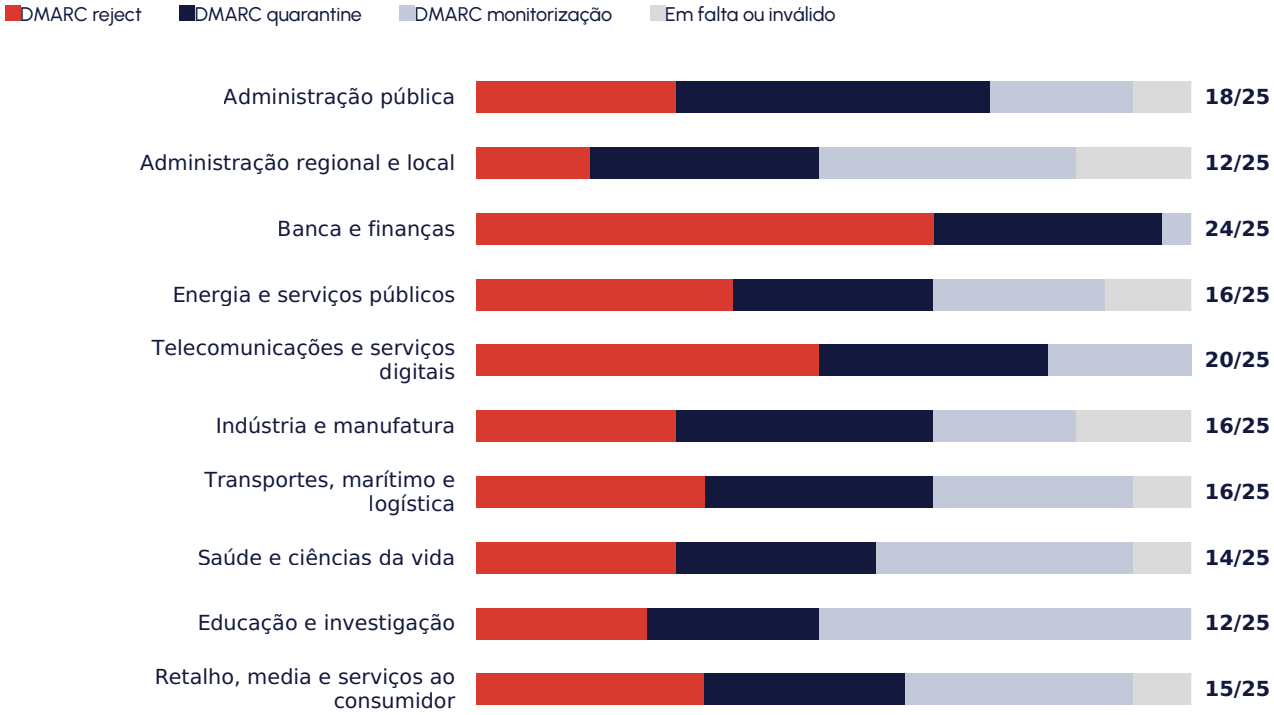
Documentos expostos surgiram em **137 de 247 domínios (55,5%)**, somando **801 documentos** [S4]. Lideram **Telecomunicações** (`314`), **Educação** (`98`), **Administração pública** (`93`) e **Retalho e consumo** (`91`) [S4]. Nomes semelhantes a 30 dias cobriram **191 de 247 domínios (77,3%)**, somando **40 060** nomes [S4]. Os volumes mais altos surgiram em **Administração regional e local** (`13 935`), **Telecomunicações** (`8 363`) e **Administração pública** (`5 032`) [S4]. Como nomes semelhantes incluem registos benignos ou coincidentes, os defensores devem filtrar primeiro por registos MX ou certificados TLS recentes.

Em todos os **250 domínios** na janela móvel de 365 dias (**27 de novembro de 2025 a 26 de novembro de 2026**), **58 domínios (23,2%)** surgiram em menções clandestinas [S4]. Concretamente, **39 domínios** apareceram em canais de chat (`363` menções) e **31 domínios** em fontes da dark web (`244` menções) [S4]. Restringindo à janela de atividade de **1 de janeiro a 26 de novembro de 2026**, **27 de 250 domínios (10,8%)** registaram **212** menções diretas [S4].

3.5 Autenticação de correio, DNSSEC, TLS e HSTS nos 250 domínios portugueses

As observações de configuração pública em **27 de novembro de 2026** abrangeram todos os **250 domínios selecionados** [S3]. No conjunto, **163 de 250 domínios (65,2%)** aplicam DMARC restritivo (**84** `reject` e **79** `quarantine`) [S3][S82]. Outros **87 domínios (34,8%)** ficam sem política restritiva (**68** em `p=none` e **19** em falta ou inválidos) [S3].

Distribuição de políticas DMARC nos 250 domínios portugueses selecionados



Os valores à direita mostram políticas restritivas (reject ou quarantine) / 25 domínios selecionados por setor. Fonte: observações de configuração passiva para 250 domínios portugueses selecionados, retrato de 27 de novembro de 2026 [S3]. As políticas publicadas não comprovam aplicação ao nível da mensagem nem impedimento de falsificação.

Célula setorial (25 domínios cada)	DMARC reject	DMARC quarantine	DMARC none	Em falta/ inválido	SPF	DKIM	DNSSEC	TLS válido	HSTS (dos acessíveis)
Administração pública	7	11	5	2	25	17	14	17/23	13/20
Administração regional e local	4	8	9	4	21	19	5	23/25	18/21
Banca e finanças	16	8	1	0	23	14	7	22/23	21/22
Energia e serviços públicos	9	7	6	3	24	21	12	23/24	20/23
Telecomunicações e serviços digitais	12	8	5	0	25	21	8	23/23	17/20

Célula setorial (25 domínios cada)	DMARC reject	DMARC quarantine	DMARC none	Em falta/ inválido	SPF	DKIM	DNSSEC	TLS válido	HSTS (dos acessíveis)
Indústria e manufatura	7	9	5	4	24	23	5	22/24	15/22
Transportes, marítimo e logística	8	8	7	2	23	21	10	23/25	17/22
Saúde e ciências da vida	7	7	9	2	24	18	4	21/22	16/24
Educação e investigação	6	6	13	0	25	20	17	20/23	14/21
Retalho, media e serviços ao consumidor	8	7	8	2	25	22	2	23/25	13/17
Total (250 domínios)	**84**	**79**	**68**	**19**	**239**	**196**	**84**	**217/237**	**164/212**

As assimetrias setoriais são nítidas e acionáveis de imediato [S3]:

- **A banca e finanças lidera a proteção de correio e transporte.** Vinte e quatro de 25 domínios financeiros (**96,0%**) aplicam DMARC (**16** `reject`, **8** `quarantine`), e **21 de 22** serviços web acessíveis (**95,5%**) publicam HSTS [S3][S82][S85].
- **Municípios, universidades e saúde apresentam atraso acentuado no DMARC.** Apenas **12 de 25** domínios (**48,0%**) aplicam DMARC na **Administração regional e local** (`9` `p=none`, `4` em falta) e **12 de 25** (**48,0%**) em **Educação e investigação** (`13` `p=none`) [S3]. **Saúde e ciências da vida** segue logo atrás com **14 de 25** (**56,0%**) [S3]. Estes três setores foram apontados no RASI 2025 como sujeitos a forte pressão de phishing e ransomware em 2025 [S5].
- **A segurança de transporte e a assinatura DNS deixam lacunas evitáveis.** Nos 250 domínios, **239 (95,6%)** publicam SPF e **196 (78,4%)** têm registo DKIM identificado, mas apenas **84 (33,6%)** publicam registos DS de DNSSEC e **34 (13,6%)** registos CAA [S3][S83][S84]. De **237** serviços TLS acessíveis no domínio raiz, **217** validaram sem falhas e **20** falharam (**10** cadeias intermédias em falta, **8** divergências de nome e **2** certificados expirados; **13** ficaram inacessíveis) [S3]. Em **212** serviços HTTP acessíveis, **164 (77,4%)** ativam HSTS (**38** indisponíveis) [S3][S85].

- **O alojamento de correio concentra-se em plataformas cloud.** Metade da carteira (**126 de 250**, **50,4%**) encaminha correio de entrada através do Microsoft 365, **12** através do Google Workspace e **13** não publicam registos MX [S3]. A plataforma **Tycoon 2FA**, desmantelada em **março de 2026**, atingiu mais de **160 organizações em Portugal** visando precisamente sessões MFA deste tipo de correio cloud [S29].

3.6 Converter sinais de exposição em filas separadas de validação

As equipas defensivas devem dividir os sinais externos em três filas operacionais distintas em vez de os misturar numa única caixa de entrada:

1. **Fila imediata de identidade:** Valide os **83 domínios** com anúncios ativos de credenciais e os **202 domínios** com dispositivos de colaboradores, revogando sessões ativas e isolando postos infetados [S4].
2. **Fila de falsificação de domínio:** Migre os **87 domínios sem DMARC restritivo** para DMARC `quarantine` ou `reject`, vigie nomes semelhantes com MX ou TLS novos e corrija as **20** falhas TLS [S3][S82].
3. **Fila de higiene de exposição pública:** Reveja as **801** associações a documentos para detetar carregamentos públicos acidentais e audite a exposição histórica de fugas (`238` domínios) para impor redefinição de palavras-passe reutilizadas [S4].

PRINCIPAIS CONCLUSÕES

01

O indicador nacional Atlas é de 51/100 nos 247 domínios avaliados (27 de novembro de 2026), com 83 domínios (33,6%) em anúncios ativos de credenciais.

02

A banca aplica DMARC em 24 de 25 domínios, enquanto autarquias e educação ficam em 12 de 25 cada.

03

A concentração em correio cloud (126 de 250 no Microsoft 365) torna essencial a MFA resistente a phishing em Portugal.

CAPÍTULO 04

Alegações e casos clandestinos

04

ESTE CAPÍTULO RESPONDE

O que anunciam, procuram e reciclam os atores de ameaça em torno de Portugal?

7

casos documentados de alegações e procura clandestina (15 publicações redigidas)

4.1 Como ler alegações clandestinas 29

4.2 Anúncios-modelo de retalho e reciclagem de bases históricas 29

4.3 Credenciais, portais públicos e ofertas alegadas de acesso inicial 32

4.4 Contactos bancários, procura de mulas KYC e abuso de canais de pagamento 35

CAPÍTULO 04

Alegações e casos clandestinos

EM RESUMO

Fóruns clandestinos e canais do Telegram dirigidos a Portugal em 2026 revelam quatro padrões principais. Vendedores publicaram anúncios-modelo de retalho, reciclaram uma base aérea histórica como "2026" e partilharam combolists mensais a par de alegados acessos Domain Admin e VPN. Compradores procuraram também mulas KYC portuguesas, contas bancárias de receção e rotas SMS falsificadas. Todos os sete casos omitem identidades de vítimas não confirmadas. Valide sempre os esquemas e datas face a arquivos históricos antes de tratar um anúncio como nova intrusão.

4.1 Como ler alegações clandestinas

Uma publicação clandestina estabelece um facto com elevada confiança: uma conta publicou aquele texto naquela data e naquele espaço [S1]. Não estabelece, porém, intrusão em servidor, recolha recente, autenticidade dos registos, acesso ativo nem transferência financeira concluída. Nos sete casos seguintes (`Caso A` a `Caso G`), omitem-se nomes de vítimas não confirmadas, domínios, dados pessoais, hashes e credenciais.

4.2 Anúncios-modelo de retalho e reciclagem de bases históricas

A

CASO A

Anúncios-modelo de três secções atribuídos a marcas portuguesas de retalho e informação empresarial

Sem verificação

Retalho e dados empresariais

ALEGAÇÃO	Em 4 de janeiro de 2026 (`B01`), um vendedor de fórum anunciou uma alegada base de 284 000 linhas de clientes, subscrições e pedidos de suporte atribuída a uma operadora portuguesa de telecomunicações [S1]. Em 3 de abril de 2026 (`B02`), a mesma conta publicou três anúncios seguidos em seis minutos [S1]. Cada anúncio alegava mais de 400 000 linhas em duas marcas portuguesas de retalho e num portal de informação empresarial [S1]. Todas as publicações repetiam o texto-modelo descrevendo os dados como "fresh and organized across 3 main sections" [S1].
O QUE NÃO ESTÁ ESTABELECIDO	Não existia confirmação oficial de intrusão até à data de corte para nenhum destes anúncios. Redação idêntica publicada com minutos de diferença sugere fortemente ficheiros extraídos, sintéticos ou reempacotados.

RESPOSTA

Os responsáveis de dados alertados para anúncios-modelo devem comparar cabeçalhos e amostras com os esquemas reais de CRM e loja online antes de emitir notificações.

Conclusão

Compare os esquemas anunciados com as exportações reais de CRM e loja online antes de emitir alertas a clientes.

Ficha de evidência B01 — 4 jan 2026

Utilizador de fórum (alcunha omitida) · Tópico de fórum · Fórum · Inglês

ORIGINAL

Offering a dataset originating from [operador português de telecomunicações]. It provides a detailed look at the organization's operations, including Customers, Service subscriptions, Support tickets. The data is fresh and organized across 3 main sections.

Nota. O operador mencionado é omitido por inexistência de confirmação oficial; a mesma redação reaparece a 3 de abril.

Observado

Um vendedor em fórum anuncia uma alegada base de 284 000 registos de clientes e pedidos de suporte atribuída a um operador português de telecomunicações.

Não estabelecido

Intrusão em sistemas, autenticidade dos registos, recolha recente em 2026, número de clientes afetados ou venda concretizada.

Ficha de evidência B02 — 3 abr 2026

Utilizador de fórum (alcunha omitida) · Tópico de fórum · Fórum · Inglês

ORIGINAL

Offering a dataset originating from [marca portuguesa de retalho]. It provides a detailed look at the organization's operations, including Contacts, Orders, Delivery Logs. The data is fresh and organized across 3 main sections.

Nota. A redação padronizada repetida em marcas portuguesas distintas constitui forte indício de listagens recicladas ou sintéticas.

Observado

Num intervalo de seis minutos a 3 de abril, a mesma conta publica três anúncios idênticos em três secções reivindicando mais de 400 mil registos cada em dois retalhistas e um diretório empresarial em Portugal.

Não estabelecido

Acesso aos sistemas de origem, autenticidade dos dados ou extração recente.

CASO B

B ■ Reciclagem repetida em 2026 de uma base histórica da aviação

Base reciclada

Aviação e dados de consumidores

ALEGAÇÃO

Em abril, setembro (`B03`) e **23 de novembro de 2026** (`B13` , janela recente), várias contas voltaram a anunciar uma base de clientes atribuída a uma companhia aérea que opera em Portugal [S1]. As datas repetidas foram 6 de abril, 12, 13 e 22 de setembro e 23 de novembro [S1]. Um anúncio de setembro acrescentou `2026` ao título, mas as amostras mantêm campos históricos de fidelização com datas de 2017-2018 de uma fuga anterior já divulgada [S1].

O QUE NÃO ESTÁ ESTABELECIDO	Nenhuma republicação de 2026 estabelece uma nova intrusão na companhia aérea nem captura recente de dados de passageiros.
RESPOSTA	Equipas de resposta que monitorizam alertas na dark web devem verificar hashes e datas de amostra face a arquivos de fugas anteriores para evitar escaladas falsas.

Conclusão

Verifique as datas de registo nas amostras face a fugas históricas antes de tratar um anúncio de 2026 como incidente novo.

Ficha de evidência B03 — 13 set 2026

Utilizador de fórum (alcunha omitida) · Tópico de fórum · Fórum · Inglês

ORIGINAL

[Companhia aérea que opera em Portugal] Customer Database with Date of Birth 2026 [...] FULL_NAME BIRTH_DATE SALUTATION COMMUNICATION_LANGUAGE NATIONALITY GENDER ADDRESS_CITY [linhas de amostra omitidas]

Nota. Tópicos correspondentes em 6 de abril, 12 e 22 de setembro e 23 de novembro (B13) mantêm os mesmos campos de fidelização e datas de registo de 2017-2018 de uma fuga anterior já divulgada.

Observado

Um intermediário em fórum anuncia registos de passageiros atribuídos a uma companhia aérea que opera em Portugal sob um título datado de 2026.

Não estabelecido

Comprometimento da companhia aérea em 2026, extração recente ou atualidade verificada dos registos.

Ficha de evidência B13 — 23 nov 2026

Utilizador de fórum (alcunha omitida) · Tópico de fórum · Fórum · Inglês

ORIGINAL

[Companhia aérea que opera em Portugal] Data [...] [loyalty_id] birth_date salutation communication_language first_name last_name full_name nationality gender address_city [omitido; registration_date 17/08/2018]

Nota. Em conjunto com B03, confirma que a atividade de fóruns no final de novembro mistura arquivos históricos reciclados com anúncios mais recentes.

Observado

Na janela recente, outro vendedor volta a oferecer a mesma tabela de passageiros vista em abril e setembro, mantendo datas de registo de 2018.

Não estabelecido

Comprometimento da companhia aérea em novembro de 2026 ou recolha recente de dados.

4.3 Credenciais, portais públicos e ofertas alegadas de acesso inicial

CASO C

C

Combolists mensais de Portugal e alegações não confirmadas sobre portais públicos

Sem verificação

Credenciais e portais públicos

ALEGAÇÃO	Entre janeiro e novembro de 2026, contas automatizadas publicaram combolists `Email:Pass` com etiqueta Portugal anunciando entre 14 150 e 356 000 linhas por ficheiro [S1]. Destacam-se um ficheiro de 101 000 linhas em abril (`B04` , republicado em agosto) e um ficheiro de 71 000 linhas em **23 de novembro de 2026** (`B14` , janela recente) [S1]. Em maio, canais de Telegram partilharam extratos de infostealers correspondentes a endereços de início de sessão de serviços públicos em Portugal [S1]. Em **14 de novembro de 2026** (`B11` , janela recente), um utilizador de fórum partilhou ainda um alegado CSV de contas de coordenadores escolares de um portal público de educação [S1].
O QUE NÃO ESTÁ ESTABELECIDO	Etiquetas como `FRESH` ou `HQ` não confirmam palavras-passe válidas nem furto de 2026, e não foi localizada confirmação oficial até ao corte para a alegação de 14 de novembro.
RESPOSTA	Organismos públicos e portais de consumo devem assumir circulação contínua de credenciais de infostealers, exigir MFA em contas administrativas e vigiar tentativas de credential stuffing.

Conclusão

Exija MFA em portais públicos e correio web e pesquise infeções por infostealers nos equipamentos de colaboradores.

Ficha de evidência B04 — 30 abr 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Inglês

ORIGINAL

Database: Portugal Type: Email : Password Date: [29/ APR/2026] Combo: [101 K++] Line Status: FRESH | HQ

Nota. Etiquetas como FRESH e HQ são fórmulas comerciais habituais em compilações recicladas; o mesmo ficheiro de 29 de abril reapareceu noutro fórum em agosto.

Observado

Um tópico de fórum promove uma lista de correio eletrónico e palavras-passe etiquetada como Portugal com mais de 101 000 linhas, refletindo publicações mensais semelhantes de janeiro a novembro.

Não estabelecido

Palavras-passe válidas, utilizadores únicos, data real de recolha ou origem numa única fuga portuguesa.

Ficha de evidência B11 — 14 nov 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Inglês

ORIGINAL

DATABASE [portal público português de programa educativo] [...] sample: id,schoolId,obs,temp,email,phone,name,password,subject,coordinato [linhas de amostra omitidas]

Nota. O domínio do portal, nome do programa, dados pessoais e hashes de palavras-passe foram omitidos por falta de confirmação oficial até à data de corte.

Observado

Na janela recente, um utilizador partilha uma alegada exportação CSV de contas de docentes e coordenadores atribuída a um portal público português de educação.

Não estabelecido

Confirmação oficial de fuga, validade atual das palavras-passe, dimensão total do ficheiro ou acesso não autorizado comprovado.

Ficha de evidência B14 — 23 nov 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Inglês

ORIGINAL

[71 K++] { Portugal } Email:Pass FRESH [23-11-2026] Database : Portugal Type : Email , Password Condition: Fresh,HQ Combo: 71 K++ Line

Nota. Segue exatamente o mesmo modelo automatizado observado nas publicações anteriores de listas de credenciais de 2026.

Observado

Na janela recente, uma conta publica uma compilação de 71 000 linhas de correio eletrónico e palavras-passe etiquetada como Portugal com data de 23 de novembro de 2026.

Não estabelecido

Contas válidas únicas, roubo de credenciais em novembro ou comprometimento de uma organização portuguesa específica.

CASO D

D

Alegadas ofertas de Domain Admin empresarial, comércio eletrónico e VPN autárquica

Sem verificação

Acessos empresariais e municipais

ALEGAÇÕES EMPRESARIAIS	Quatro publicações clandestinas em 2026 anunciaram alegado acesso direto em Portugal [S1]. Em 28 de fevereiro, um vendedor anunciou acesso administrativo a uma loja online (alegando mais de EUR 2 milhões anuais) [S1]. Em 1 de maio (`B05`), surgiu uma oferta de **Active Directory Domain Admin** numa tecnológica portuguesa (`$100M-$500M`) [S1].
ALEGAÇÕES NO SETOR PÚBLICO	Em 2 de junho (`B06`), um canal Telegram divulgou alegadas credenciais GlobalProtect VPN de uma entidade autárquica portuguesa, e em 9 de julho surgiu alegado acesso administrativo a um subdomínio `.gov.pt` do setor público [S1].
O QUE NÃO ESTÁ ESTABELECIDO	Nenhuma das quatro publicações dispõe de confirmação independente da entidade, verificação de validade ativa das credenciais ou confirmação de ransomware subsequente.
RESPOSTA	As equipas de segurança devem impor MFA resistente a phishing em todas as VPN e consolas administrativas, auditar contas privilegiadas de Active Directory e rodar credenciais imediatamente perante qualquer exposição.

Conclusão

Implemente MFA resistente a phishing em todas as VPN, painéis administrativos e contas privilegiadas de Active Directory.

Ficha de evidência B05 — 1 mai 2026

Canal de monitorização (alcunha omitida)

Reenvio em canal Telegram | Telegram | Inglês

ORIGINAL

Selling: [Active Directory (Domain Admin)] Technology / SaaS - Portugal ($100M - $500M revenue) [referência de fórum omitida]

Nota. As ofertas de acesso inicial em Portugal surgem com pouca frequência em canais públicos, mas constituem precursores de impacto elevado quando válidas.

Observado

Um canal de monitorização reenvia um anúncio de fórum que oferece alegado acesso Active Directory Domain Admin a uma empresa tecnológica de média ou grande dimensão em Portugal.

Não estabelecido

Acesso ativo ao domínio, identidade confirmada da organização, exatidão da faturação indicada, ataque de ransomware posterior ou venda concluída.

Ficha de evidência B06 — 2 jun 2026

Autor em canal (alcunha omitida)

Canal Telegram | Telegram | Inglês

ORIGINAL

Here are some brief steps to configure access to [entidade local portuguesa]. 1. Access the website [URL VPN omitido]/global-protect/login.esp [credenciais omitidas]

Nota. Todos os identificadores da entidade, URL e credenciais foram removidos; o registo ilustra a exposição de portais VPN sem autenticação multifator.

Observado

Um canal Telegram publica alegadas credenciais em texto simples e instruções de ligação para um portal VPN GlobalProtect de uma entidade da administração local portuguesa.

Não estabelecido

Validade ativa das credenciais, ausência de MFA, entrada não autorizada na rede ou acesso confirmado a dados municipais.

4.4 Contactos bancários, procura de mulas KYC e abuso de canais de pagamento

CASO E

E

Listagens recentes de contactos bancários e de consumidores em Portugal

Sem verificação

Banca e contactos de clientes

ALEGAÇÕES NA JANELA RECENTE	Entre **12 e 26 de novembro de 2026**, uma conta anunciou 55 000 alegados contactos com **NIF** atribuídos a um grande banco em **21 de novembro** (B12) [S1]. Em **23 de novembro** (B15), a mesma conta anunciou 500 000 contactos de consumidores sem amostras [S1].
ALEGAÇÕES ANTERIORES	Em abril e maio, outro utilizador anunciou alegadas bases atribuídas a duas outras organizações portuguesas [S1].
O QUE NÃO ESTÁ ESTABELECIDO	Não existia confirmação oficial de fuga até ao corte para a lista atribuída ao banco, para os 500 000 contactos nem para as duas alegações de abril e maio. Listas comerciais com **NIF** e moradas resultam frequentemente de agregadores de marketing ou fugas históricas.

RESPOSTA

Bancos e operadoras devem monitorizar campanhas de vishing e smishing que citam o **NIF** mesmo sem intrusão interna, porque identificadores reais elevam a taxa de sucesso da fraude.

Conclusão

Monitorize campanhas de phishing e smishing com referência ao NIF mesmo quando a lista bancária anunciada não é confirmada.

Ficha de evidência B12 — 21 nov 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Inglês

ORIGINAL

[SELLING] 55k LEADS [banco comercial português] [...] format: NAME,TELEPHONE,EMAIL,NIF,ADDRESS,CITY,COUNTRY,ZIPCODE [linhas de amostra omitidas]

Nota. A identidade do banco e todos os dados pessoais foram removidos; listas com NIF resultam frequentemente de corretores terceiros ou fugas anteriores.

Observado

Na janela recente, um vendedor anuncia 55 000 alegados contactos comerciais contendo NIF e moradas atribuídos a um banco de retalho português.

Não estabelecido

Intrusão nos sistemas bancários, proveniência autêntica dos clientes, atualidade dos dados ou venda realizada.

Ficha de evidência B15 — 23 nov 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Inglês

ORIGINAL

[SELLING] 500k LEADS PORTUGAL (PT) I am selling 500k leads from Portugal {PT}, these are updated leads, one-time sale. Those interested should send a PM.

Nota. Ilustra a agregação comercial de contactos de consumidores portugueses que alimenta campanhas de fraude telefónica, SMS e falsos investimentos.

Observado

Dois dias após B12, a mesma conta anuncia um pacote de 500 000 contactos de consumidores em Portugal como venda única sem linhas de amostra.

Não estabelecido

Origem dos registos, exatidão dos dados, proveniência de fuga ou compra concretizada.

CASO F

F ■ Recrutamento de mulas KYC portuguesas, contas de receção e rotas SMS falsificadas

Procura por apurar

Identidade, telecomunicações e mulas

PROCURA DE IDENTIDADE E CONTAS MULA

Compradores recrutaram residentes em Portugal para verificação KYC em direto em janeiro e abril (USD 30 por verificação) e procuraram contas Wise e Revolut Pro portuguesas em março [S1]. Em 30 de junho (B08), um comprador em russo pediu uma conta portuguesa para transferências internas entre **EUR 2 000 e EUR 10 000** [S1].

OFERTA DE TELECOMUNICAÇÕES E SMS FALSIFICADO

Um bot adicionou números portugueses +351 descartáveis em 31 de março (B07) [S1]. Em **17 de novembro de 2026** (B10 , janela recente), uma publicação em português no Telegram anunciou rotas SMS em massa com remetentes falsificados visando clientes de um grande banco [S1].

O QUE NÃO ESTÁ ESTABELECIDO	Os anúncios de recrutamento e rotas não confirmam quantas contas foram abertas, quantas mensagens chegaram aos telemóveis nem que perdas concretas resultaram.
RESPOSTA	As instituições financeiras devem reforçar provas de vida na abertura remota de contas, sinalizar entradas rápidas em contas recentes e articular com operadoras e a **ANACOM** o bloqueio de cabeçalhos SMS falsificados.

Conclusão

Reforce a verificação biométrica na abertura de contas, sinalize entradas atípicas e vigie a usurpação de remetentes SMS.

Ficha de evidência B07 — 31 mar 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Russo / Inglês

ORIGINAL

Hello, dear forum members! Portugal has been added to the bot for disposable numbers. SMS numbers in the bot [identificador omitido]

Nota. Os serviços descartáveis de SMS +351 reduzem o custo de ultrapassar verificações telefónicas locais na criação fraudulenta de contas.

Observado
Um operador automatizado de cartões SIM virtuais anuncia a adição de números portugueses (+351) descartáveis para receção de SMS no seu bot de Telegram.

Não estabelecido
Volume de números portugueses disponíveis, operador de origem ou ligação confirmada a um caso concreto de fraude.

Ficha de evidência B08 — 30 jun 2026

Utilizador de fórum (alcunha omitida) | Tópico de fórum | Fórum | Russo

ORIGINAL

[Traduzido] Procura-se conta mula pontual em PT (Portugal) para transferências internas de 2 a 10 mil euros; apenas serviços com reputação, contacto por mensagem privada.

Nota. Alinha-se com pedidos de verificação KYC em Portugal registados em janeiro, março e abril e com o RASI 2025 da PJ sobre dispersão de fundos por mulas financeiras.

Observado
Um comprador num fórum em língua russa procura uma conta bancária intermediária em Portugal para receber transferências internas entre 2 000 e 10 000 euros.

Não estabelecido
Recrutamento concretizado, banco recetor identificado ou prejuízo financeiro comprovado.

Ficha de evidência B10 — 17 nov 2026

Autor em canal (alcunha omitida) | Canal Telegram | Telegram | Português

ORIGINAL

[Banco comercial português] em Portugal [...] temos rotas para dar suporte perfeito [...] Rotas novas, Sender ID estável [identificadores omitidos]

Nota. Nome do banco omitido. A publicação é compatível com os alertas da ANACOM e do Banco de Portugal sobre smishing bancário com usurpação de identificador.

Observado
Na janela recente, uma publicação em português no Telegram anuncia novas rotas de SMS em massa com remetentes alfanuméricos falsificados dirigidas a clientes de um grande banco português.

Não estabelecido
Taxa de entrega nas redes móveis portuguesas, volume real de campanha ou comprometimento do banco mencionado.

CASO G

G Ferramentas de referências Multibanco, canais MB WAY de alto risco e malware bancário móvel

Evidência mista

Pagamentos e banca móvel

ABUSO DE CANAIS DE PAGAMENTO	Em 5 de abril (`B09`), um fórum promoveu um gerador online de referências Multibanco pela característica "No Refunds - Realtime transactions" em Portugal [S1]. Em setembro, um processador em russo anunciou liquidação **Multibanco** e **MB WAY** para comerciantes de alto risco [S1].
MALWARE BANCÁRIO MÓVEL	Em 21 de fevereiro, fóruns recircularam detalhes do trojan Android **Massiv** dirigido à **Chave Móvel Digital** [S1][S81]. Entre junho e agosto e em 8 de novembro, publicações promoveram kits Android NFC e trojans (`VIPER NFC` , `RedHook` , `WindRelay`) na Península Ibérica [S1].
O QUE NÃO ESTÁ ESTABELECIDO	A promoção de ferramentas e malware não estabelece intrusão na infraestrutura SIBS ou Multibanco, nem quantifica infeções ativas em Portugal além dos casos investigados [S81].
RESPOSTA	Os bancos de retalho e gestores de identidade digital devem combinar telemetria de Serviços de Acessibilidade e sobreposição em Android com alertas contra aplicações IPTV externas e referências Multibanco não solicitadas.

Conclusão

Detete o abuso de Serviços de Acessibilidade em Android e alerte clientes contra aplicações IPTV externas e referências Multibanco fraudulentas.

Ficha de evidência B09 — 5 abr 2026

Utilizador de fórum (alcunha omitida) · Tópico de fórum · Fórum · Inglês

ORIGINAL

Multibanco Reference Generator - Online Version [...] For Sellers: Method number 1 in Portugal - No Refunds - Realtime transactions - Automatic Process. For Clients: ATM Payment (Multibanco).

Nota. Ilustra como os agentes de fraude exploram a familiaridade e irreversibilidade dos meios de pagamento nacionais em vez de falhas técnicas na rede interbancária.

Observado
Um utilizador reativa um tópico de fórum que promove um gerador online de referências Multibanco pela liquidação imediata e irreversível em Portugal.

Não estabelecido
Disponibilidade ativa da ferramenta, volume de transações ou comprometimento da infraestrutura da SIBS ou da rede Multibanco.

PRINCIPAIS CONCLUSÕES

01

As publicações clandestinas mostram procura criminosa ativa em torno de Portugal, não fugas verificadas.

02

A verificação de datas detetou registos aéreos antigos ainda vendidos como "2026" em 23 de novembro a par de anúncios-modelo de retalho.

03

A procura de mulas KYC portuguesas, números +351 descartáveis e rotas SMS falsificadas alimenta diretamente a fraude doméstica.

CAPÍTULO 05

Incidentes públicos confirmados e divulgações

ESTE CAPÍTULO RESPONDE

Que ciberincidentes de 2026 foram confirmados publicamente em Portugal e perturbaram serviços reais?

20

incidentes públicos oficialmente confirmados e amplamente noticiados (14 dossiês)

5.1 Disciplina de nomeação e âmbito dos incidentes 42

5.2 Incidentes confirmados de janeiro ao início de novembro de 2026 42

5.3 Atividade recente: 12 a 26 de novembro de 2026 50

CAPÍTULO 05

Incidentes públicos confirmados e divulgações

EM RESUMO

Entre janeiro e 26 de novembro de 2026, autoridades públicas, serviços essenciais, municípios, saúde, universidades e retalho em Portugal confirmaram 20 incidentes relevantes em catorze dossiês. Ransomware, encriptação municipal, extração de registos, servidores de testes de subcontratados, DDoS e ataques a frio OT atingiram serviços portugueses. Seis incidentes confirmados tiveram divulgações ou avisos a clientes na janela recente de 12 a 26 de novembro. Isole as TI administrativas das redes clínicas e operacionais, limite exportações de registos e reforce formulários web de imediato.

5.1 Disciplina de nomeação e âmbito dos incidentes

Uma organização portuguesa afetada só é nomeada neste capítulo quando se verificam **ambas** as condições: confirmação oficial pela própria entidade ou autoridade competente **e** ampla cobertura nos meios nacionais ou regionais (`public_names.json`). Alegações sem confirmação oficial, notícias isoladas sem confirmação institucional e casos municipais de 2023 ficam fora das contagens confirmadas, conforme detalhado no Apêndice A.7.

5.2 Incidentes confirmados de janeiro ao início de novembro de 2026

H

CASO H

Paralisação prolongada dos serviços digitais da Câmara Municipal da Guarda

Ataque confirmado

Administração municipal

CRONOLOGIA E IMPACTO	Em **12 de fevereiro de 2026**, a **Câmara Municipal da Guarda** detetou um ciberataque complexo que interrompeu comunicações externas e forçou o encerramento preventivo de plataformas municipais e do portal público durante semanas [S34][S35]. Em 4 de março, o município emitiu despacho formal a suspender prazos administrativos com efeitos retroativos a 12 de fevereiro enquanto reconstruía os serviços [S36].
NOTIFICAÇÃO OFICIAL	As autoridades municipais confirmaram a participação à **Polícia Judiciária** e a articulação da contenção com equipas nacionais [S35].
RESPOSTA	Os municípios devem manter cópias de segurança imutáveis offline testadas e despachos jurídicos preparados para suspender prazos legais caso os portais fiquem indisponíveis.

Conclusão

Mantenha cópias de segurança imutáveis offline e procedimentos jurídicos preparados para suspender prazos administrativos.

CASO I

I Fuga global na plataforma Instructure Canvas com impacto no ensino superior português

Fuga confirmada

Ensino superior (fornecedor)

CRONOLOGIA E IMPACTO

No início de **maio de 2026**, o fornecedor global **Instructure** confirmou um incidente de segurança na plataforma **Canvas** que atingiu estudantes e docentes de várias instituições portuguesas de ensino superior [S37][S38]. Os registos expostos incluíram nomes, endereços institucionais de correio eletrónico, identificadores de estudante e mensagens da plataforma, sem afetar palavras-passe, dados financeiros nem redes internas universitárias [S37] [S38].

NOTIFICAÇÃO OFICIAL

As instituições portuguesas afetadas notificaram a **Comissão Nacional de Proteção de Dados (CNPD)** e alertaram as comunidades académicas contra phishing com contexto real de disciplinas [S37]. Não se enumeram instituições individuais além de Instructure e Canvas devido à variação de âmbito nos comunicados.

RESPOSTA

As universidades devem inventariar todas as plataformas educativas SaaS com diretórios de estudantes e emitir alertas rápidos de phishing contextual perante falhas de fornecedores.

Conclusão

Inventarie plataformas educativas de terceiros com dados de estudantes e prepare alertas de phishing após falhas de fornecedores.

CASO J

J Extração não autorizada de dados de utentes no SNS 24 / SPMS

Fuga confirmada

Serviços nacionais de saúde

CRONOLOGIA E ÂMBITO

Em **21 de maio de 2026**, os **SPMS** (Serviços Partilhados do Ministério da Saúde) notificaram o **CNCS** após detetarem consultas automatizadas não autorizadas no portal **SNS 24** [S39][S40]. A investigação apurou que credenciais furtadas de um médico foram usadas durante vários dias para consultar dados administrativos de **mais de 100 000 utentes em todo o país** (sem processos clínicos) [S39][S41].

INVESTIGAÇÃO OFICIAL	O diretor da unidade de cibercrime da **Polícia Judiciária** (**UNC3T**) referiu que a velocidade de extração levantou a hipótese de apoio automatizado ou de IA [S39]. Os SPMS desativaram as credenciais usadas indevidamente para travar a extração, o **CNCS / CERT.PT** e a **PJ** conduziram perícias conjuntas e a reguladora **ERS** emitiu comunicado [S40][S42]. Não se identifica qualquer médico ou unidade local de saúde.
RESPOSTA	Os registos nacionais de saúde devem exigir MFA resistente a phishing nos portais clínicos, limitar a velocidade de consulta por conta e revogar sessões perante pesquisas anómalas à escala nacional.

Conclusão

Aplique limites de consulta, alertas de extração anómala e MFA resistente a phishing em portais clínicos com acesso a registos nacionais.

K

CASO K

Ataque de encriptação de ficheiros na Câmara Municipal de Serpa

Ataque confirmado

Administração municipal

CRONOLOGIA E IMPACTO	Entre as 04:00 e as 08:30 de **27 de maio de 2026**, um ciberataque de encriptação paralisou os sistemas informáticos e as linhas telefónicas fixas e móveis da **Câmara Municipal de Serpa** [S43][S44]. As equipas desligaram servidores e reconstruíram os sistemas com cópias diárias [S43]. A perda operacional permanente limitou-se assim à janela entre as 18:00 de 26 de maio e as 08:00 de 27 de maio [S43].
NOTIFICAÇÃO OFICIAL	O município alertou os munícipes para a possibilidade de alguns documentos terem sido copiados antes da encriptação e notificou formalmente o **CNCS**, o **Ministério Público**, a **CNPD** e a **Polícia Judiciária** [S43][S45].
RESPOSTA	As autarquias devem testar a reposição integral a partir de cópias diárias offline e segmentar servidores financeiros e de atendimento ao cidadão face aos postos comuns.

Conclusão

Teste a reposição integral a partir de cópias diárias offline e segmente os sistemas financeiros municipais dos postos comuns.

CASO L

L ■ Ransomware Qilin na Santa Casa da Misericórdia de Santo Tirso

Ataque confirmado

Saúde e apoio social

CRONOLOGIA E IMPACTO	Em **8 de junho de 2026**, a **Santa Casa da Misericórdia de Santo Tirso** sofreu ransomware que perturbou consultas médicas de ambulatório e meios de diagnóstico [S46][S47]. O apoio residencial a idosos prosseguiu em funcionamento normal [S46]. Uma equipa externa foi contratada para contenção e reconstrução [S46].
NOTIFICAÇÃO OFICIAL E REGISTO DE EXTORSÃO	A instituição comunicou o caso à **Polícia Judiciária**, ao **CNCS** e à **CNPD** [S47]. Em **16 de junho de 2026**, a etiqueta **Qilin** listou a organização na Ransompedia e publicou alegados ficheiros furtados [S2][S47].
RESPOSTA	As entidades de saúde e apoio social devem isolar redes clínicas dos servidores administrativos e validar qualquer publicação de extorsão face a registos forenses internos.

Conclusão

Isole sistemas clínicos das redes administrativas e valide quaisquer reivindicações em portais de extorsão face a registos forenses.

CASO M

M ■ Ransomware na Metro Mondego e alerta aos titulares de passes

Ataque confirmado

Transportes públicos

CRONOLOGIA E IMPACTO	Em **6 de julho de 2026**, a **Metro Mondego** sofreu um ataque de ransomware em parte dos sistemas administrativos internos [S48][S49]. A operadora confirmou que o transporte de passageiros em metrobus não foi afetado e que os terminais de pagamento com cartão estavam estritamente isolados das TI corporativas [S49].
EXPOSIÇÃO DE DADOS E REGISTO DE EXTORSÃO	Em **16 de julho**, a etiqueta **The Gentlemen** publicou uma reivindicação correspondente na Ransompedia [S2]. Em **26 de julho**, a Metro Mondego alertou titulares de passes personalizados e contactos por correio eletrónico para provável cópia de dados pessoais [S48]. Os campos incluíram nome, nascimento, morada, telefone, foto, **NIF**, documento e utilizações [S48]. A empresa confirmou notificações ao **CNCS**, à **CNPD** e à **Polícia Judiciária** [S50].
RESPOSTA	Os operadores de transportes devem manter separação rigorosa entre terminais de bilhética, operação de veículos e redes de escritório, preparando alertas diretos rápidos aos utilizadores.

Conclusão

Mantenha terminais de pagamento e operação de transportes isolados das TI corporativas e notifique rapidamente os titulares de passes.

CASO N

N ■ Ransomware na Universidade de Aveiro com exfiltração de correio e base de dados

Ataque confirmado

Ensino superior

CRONOLOGIA E IMPACTO	O **CNCS / CERT.PT** confirmou a receção de notificação em **20 de julho de 2026** sobre um ataque de ransomware na **Universidade de Aveiro**, divulgado publicamente em 29 de julho [S51]. A universidade confirmou exfiltração de contas de correio e de pelo menos uma base de dados [S51]. Impôs a alteração geral de palavras-passe e repôs serviços com cópias de segurança [S51][S52].
COORDENAÇÃO OFICIAL E ESCLARECIMENTO POSTERIOR	A Universidade de Aveiro articulou a resposta com o **CNCS**, a **CNPD**, a **Polícia Judiciária** e o **SIS** [S52]. Em setembro de 2026, a instituição esclareceu separadamente que falhas breves na rede resultaram de uma atualização de rotina de agosto sem ligação ao ataque de julho [S52].
RESPOSTA	As instituições académicas devem segmentar o correio institucional e bases de investigação, ensaiar planos de rotação global de credenciais e distinguir claramente avarias de rotina de incidentes anteriores.

Conclusão

Segmente o correio académico e bases de investigação, prepare planos de rotação global de palavras-passe e valide cópias de segurança.

CASO O

O ■ Ciberataque às TI administrativas do Grupo Águas de Portugal

Ataque confirmado

Abastecimento de água

CRONOLOGIA E IMPACTO	Em **31 de julho de 2026** (confirmado a 4 de agosto), o **Grupo Águas de Portugal (AdP)** sofreu um ciberataque complexo nas TI administrativas de 13 empresas operacionais [S53].
FRONTEIRA OPERACIONAL E NOTIFICAÇÕES	Em 4 e 7 de agosto, a AdP e a Ministra do Ambiente confirmaram que o abastecimento, tratamento e qualidade da água não foram afetados [S53] [S54]. Confirmaram também ausência de indícios de exfiltração de dados pessoais [S53]. A AdP notificou a **Polícia Judiciária**, o **CNCS** e a **CNPD** [S53].

RESPOSTA	Os serviços essenciais devem manter isolamento auditável entre TI corporativas e tecnologia operacional para que uma intrusão administrativa nunca atinja o controlo de abastecimento.

Conclusão

Preserve a separação estrita entre redes TI e OT para que uma intrusão administrativa não atinja o controlo do abastecimento.

CASO P

P

Vagas volumétricas DDoS na MEO e volume de ataques na Web Summit 2026

DDoS confirmado

Telecomunicações

CRONOLOGIA E IMPACTO	Entre **14 e 15 de setembro de 2026**, a **MEO** mitigou três vagas volumétricas de negação de serviço distribuída (**DDoS**) (00:45-02:55, 17:30-19:30 e 22:45-01:05) dirigidas a ligações internacionais [S55][S56]. Instabilidade secundária em BGP gerou mais de 7 200 reportes de falha no Downdetector antes da estabilização [S55]. A MEO confirmou ausência total de intrusão interna ou acesso a dados de clientes [S55][S56].
REFERÊNCIA EM GRANDE EVENTO	Separadamente, nos dois primeiros dias da **Web Summit 2026** em Lisboa (**9 e 10 de novembro**), a MEO intercetou **6 020 686** tentativas de ataque sem perturbação grave [S57].
RESPOSTA	As operadoras e anfitriões de grandes eventos devem ensaiar mitigação volumétrica a montante, salvaguardas de estabilidade BGP e boletins claros de estado de serviço.

Conclusão

Teste a mitigação volumétrica DDoS a montante, a resiliência de encaminhamento BGP e a comunicação de falhas antes de grandes eventos.

CASO Q

Q ■ Fuga em servidor de testes de subcontratado web externo do SIRP

Nota oficial

Cadeia de fornecimento pública

CRONOLOGIA E ESCLARECIMENTO OFICIAL	Em **7 de outubro de 2026**, um fórum anunciou um alegado arquivo de 120 GB associado a portais dos serviços de informações [S58][S59]. O anúncio alegava 312 144 ficheiros, 96 bases de dados e 180 sítios web [S58]. Em **8 de outubro**, o **Sistema de Informações da República Portuguesa (SIRP)** confirmou que os ficheiros provinham de um servidor de desenvolvimento e testes de um fornecedor web externo [S58][S59]. Esse servidor alojava os sítios públicos institucionais (`SIRP`, `SIS`, `SIED`) a par de sítios de dezenas de outros clientes desse subcontratado [S58].
LIMITE DO IMPACTO	O SIRP confirmou que **nenhum sistema ou dado classificado, operacional ou interno** do SIRP, SIS ou SIED foi afetado, notando apenas elementos não confidenciais de recrutamento na cópia de testes [S58]. O SIRP participou formalmente o caso à **Procuradoria-Geral da República (PGR)** [S59]. O subcontratado externo não é nomeado além do âmbito oficial do SIRP.
RESPOSTA	Os organismos públicos devem proibir contratualmente dados reais de cidadãos em servidores de testes de fornecedores e auditar a destruição periódica de cópias.

Conclusão

Proíba dados reais de cidadãos em servidores de testes de fornecedores externos e audite contratualmente a destruição de dados.

CASO R

R ■ Fuga no Registo Nacional de Bombeiros da ANEPC e paragens municipais no distrito de Aveiro

Casos confirmados

Proteção civil e municípios

FUGA NO RNBP DA ANEPC (24 DE OUTUBRO)	Em **24 de outubro de 2026**, a **Autoridade Nacional de Emergência e Proteção Civil (ANEPC)** confirmou um ataque que copiou registos do **Registo Nacional de Bombeiros Portugueses (RNBP)** [S62]. A fuga abrangeu cerca de **60 000 bombeiros** [S62][S63]. Os campos expostos incluíram nome, Cartão de Cidadão (`CC`), `NIF`, `NISS`, número de `SNS`, carta de condução, morada, fotografia e grupo sanguíneo, sem afetar dados bancários [S62][S63]. A ANEPC suspendeu o registo com o **CNCS** e a **Rede Nacional de Segurança Interna (RNSI)**, alertando operacionais com a **Liga dos Bombeiros Portugueses** contra phishing, smishing, vishing e quishing [S62][S63].

MUNICÍPIOS DO DISTRITO DE AVEIRO (18 DE OUTUBRO E 5 DE NOVEMBRO)	Com dezoito dias de intervalo no mesmo distrito, dois municípios sofreram intrusões disruptivas sem ligação técnica estabelecida entre si [S60][S66]. A **Câmara Municipal de Ovar** encerrou serviços digitais em **18 de outubro**, suspendeu prazos administrativos, alertou munícipes para possível exposição de dados pessoais e prolongou a recuperação por novembro [S60][S61]. Em **5 de novembro**, a **Câmara Municipal de Santa Maria da Feira** confirmou um ciberataque noturno que paralisou sistemas informáticos, correio eletrónico e telefones fixos, notificando o **CNCS** [S66][S67].
RESPOSTA	Os registos nacionais devem limitar exportações em massa e auditar descarregamentos de API, enquanto os municípios devem partilhar monitorização SOC 24/7 através do **Fórum de Cibersegurança da Administração Local (FCSAL)** [S5].

Conclusão

Restrinja exportações em massa em registos nacionais de pessoal e reforce a monitorização municipal partilhada através do Fórum de Cibersegurança da Administração Local (FCSAL).

CASO S

S

Ataque na cadeia de fornecimento OT de refrigeração no Intermarché Portugal

Ataque confirmado

Refrigeração OT no retalho

CRONOLOGIA E IMPACTO FÍSICO	Em **2 de novembro de 2026**, um ciberataque pan-europeu dirigido a um fornecedor de gestão remota de frio elevou temperaturas em frigoríficos e congeladores de supermercados em vários países europeus [S64][S65]. O **Grupo Mosqueteiros** e a **APED** confirmaram que **sete lojas Intermarché em Portugal** foram atingidas: **três lojas** sofreram perda total de mercadoria refrigerada, enquanto **quatro lojas** evitaram estragos de mercadoria [S64][S65]. A cadeia logística central do grupo não foi afetada [S64].
RESPOSTA	O retalho e as equipas de manutenção devem eliminar a exposição direta à Internet de controladores de frio de terceiros, exigir MFA nos acessos remotos de fornecedores e validar comandos manuais locais.

Conclusão

Elimine a exposição direta à Internet de controladores de frio de terceiros e imponha MFA nos acessos remotos de manutenção.

5.3 Atividade recente: 12 a 26 de novembro de 2026

Os últimos 15 dias (**12 a 26 de novembro de 2026**) registaram **715 publicações com etiqueta Portugal**, incluindo **6** em fóruns e **8** em português no Telegram (entre as quais `B10`) [S1]. Separadamente, **25 publicações em fóruns** mencionaram Portugal em tópicos com e sem etiqueta de país (de onde provêm `B11` - `B15`), a par de **seis incidentes públicos confirmados** (`Casos T-U`) [S1]. A Ransompedia registou **2 entradas não verificadas com etiqueta Portugal** (`Booba-project` em 17 de novembro e `N0n` em 25 de novembro, identidades omitidas) [S2]. Estes números aplicam-se estritamente a esta janela recente de 15 dias e não implicam um período de observação mais longo.

CASO T

T ■ Fuga de dados de clientes na Worten e exposição de formulários nos SMAS de Sintra

Fugas confirmadas

Retalho e água municipal (recente)

WORTEN (DIVULGADO EM 11 DE NOVEMBRO; AVISOS A CLIENTES EM 12 DE NOVEMBRO)	A **Worten** confirmou acesso não autorizado a dados limitados de clientes e prestadores (`NIF`, telefone, correio eletrónico e alguns números de encomenda) [S68][S70]. A empresa confirmou que **nenhuma palavra-passe ou dado de cartão** foi acedido [S69]. A Worten corrigiu a falha técnica explorada e notificou o **CNCS**, a **CNPD** e a **Polícia Judiciária** [S68][S70].
SMAS DE SINTRA (CONFIRMADO EM 12 DE NOVEMBRO)	Os serviços municipalizados **SMAS de Sintra** confirmaram um ciberataque contra formulários online que copiou registos (`nome`, `morada`, `telefone`, `NIF`, `documento de identificação` e `IBAN`) de um subconjunto de clientes [S71][S72]. Os SMAS de Sintra confirmaram que históricos de pagamentos e débitos diretos não foram afetados e notificaram a **CNPD** e o **CNCS** [S72].
RESPOSTA	O retalho e os serviços de água devem corrigir de imediato falhas em formulários web, reduzir o armazenamento prolongado de `NIF` e `IBAN` nos servidores web e alertar clientes contra burlas de alteração de faturação.

Conclusão

Corrija rapidamente falhas em formulários públicos, reduza a retenção de NIF e IBAN e alerte clientes contra fraudes direcionadas.

CASO U

U

Perturbações em portais públicos no final de novembro e intrusão no SCE da ADENE

Casos confirmados

Portais públicos e energia (recente)

IMT (PERTURBADO DESDE 14 DE NOVEMBRO; CONFIRMADO A MEIO DO MÊS)	O **Instituto da Mobilidade e dos Transportes (IMT)** confirmou ciberataques consecutivos que obrigaram à suspensão preventiva dos serviços digitais, afetando escolas de condução e processos de habilitação sem indícios de exfiltração de dados pessoais [S74].
ASAE (15 DE NOVEMBRO) E CÂMARA MUNICIPAL DO PORTO (21 DE NOVEMBRO)	Em **15 de novembro**, fonte oficial da **ASAE** (Autoridade de Segurança Alimentar e Económica) confirmou a desfiguração do portal que o deixou indisponível, com contacto confirmado pelo **CNCS** [S73]. Em **21 de novembro**, a **Câmara Municipal do Porto** confirmou uma alteração no gestor de conteúdos na página principal e subpáginas sem **qualquer fuga de dados pessoais**, notificando o **CNCS** [S75][S76]. Imagens de protesto e palavras de ordem dos intrusos são omitidas.
ADENE (23 DE NOVEMBRO)	Em **23 de novembro de 2026**, a agência nacional de energia **ADENE** confirmou uma intrusão não autorizada e isolou os sistemas afetados [S77]. A ADENE suspendeu temporariamente o **Sistema de Certificação Energética dos Edifícios (Portal SCE)** mantendo válidos os certificados já emitidos, e notificou o **CNCS** e a **Polícia Judiciária** [S77][S78].
OPERAÇÕES POLICIAIS NA MESMA JANELA	Em **17 de novembro**, a **PJ UNC3T** deteve dois suspeitos pela utilização fraudulenta no retalho de cartões bancários franceses clonados em montante superior a **EUR 48 000** [S31]. Em **23 de novembro**, a **PJ** participou na **Operação PowerOFF** da Europol contra plataformas de DDoS a pedido, conseguindo **59 remoções na Google em 62 pedidos**, o registo mais elevado entre 20 países participantes [S32].
OUTROS SINAIS CLANDESTINOS DE 12 A 26 DE NOVEMBRO (`B10-B15`)	Nesta janela de 15 dias surgiram rotas SMS bancárias falsificadas (`B10` , 17 nov), um alegado CSV de portal educativo (`B11` , 14 nov) e 55 000 contactos bancários (`B12` , 21 nov) [S1]. Em 23 de novembro, surgiram ainda registos aéreos históricos reciclados (`B13`), um combolist Portugal de 71 000 linhas (`B14`) e 500 000 alegados contactos de consumidores (`B15`) [S1].

Conclusão

Reforce os gestores de conteúdos web, separe portais públicos dos registos centrais e ensaie o restauro rápido em servidores isolados.

PRINCIPAIS CONCLUSÕES

01

Vinte incidentes confirmados em 2026 demonstram impacto operacional real em autarquias, registos nacionais, saúde, água, retalho e telecomunicações.

02

O abastecimento do Grupo Águas de Portugal e a operação do metrobus da Metro Mondego foram dados como não afetados, enquanto um sistema de frio gerido por fornecedor foi atingido em sete lojas Intermarché.

03

Seis incidentes confirmados (divulgados ou notificados a clientes desde 12 de novembro) e duas operações da PJ concentraram-se na janela recente.

CAPÍTULO 06

Perturbação, hacktivismo e alegação face à realidade

ESTE CAPÍTULO RESPONDE

Como devem os defensores em Portugal separar impacto operacional real de alegações hacktivistas e falhas não cibernéticas?

+36%

subida homóloga de incidentes de disponibilidade DDoS no CERT.PT em 2025 (115 casos)

6.1 Cronologia dos marcos de perturbação, ação policial e resiliência em 2026 54

6.2 Hacktivismo, pressão DDoS e prontidão municipal 55

6.3 Alegação face ao registo oficial 55

CAPÍTULO 06

Perturbação, hacktivismo e alegação face à realidade

EM RESUMO

A perturbação em Portugal em 2026 junta DDoS e desfigurações confirmadas, alegações hacktivistas no Telegram e avarias técnicas não cibernéticas. Em março de 2026, o relatório técnico da ENTSO-E atribuiu o apagão ibérico de 28 de abril de 2025 a fatores técnicos de controlo de tensão, e as fontes oficiais citadas não identificam causa cibernética. Em 2025, os casos DDoS no CERT.PT subiram 36% e o SIS alertou para riscos de sabotagem OT. Baseie a comunicação de crise em telemetria própria e relatórios oficiais.

6.1 Cronologia dos marcos de perturbação, ação policial e resiliência em 2026

15 jan 2026	CNPD e CNCS assinam protocolo nacional de cooperação para articulação de emergência 24/7 [S9]
12 fev 2026	Câmara Municipal da Guarda sofre ciberataque prolongado que bloqueia serviços digitais [S34][S35]
4 mar 2026	PJ detém dois suspeitos no desmantelamento LeakBase da Europol e apoia ação Tycoon 2FA (>160 entidades em Portugal) [S29]
20 mar 2026	Relatório técnico da ENTSO-E sobre o apagão ibérico de 28 de abril de 2025 aponta fatores de controlo de tensão; sem causa cibernética identificada [S16][S17]
3 abr 2026	Entra em vigor em Portugal o Decreto-Lei n.º 125/2025 (transposição NIS2) [S22]
21 mai 2026	SPMS notifica o CNCS sobre acesso indevido ao SNS 24 atingindo mais de 100 000 utentes [S39][S40]
23 jun 2026	Entra em vigor o Regulamento n.º 756/2026 do CNCS que operacionaliza a plataforma MyCiber [S23] [S24]
31 jul 2026	Grupo Águas de Portugal deteta ciberataque nas TI administrativas sem impacto no abastecimento de água [S53][S54]
14 set 2026	MEO mitiga três vagas volumétricas DDoS em ligações internacionais sem intrusão [S55][S56]
28 set 2026	Câmara Municipal de Valongo realiza o exercício municipal de ciberemergência CIBER 26 [S21]
24 out 2026	ANEPC suspende o Registo Nacional de Bombeiros (RNBP) após cópia de cerca de 60 000 registos [S62] [S63]
2 nov 2026	Ataque pan-europeu a controladores OT de frio atinge sete lojas Intermarché em Portugal [S64][S65]
23 nov 2026	ADENE isola o Portal SCE após intrusão; PJ soma 59 remoções na Operação PowerOFF da Europol [S32] [S77]

6.2 Hacktivismo, pressão DDoS e prontidão municipal

Os dados oficiais do **RASI 2025** fixaram uma base clara de disponibilidade à entrada de 2026: o **CERT.PT** registou um **aumento homólogo de 36%** em incidentes de negação de serviço (**115** casos) [S5]. No mesmo relatório, o **SIS** alertou que coletivos hacktivistas nacionalistas pró-russos constituem uma ameaça contínua de cibersabotagem contra infraestruturas críticas europeias e portuguesas e sistemas de gestão industrial e operacional [S5]. Em julho de 2025, a **Eurojust** e a **Europol** desmantelaram infraestrutura DDoS do grupo **NoName057(16)** (descrito pela Eurojust como pró-russo) em 12 países, desativando mais de 100 servidores e emitindo sete mandados de detenção [S33].

Na nossa recolha de Telegram de 2026 com etiqueta Portugal, surgiram três alegações hacktivistas não verificadas que exigem tratamento sem amplificação [S1]:

- **313 Team (26 de março de 2026):** Um canal no Telegram reivindicou um breve ataque DDoS contra um sítio web de uma força de segurança portuguesa; não foi encontrada confirmação oficial de indisponibilidade [S1].
- **Z-Pentest Alliance (11 de maio de 2026):** Uma retransmissão em espanhol no Telegram publicou uma alegação não verificada visando um controlador industrial de iluminação e automação exposto à Internet em Portugal [S1]. Nenhuma perturbação oficial foi confirmada, embora a classe de alvo se insira no alerta do SIS no RASI 2025 sobre cibersabotagem contra sistemas de infraestruturas críticas e de gestão industrial e operacional [S5].
- **BNCT (31 de outubro de 2026):** Um canal reivindicou a desfiguração de dois subdomínios de exposições de uma instituição cultural pública portuguesa (entidade e subdomínios omitidos por ausência de confirmação oficial) [S1].

Separadamente, as autoridades portuguesas de proteção civil e poder local reforçaram exercícios práticos em 2026. Em **28 de setembro de 2026**, a **Câmara Municipal de Valongo** conduziu o exercício **CIBER 26**, simulando paragens simultâneas no abastecimento de água, distribuição elétrica e escolas [S21]. Antes das **eleições presidenciais de 2026**, a **Comissão Nacional de Eleições (CNE)** abriu um canal de denúncia de desinformação [S18]. A **ERC** publicou ainda um estudo com o **LabCom-UBI** sobre desinformação online [S19]. Estas iniciativas incidiram sobre integridade informativa online, e não sobre intrusões técnicas nos sistemas eleitorais.

6.3 Alegação face ao registo oficial

Avarias informáticas de rotina, eventos históricos e publicações oportunistas no Telegram distorcem frequentemente a perceção pública em Portugal. O rastreio do Ciberseguranca.PT contabilizou **32 eventos cibernéticos públicos em Portugal** até 23 de novembro de 2026 [S79]. A lista separa claramente avarias informáticas sem ataque, como falhas clínicas, de despacho de emergência e no Microsoft 365 [S79].

Alegação ou perceção pública	Registo estabelecido	Disciplina defensiva
Especulação atribuindo o apagão ibérico de 28 de abril de 2025 a um ciberataque [S16][S17]	O relatório técnico da ENTSO-E validado pela ACER e apresentado a 20 de março de 2026 atribui o apagão a múltiplos fatores técnicos, incluindo controlo de tensão insuficiente, com falhas iniciais em Granada, Badajoz e Sevilha, e sem causa cibernética identificada [S16] [S17]	Nunca atribua falhas elétricas ou de infraestruturas a ciberataques sem confirmação técnica oficial
Publicações de fórum em 7 de outubro alegam intrusão nas redes classificadas das secretas portuguesas [S58][S59]	O SIRP confirmou em 8 de outubro que os ficheiros provinham do servidor de testes de um subcontratado web para sítios públicos, sem qualquer sistema classificado ou operacional afetado [S58][S59]	Separe o alojamento web externo dos ambientes internos e verifique rapidamente comunicados oficiais de âmbito
Vendedores anunciam uma base aérea como "2026" em 13 de setembro e 23 de novembro (`B03` , `B13`) [S1]	As amostras exibem campos históricos de fidelização com datas de 2017-2018 de uma fuga anterior já divulgada; não está estabelecida qualquer intrusão aérea em 2026 [S1]	Valide hashes e datas de amostra face a arquivos históricos antes de escalar o incidente
Falhas de rede em setembro na Universidade de Aveiro percebidas como um segundo ciberataque [S52]	A Universidade de Aveiro esclareceu que a avaria de setembro resultou de uma atualização de rotina de agosto sem ligação ao ransomware confirmado em julho [S52]	Publique notas claras de causa-raiz distinguindo avarias de manutenção de incidentes de segurança
Publicações hacktivistas no Telegram alegam ataques a portais policiais ou controladores OT (313 Team, Z-Pentest Alliance) [S1]	Nenhuma alegação teve confirmação oficial de impacto operacional; contudo, controladores OT expostos comportam risco real, como ficou evidente em novembro (`Caso S`) [S5][S64]	Meça a disponibilidade real, inspecione ativos OT expostos diretamente e omita retórica de atacantes nos avisos

PRINCIPAIS CONCLUSÕES

01

As conclusões técnicas oficiais atribuem o apagão ibérico de abril de 2025 a fatores de controlo de tensão e não identificam causa cibernética.

02

Distinga ataques DDoS e desfigurações confirmadas de alegações no Telegram e falhas informáticas de rotina.

03

Ensaie continuidade municipal multisserviço (como o CIBER 26 de Valongo) e comunique apenas com base em telemetria própria.

CAPÍTULO 07

Ransomware, registos de extorsão e perfis de ameaça

ESTE CAPÍTULO RESPONDE

Que etiquetas de extorsão visam Portugal em 2026 e como se posiciona o país face aos pares regionais?

36

registos de ransomware com etiqueta Portugal em 17 etiquetas (face a 21 em 2025)

7.1 Trajetória do ransomware em Portugal e comparação regional 58

7.2 Rede de relações e perfis de grupos 60

7.3 Contexto de ciberespionagem atribuída oficialmente e perfis hacktivistas 65

CAPÍTULO 07

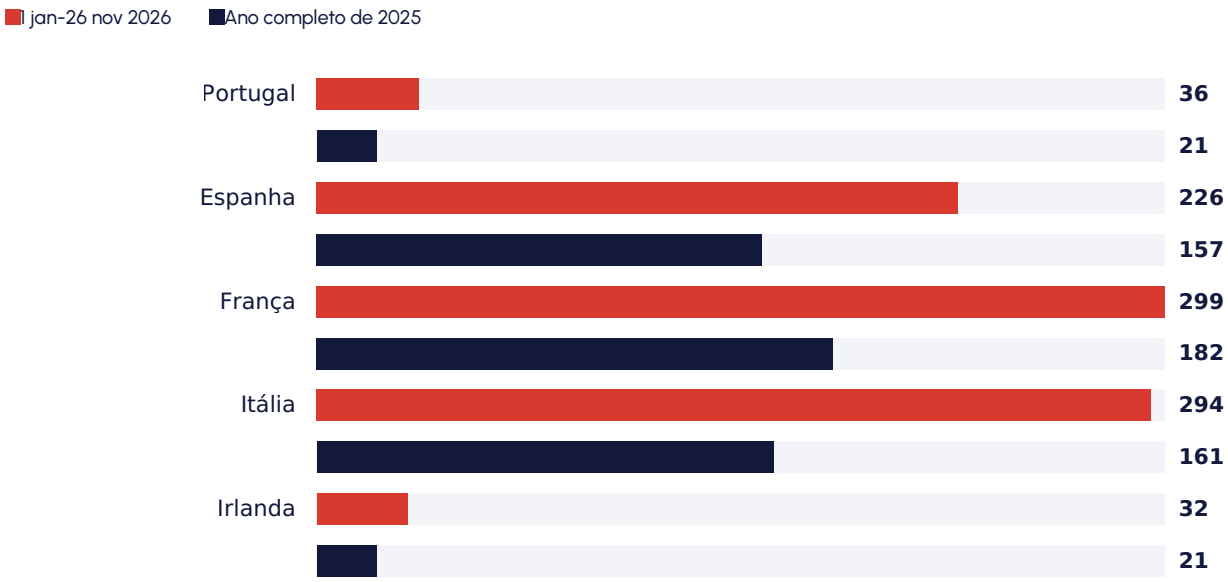
Ransomware, registos de extorsão e perfis de ameaça

EM RESUMO

A Ransompedia registou 36 entradas com etiqueta Portugal até 26 de novembro de 2026 (face a 21 em 2025), com 30 (83,3%) entre junho e novembro. The Gentlemen (9) e Qilin (7) lideram e coincidem com duas vítimas confirmadas (Metro Mondego e Santa Casa da Misericórdia de Santo Tirso). Trinta e quatro registos ficam por verificar e uma duplicação da Nova limita as entidades a no máximo 35. Valide cada registo em logs forenses e teste cópias imutáveis offline.

7.1 Trajetória do ransomware em Portugal e comparação regional

Os 36 registos de ransomware em Portugal em 2026 superam o total de 2025 a par dos pares regionais



Fonte: Brandefense Ransompedia, 1 de janeiro-26 de novembro de 2026 face ao ano completo de 2025 [S2]. Períodos desiguais; alegações com etiqueta de país, não vítimas únicas, intrusões confirmadas nem classificação nacional de segurança.

Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

Entre **1 de janeiro e 26 de novembro de 2026**, a Ransompedia registou **36 entradas com etiqueta Portugal** em **17 etiquetas** [S2]. O valor sobe **71,4%** face às **21 entradas** de todo o ano de **2025**, somando **104** registos acumulados [S2]. Nos quatro comparadores regionais de Portugal na mesma janela de 2026 face ao ano completo de 2025, **Espanha** registou **226** entradas (vs 157) e **França 299** (vs 182) [S2]. **Itália** contabilizou **294** entradas (vs 161) e a **Irlanda 32** (vs 21) [S2].

Quatro matizes analíticos mantêm precisa a leitura da contagem portuguesa de 2026 [S2]:

- **Forte aceleração no segundo semestre.** As entradas mensais em Portugal subiram acentuadamente após maio: fevereiro (1), março (3), abril (1), maio (1), junho (5), julho (10), agosto (2), setembro (7), outubro (3) e novembro (3) [S2]. Duas das três entradas de novembro surgiram na janela recente de 12-26 de novembro [S2]. Exatamente **30 de 36 entradas (83,3%)** ocorreram a partir de junho [S2].
- **Entidades distintas alegadas.** Em 24 de junho de 2026, a etiqueta `Nova` publicou no mesmo dia duas entradas para a mesma organização portuguesa usando o domínio e o nome curto [S2]. Os 36 registos correspondem assim a **no máximo 35 entidades distintas alegadas** [S2].
- **Apenas duas entradas têm confirmação pública.** Existem confirmações independentes para a **Santa Casa da Misericórdia de Santo Tirso** (`Qilin`, 16 de junho, `Caso L`) e a **Metro Mondego** (`The Gentlemen`, 16 de julho, `Caso M`) [S2][S47][S48]. Os restantes **34 registos** mantêm-se alegações criminosas não verificadas com identidades omitidas.
- **Etiquetas setoriais.** As etiquetas setoriais de origem lideram em **indústria/manufatura (7)**, **consultoria (4)**, **construção (3)**, **finanças (3)**, **educação (3)**, **global (3)**, **logística (2)** e **saúde (2)** [S2]. Entradas isoladas abrangeram agronegócio, engenharia, indústria pesada, transporte rodoviário, software/SaaS, universidades, alta tecnologia e cultura [S2]. Vários ataques municipais confirmados (`Casos H, K, R`) não apareceram em portais de extorsão monitorizados, o que lembra que estes rastreadores podem subestimar o total de encriptações operacionais.

Etiqueta reivindicante	Entradas PT 2026	Meses ativos (2026)	Estado de verificação
The Gentlemen	9	Fev, Mar, Jun, Jul, Set	1 confirmada publicamente (`Metro Mondego`, `Caso M`); 8 não verificadas [S2] [S48]
Qilin	7	Mar, Jun, Jul, Ago, Out, Nov	1 confirmada publicamente (`Santo Tirso`, `Caso L`); citada pelo CERT.PT no RASI 2025; 6 não verificadas [S2] [S5][S47]
SafePay	3	Mar, Mai, Set	Registou também 12 entradas com etiqueta Espanha em 2026; entradas PT não verificadas [S2]
N0n	2	Out, Nov (25 nov)	Ativa na janela recente de 12-26 nov; alegações não verificadas [S2]
Majinahanashi	2	Jul, Out	Alegações não verificadas [S2]
Nova	2	Jun (mesmo dia)	Duas entradas no mesmo dia para uma entidade; alegação não verificada [S2]

Etiqueta reivindicante	Entradas PT 2026	Meses ativos (2026)	Estado de verificação
Onze etiquetas com entrada única	11	Mar-Nov	`Arcus Media`, `Booba-project` (17 nov), `Dead-lock`, `DragonForce`, `Lockbit5`, `M3rx`, `Panzer`, `Section9`, `Settra`, `Space Bears`, `UnSafe`; todas não verificadas [S2]
Total registado	**36**	**Fev-Nov 2026**	**No máximo 35 entidades distintas alegadas; 2 confirmadas publicamente** [S2]

7.2 Rede de relações e perfis de grupos

A vista de relações abaixo separa estritamente observações próprias da Brandefense (`own data`), relatórios oficiais (`official`) e confirmações públicas (`public reporting`). Não se infere qualquer ligação operacional não comprovada entre etiquetas criminosas de ransomware, canais hacktivistas e avaliações oficiais de ciberespionagem estatal.

Publicação própria Reenvio Comunicado oficial Informação pública A nossa observação

SafePay

Dados próprios
3 listagens, S2 ↓

Listagens associadas a Portugal

Dados próprios
9 listagens, S2 ↑

The Gentlemen

Informação pública
Metro Mondego confirmou ransomware de 6 jul, S48-S50 ↓

Ransomware PT confirmado

Informação pública
Santo Tirso confirmou ransomware de 8 jun, S46-S47 ↑

Qilin

N0n

Dados próprios
2 listagens incl. 25 nov, S2 ↓

Listagens associadas a Portugal

Dados próprios
7 listagens, S2 ↑

Qilin

Nova e Majinahanashi

Dados próprios
2 listagens cada (incl. 1 duplicado Nova), S2 ↓

Listagens associadas a Portugal

Z-Pentest Alliance

Dados próprios
Classe de alvo coincide com contexto OT do SIS (S1, S5); sem ligação oficial ao grupo ↓

RASI 2025 / Eurojust

Comunicado oficial
Operação Eurojust (S33); contexto DDoS SIS/CERT.PT (S5) ↓

NoName057(16)

The Gentlemen

Thegentlemen (designação na Ransompedia)

Designação de extorsão / ransomware | Sem atribuição estatal estabelecida

EM PORTUGAL, 2026

Janela de 2026

9 listagens associadas a Portugal (fevereiro, março, junho, julho e setembro de 2026), S2; 1 confirmada publicamente (Metro Mondego, S48-S50)

ALVOS ALEGADOS

Entradas associadas a Portugal nos transportes, construção, indústria, finanças e educação; 8 identidades não confirmadas omitidas

EM FONTES PÚBLICAS

[S2] 9 listagens registadas na Ransompedia (maior reivindicador isolado sobre Portugal em 2026)

[S48-S50] A Metro Mondego confirmou o ataque de ransomware de 6 de julho e a reivindicação pública sobre dados de titulares de passes personalizados

A NOSSA AVALIAÇÃO

The Gentlemen concentrou um quarto das listagens de ransomware associadas a Portugal em 2026 (9 em 36), com picos em julho e setembro. A Metro Mondego confirmou de forma independente o incidente de 6 de julho correspondente à listagem de 16 de julho; as restantes oito listagens permanecem alegações não verificadas.

CONFIANÇA

Elevada para a contagem registada e para a confirmação da Metro Mondego; restantes 8 alegações não verificadas

Qilin

Designação na Ransompedia e na taxonomia CERT.PT 2025

Designação de ransomware-as-a-service / extorsão | Sem atribuição estatal estabelecida

EM PORTUGAL, 2026

Janela de 2026

7 listagens associadas a Portugal (março, junho, julho, agosto, outubro e novembro de 2026), S2; 1 confirmada publicamente (Santa Casa da Misericórdia de Santo Tirso, S46-S47)

ALVOS ALEGADOS

Entradas associadas a Portugal em logística, saúde, indústria, tecnologia, finanças e consultoria; 6 identidades não confirmadas omitidas

EM FONTES PÚBLICAS

[S2] 7 listagens registadas na Ransompedia (segundo maior reivindicador sobre Portugal em 2026)

[S5] Referido pelo CERT.PT no RASI 2025 entre as variantes de ransomware mais frequentemente observadas em Portugal em 2025

[S46-S47] A Santa Casa da Misericórdia de Santo Tirso confirmou a intrusão de 8 de junho; a Qilin listou a organização a 16 de junho

A NOSSA AVALIAÇÃO

A Qilin evidencia pressão contínua ao longo de dois anos sobre organizações portuguesas, ligando os registos de resposta a incidentes do CERT.PT em 2025 a sete listagens em 2026. Embora a Santa Casa da Misericórdia de Santo Tirso tenha confirmado o ataque de junho, as outras seis listagens exigem validação forense independente.

CONFIANÇA
Elevada para as contagens, base RASI 2025 e confirmação de Santo Tirso; restantes 6 alegações não verificadas

SafePay

Safepay (designação na Ransompedia)

Designação de extorsão / ransomware | Sem atribuição estatal estabelecida

EM PORTUGAL, 2026

Janela de 2026

3 listagens associadas a Portugal (março, maio e setembro de 2026), S2

ALVOS ALEGADOS

Entradas comerciais, industriais e de consultoria associadas a Portugal; todas as identidades omitidas

EM FONTES PÚBLICAS

[S2] 3 listagens associadas a Portugal e 12 associadas a Espanha registadas na Ransompedia em 2026

A NOSSA AVALIAÇÃO

A SafePay ocupa o terceiro lugar nas entradas associadas a Portugal (3 em 36) e mantém atividade paralela na vizinha Espanha (12 listagens). Nenhuma das três entradas portuguesas teve confirmação oficial pública até à data de corte, pelo que devem ser tratadas estritamente como alegações não verificadas.

CONFIANÇA
Elevada para a contagem registada; alegações individuais em Portugal não verificadas

N0n

Designação na Ransompedia

Designação de extorsão / ransomware | Sem atribuição estatal estabelecida

EM PORTUGAL, 2026

Janela de 2026

2 listagens registadas associadas a Portugal (24 de outubro; 25 de novembro, dentro da janela recente), S2

ALVOS ALEGADOS

Entradas na indústria e construção; identidades omitidas

EM FONTES PÚBLICAS

[S2] 2 listagens associadas a Portugal registadas na Ransompedia em outubro-novembro de 2026

A NOSSA AVALIAÇÃO

O grupo N0n corresponde a uma das duas listagens de ransomware associadas a Portugal publicadas durante a janela recente de 12 a 26 de novembro (juntamente com Booba-project a 17 de novembro). As listagens carecem de confirmação independente e exigem validação técnica antes de presumir impacto operacional.

CONFIANÇA

Elevada para a contagem registada; alegações individuais não verificadas

Nova e Majinahanashi

Designações na Ransompedia

Designações de extorsão / ransomware | Sem atribuição estatal estabelecida

EM PORTUGAL, 2026

Janela de 2026

2 listagens registadas cada na Ransompedia (Nova a 24 de junho; Majinahanashi em julho e outubro de 2026), S2

ALVOS ALEGADOS

Entradas em consultoria, agroindústria e indústria transformadora; identidades omitidas

EM FONTES PÚBLICAS

[S2] A Nova publicou duas entradas no mesmo dia para a mesma entidade a 24 de junho; a Majinahanashi tem duas entradas registadas (julho e outubro)

A NOSSA AVALIAÇÃO

As duas entradas da Nova de 24 de junho referem-se à mesma organização, sob um domínio e um nome curto, pelo que as 36 listagens correspondem a no máximo 35 entidades distintas reivindicadas.

CONFIANÇA
Elevada para as contagens registadas; alegações individuais não verificadas

7.3 Contexto de ciberespionagem atribuída oficialmente e perfis hacktivistas

No **RASI 2025**, a **Polícia Judiciária** e o **Serviço de Informações de Segurança (SIS)** avaliam riscos persistentes de ciberespionagem e perturbação estatal contra setores críticos, diplomacia e investigação de uso duplo em Portugal [S5]. As autoridades portuguesas atribuem essas principais ameaças estatais a atores ligados à **Rússia, Coreia do Norte, China e Irão** [S5]. Estas atribuições pertencem estritamente às autoridades portuguesas no RASI 2025; não se acrescenta aqui atribuição estatal própria da Brandefense. A par da espionagem, o **SIS** e a **Eurojust** destacam a pressão contínua de hacktivistas pró-russos contra portais públicos e controladores industriais expostos [S5][S33].

Z-Pentest Alliance

Z-Alliance (designação de canal Telegram)

Canal hacktivista (autodescrito como pró-russo) | Alinhamento pró-russo autodeclarado no seu canal Telegram; o RASI 2025 não refere o grupo

EM PORTUGAL, 2026

Maio de 2026

Alegação de ciberataque contra um controlador industrial de iluminação/automação em Portugal a 11 de maio de 2026, S1

ALVOS ALEGADOS

Controladores de automação industrial e sistemas OT expostos na Internet

EM FONTES PÚBLICAS

[S1] Reenvio em canal Telegram em espanhol de uma reivindicação da Z-Pentest Alliance visando um controlador industrial de iluminação e automação exposto à Internet em Portugal (11 de maio de 2026)

[S5] O capítulo do SIS no RASI 2025 destaca riscos de cibersabotagem por grupos hacktivistas nacionalistas pró-russos contra sistemas industriais e OT em Portugal

A NOSSA AVALIAÇÃO

A reivindicação de maio no Telegram permanece sem confirmação das autoridades portuguesas e sem prova de perturbação física. Contudo, insere-se na classe de alvos descrita pelo SIS no RASI 2025: sistemas de infraestruturas críticas e de gestão industrial e operacional.

CONFIANÇA

Elevada para o registo no Telegram e base do SIS; impacto técnico não verificado

NoName057(16)

Coletivo hacktivista DDoSia

Coletivo hacktivista DDoS pró-russo (atribuição Eurojust) | Alinhamento hacktivista pró-russo conforme indicado pela Eurojust

EM PORTUGAL, 2026

Contexto 2025-2026

Em julho de 2025, uma operação internacional Eurojust/Europol neutralizou mais de 100 servidores e emitiu sete mandados de detenção (S33); o SIS no RASI 2025 assinala risco contínuo de hacktivismo pró-russo contra infraestruturas críticas europeias e portuguesas (S5)

ALVOS ALEGADOS

Portais governamentais, transportes, energia e sítios públicos financeiros nos Estados-Membros da UE e NATO

EM FONTES PÚBLICAS

[S33] Comunicado da Eurojust sobre a operação de 12 países contra a botnet e infraestrutura de mobilização do NoName057(16)

[S5] O RASI 2025 regista um aumento de 36% nos incidentes DDoS do CERT.PT em 2025 a par dos alertas do SIS sobre hacktivismo pró-russo

A NOSSA AVALIAÇÃO

Embora não tenham surgido reivindicações específicas do NoName057(16) contra Portugal no corpus de 2026 após a desarticulação internacional, a subida de 36% em DDoS reportada pelo CERT.PT em 2025 e o ataque volumétrico à MEO em setembro de 2026 evidenciam exposição persistente de disponibilidade.

CONFIANÇA

Elevada para a documentação oficial da Eurojust e do RASI 2025

Os identificadores de técnicas são omitidos onde as fontes públicas citadas não fornecem mapeamento explícito. Tanto a subida do ransomware como a referência do RASI 2025 justificam ação imediata. Atualize equipamentos de perímetro (§12.2), imponha MFA resistente a phishing e teste restauros imutáveis offline.

PRINCIPAIS CONCLUSÕES

01

Os 36 registos de Portugal na Ransompedia subiram 71,4% face a 2025, com 83,3% concentrados entre junho e novembro.

02

The Gentlemen (9) e Qilin (7) concentram quase metade dos registos e correspondem a duas vítimas portuguesas confirmadas em 2026.

03

Mantenha estritamente separadas as etiquetas criminosas, as alegações hacktivistas e as avaliações estatais do RASI 2025.

CAPÍTULO 08

Fraude, abuso de identidade e dano secundário

08

ESTE CAPÍTULO RESPONDE

Como moldam o phishing, o spoofing SMS e os identificadores expostos a economia de fraude em Portugal?

EUR 14,7M

perdas em falsas plataformas de criptoativos em português registadas pela PJ no RASI 2025

8.1 Tendências nacionais de fraude digital no Banco de Portugal, PJ, CNCS e ANACOM 69

8.2 Dano secundário das fugas de dados de 2026 e malware móvel 70

8.3 Publicações observadas de cartões de pagamento: âmbito restrito 70

CAPÍTULO 08

Fraude, abuso de identidade e dano secundário

EM RESUMO

O dano cibernético diário em Portugal centra-se em engenharia social, phishing, spoofing e burlas de investimento. No 1.º semestre de 2025, o Banco de Portugal registou -40,4% nas perdas de pagamentos (EUR 5,3 milhões) com Autenticação Forte e Confirmação de Beneficiário. Porém, a PJ somou EUR 14,7 milhões em burlas cripto, o CERT.PT registou +93% em phishing e a ANACOM viu duplicar as queixas de spoofing até meados de 2025. Ligue cada fuga (NIF, CC, IBAN) a alertas antifraude e bloqueios de spoofing.

8.1 Tendências nacionais de fraude digital no Banco de Portugal, PJ, CNCS e ANACOM

Várias entidades oficiais portuguesas oferecem referências complementares que mostram ganhos defensivos nos pagamentos regulados a par de perdas persistentes em engenharia social:

- **Controlos do Banco de Portugal (relatório de maio de 2026):** No 1.º semestre de 2025, as perdas em pagamentos caíram **40,4%** para **EUR 5,3 milhões** [S12]. A fraude em cartões ficou em **66 casos por milhão** (média **EUR 48**), com a **SCA** a cortar taxas mais de sete vezes (**0,0008%** vs **0,0058%**) [S12]. Transferências somaram **10 por milhão** (**EUR 2 564**) e débitos diretos **4 por milhão** (**EUR 11,50**) [S12].
- **Confirmação de Beneficiário e nova plataforma:** Desde maio de 2024, a **Confirmação de Beneficiário** e o **SPIN** evitaram **EUR 6,5 milhões** e reduziram em **21%** a manipulação do ordenante [S13]. Em **25 de maio de 2026**, abriu a **Plataforma de Acompanhamento da Fraude Digital** [S13][S14].
- **Polícia Judiciária e Ministério Público:** No **RASI 2025**, a **PJ** registou **EUR 14 715 736,21** em falsas plataformas cripto em português e crescimento da burla informática [S5]. O **Gabinete de Cibercrime do Ministério Público** confirmou **+13,16%** nas denúncias por correio eletrónico em 2025 [S8]. Em 2026, a PJ recuperou **EUR 500 000** na **Operação Cryptoclaim** e apoiou as ações contra **Tycoon 2FA** (>160 entidades portuguesas) e **LeakBase** (duas detenções) [S29][S30]. Em **17 de novembro**, a PJ UNC3T deteve ainda dois suspeitos pelo uso fraudulento de cartões bancários franceses clonados acima de **EUR 48 000** [S31].
- **Iscos no CNCS / CERT.PT e ANACOM:** No **RASI 2025**, o CERT.PT registou **+93% em phishing**, **192** Fraudes ao CEO (**+20%**) e **118** falsos empregos [S5]. Somou **99** burlas "Olá Pai / Olá Mãe", **85** de vishing e **ToxicPanda**; em **25 de junho de 2026**, alertou para correios falsos em nome do CNCS [S5][S80]. Até meados de julho de 2025, a **ANACOM** recebeu cerca de **70** queixas de spoofing telefónico e SMS, mais do dobro das cerca de **30** de todo o ano de 2024 [S15]. Cerca de 75% ocorreram no 2.º trimestre de 2025, e o regulador propôs alterações legislativas [S15].

Indicador oficial	Valor	Período e emissor	Relevância operacional
Perdas em fraude de pagamentos	EUR 5,3M (-40,4% homólogo)	1.º sem. 2025 (Banco de Portugal, maio 2026) [S12]	SCA (0,0008% vs 0,0058%) e verificação de beneficiário reduzem perdas nos canais

Indicador oficial	Valor	Período e emissor	Relevância operacional
Fraude evitada via CoP e SPIN	EUR 6,5M (-21% manipulação)	Maio 2024-Maio 2026 (Banco de Portugal) [S13]	Validação do beneficiário em tempo real trava burlas de transferência
Perdas em falsas plataformas cripto	EUR 14 715 736,21	RASI 2025 (Polícia Judiciária) [S5]	Burlas de investimento autorizadas superam amplamente o furto técnico de cartões
Fraude CEO / falso emprego / família	192 / 118 / 99	2025 (CNCS / CERT.PT via RASI 2025) [S5]	Phishing subiu +93%; BEC empresarial e burlas por mensagens alargam-se
Queixas de spoofing de voz e SMS	~70 (vs ~30 em 2024)	Jan. a meados de jul. 2025 vs ano de 2024 (ANACOM) [S15]	Coincide com anúncios ativos de rotas SMS bancárias falsificadas (`B10`)

8.2 Dano secundário das fugas de dados de 2026 e malware móvel

As fugas confirmadas em 2026 expuseram repetidamente identificadores estruturados (`NIF` , Cartão de Cidadão `CC` , `NISS` , `SNS` , `IBAN` , correio eletrónico e telefones). As divulgações abrangidas incluíram **SNS 24** (`>100 000`), **ANEPC RNBP** (`~60 000`), **Metro Mondego**, **Worten**, **SMAS de Sintra** e **Canvas** [S37][S39][S48][S62][S70][S72]. Nenhuma destas fugas expôs palavras-passe bancárias ou cartões de pagamento, mas a combinação de `NIF` , morada e `IBAN` oferece contexto altamente credível para SMS falsificados (`B10`), pretexting telefónico e referências **Multibanco** fraudulentas (`B09`) [S1][S63][S72].

Em **fevereiro de 2026**, a **ThreatFabric** documentou o trojan bancário Android **Massiv**, disfarçado de aplicação IPTV externa dirigida ao ecossistema português **Chave Móvel Digital** [S81]. O malware abusa dos Serviços de Acessibilidade do Android para capturar credenciais e autorizar transferências fraudulentas [S81]. Esta investigação alinha-se diretamente com a recirculação em fóruns a **21 de fevereiro** da mecânica do Massiv e com anúncios ibéricos de verão-outono de kits Android de retransmissão NFC (`Caso G`) [S1].

8.3 Publicações observadas de cartões de pagamento: âmbito restrito

ÂMBITO DOS NÚMEROS DE CARTÕES

Estes números descrevem uma população limitada de publicações observadas nos registos clandestinos retidos. Não estimam o furto de cartões em Portugal, perdas nacionais de fraude nem a validade ativa dos cartões.

Nas publicações clandestinas retidas de 2026, a Brandefense observou **155 ocorrências de cartões de emissores portugueses**, correspondendo a **132 números mascarados distintos** em **114 publicações** [S1]. Estes registos abrangem **51 BIN distintos de seis dígitos** e **6 instituições emissoras portuguesas nomeadas** (identidades omitidas) [S1]. Por rede, **Mastercard** representou **73** registos distintos, **Visa 44** e outras redes **15**; por tipo, **Débito** somou **46**, **Crédito 42** e não especificados **44** [S1].

Um cartão pode surgir em mais do que um espaço: **80** cartões distintos (**89** ocorrências) surgiram em saídas de bots verificadores, **35** (**36** ocorrências) em chats e **21** (**30** ocorrências) em fóruns [S1]. O estado não estava indicado em **72** cartões (**85** ocorrências), erro de rede em **46** (**48**), recusado em **9** (**13**) e aprovado em **9** (**9**) [S1].

Separadamente, **1 776 publicações de oferta** sem números em texto claro mencionaram Portugal, incluindo **1 433 listagens de lotes multipaís de lojas de cartões** [S1]. Nestes lotes, **49** listaram Portugal primeiro, com medianas de **49 países**, **1 485 cartões** e **USD 10 a 25** por cartão [S1].

PRINCIPAIS CONCLUSÕES

01

As perdas em fraude de pagamentos caíram 40,4% no 1.º semestre de 2025, o que o Banco de Portugal associa à SCA, à Confirmação de Beneficiário e ao SPIN. As perdas por engenharia social e burlas cripto continuam elevadas.

02

Registos de NIF, CC e IBAN das fugas de 2026 alimentam diretamente SMS falsificados, referências Multibanco fraudulentas e malware dirigido à Chave Móvel Digital.

03

Trate os 132 registos observados de cartões como um sinal restrito de publicação, nunca como medida do furto nacional.

CAPÍTULO 09

Banca, pagamentos e resiliência da identidade digital

ESTE CAPÍTULO RESPONDE

Qual é a exposição externa do setor financeiro português e onde são mais fortes os controlos operacionais?

51

incidentes TIC graves ao abrigo do DORA reportados ao Banco de Portugal em 2025 (+16 homólogo)

9.1 Agregados de exposição do setor bancário (sem nomes nem pontuações) 73

9.2 Abuso de canais nacionais, Chave Móvel Digital e continuidade DORA 74

CAPÍTULO 09

Banca, pagamentos e resiliência da identidade digital

EM RESUMO

A banca portuguesa lidera a higiene de domínios, com 24 de 25 a aplicar DMARC e 21 de 22 servidores acessíveis com HSTS. Contudo, 13 de 25 domínios apresentavam anúncios ativos de credenciais e 99,1% dos dispositivos pertencem a não colaboradores. Em 2025, o Banco de Portugal registou 51 incidentes DORA graves (1,3 milhões de utilizadores), enquanto criminosos anunciam rotas SMS bancárias falsas e contas mula. Separe a contenção interna das filas de fraude e teste continuamente o DORA.

9.1 Agregados de exposição do setor bancário (sem nomes nem pontuações)

No retrato de **27 de novembro de 2026**, todos os **25 domínios** da célula portuguesa de **Banca e finanças** foram avaliados tanto em configuração passiva como em exposição Atlas [S3][S4]. Todos os valores abaixo são estritamente agregados da célula ou subconjunto; **nenhum banco individual é nomeado** e **nenhuma pontuação Atlas setorial ou de grupo é publicada**:

- **Melhor higiene de correio e transporte em Portugal:** Vinte e quatro de 25 domínios bancários (**96,0%**) aplicam DMARC (**16** `reject`, **8** `quarantine`, `1` `p=none`, `0` em falta) [S3][S82]. Nos servidores acessíveis, **22 de 23** mantêm certificados TLS de raiz válidos e **21 de 22** (**95,5%**) publicam HSTS [S3][S85].
- **Célula completa de 25 domínios de Banca e finanças:** Treze de 25 domínios (**52,0%**) apresentavam um anúncio ativo de credenciais na verificação [S4]. Vinte e quatro de 25 apresentavam **50 346** associações acumuladas de dispositivos: **429** de colaboradores (**0,9%**) face a **49 917** não colaboradores (**99,1%**) [S4]. Todos os **25** apresentavam **119 409** credenciais históricas (`63 836` em bases de fugas, `46 279` em combolists, `9 294` em infostealers), enquanto **23** somaram **2 374** nomes semelhantes e os documentos totalizaram **53** [S4].
- **Subconjunto estrito de 15 bancos emissores de cartões identificados:** Dentro da célula, **10 de 15** instituições emissoras tinham anúncio ativo na verificação [S4]. Catorze de 15 apresentaram **34 341** dispositivos não colaboradores (os três maiores representam **56,4%**), e **13 de 15** apresentaram **327** dispositivos de colaboradores [S4]. Seis emissores corresponderam a **86** cartões mascarados atribuídos na secção §8.3 (os três maiores com **79,1%**) [S1]. Os dispositivos não colaboradores refletem equipamentos infetados de consumidores, e não intrusões bancárias, e os cartões observados não estabelecem qualquer ordenação de segurança entre emissores.

Questão do setor bancário	Sinal agregado observado (27 nov 2026)	Responsável
Os domínios bancários portugueses aplicam DMARC e HSTS?	24 de 25 com DMARC restritivo (96,0%); 21 de 22 acessíveis com HSTS (95,5%) [S3]	Segurança de correio e domínios
Quantos domínios financeiros têm anúncios ativos de credenciais?	13 de 25 domínios financeiros (10 de 15 no subconjunto emissor) [S4]	Operações de identidade e SOC
Os registos de dispositivos pertencem a colaboradores ou clientes?	50 346 no total: 429 colaboradores (0,9%) vs 49 917 não colaboradores (99,1%) [S4]	Contenção interna vs fraude de retalho
Que serviços clandestinos visam clientes bancários em Portugal?	Rotas SMS falsificadas (`B10`), drops EUR 2K-10K (`B08`), ferramentas Multibanco (`B09`), 55K contactos (`B12`) [S1]	Operações antifraude e proteção de marca
Um BIN observado ou lista de contactos comprova intrusão bancária?	Não; nem registos BIN nem listas comerciais comprovam intrusão em banco [S1]	Triagem SOC e inteligência antifraude

9.2 Abuso de canais nacionais, Chave Móvel Digital e continuidade DORA

A banca de retalho portuguesa assenta em canais nacionais estreitamente interligados (**SIBS**, **Multibanco**, **MB WAY**, **SPIN**) e na identidade digital nacional (**Chave Móvel Digital**). As publicações clandestinas de 2026 visaram as bordas humanas e de telecomunicações dessa arquitetura, e não os sistemas centrais de compensação. A atividade abrangeu recrutamento KYC em Portugal (`USD 30`), contas bancárias de receção para **EUR 2 000-10 000** (`B08`) e gateways SMS falsificados (`B10`) [S1]. Os atores promoveram também ferramentas de referências Multibanco (`B09`) e trojans Android (`Massiv` , `ToxicPanda`) visando fluxos de assinatura móvel [S1][S5][S81].

O Relatório dos Sistemas de Pagamentos 2025 do **Banco de Portugal** sublinhou também a continuidade operacional como risco prioritário de administração [S12]. As entidades supervisionadas reportaram **51 incidentes DORA graves em 2025** (**+16** homólogo), afetando **1,3 milhões de utilizadores** [S12]. O valor transacionado atingido somou **EUR 2,4 mil milhões** (**EUR 751 milhões** excluindo o TARGET) [S12].

Ao abrigo da **Lei n.º 73/2025**, o **Banco de Portugal** atua como ponto único de receção DORA para instituições de crédito e pagamento, a par da **CMVM** e da **ASF** [S25]. Os CISO financeiros devem ensaiar três cenários DORA: degradação de telecomunicações em picos Multibanco/MB WAY, vagas de trojans Android visando a `Chave Móvel Digital` e deteção rápida de contas mula recentes.

PRINCIPAIS CONCLUSÕES

01

A banca lidera Portugal em DMARC (24/25) e HSTS (21/22), mas 13 de 25 domínios avaliados apresentam anúncios ativos que exigem triagem rápida.

02

Dispositivos não colaboradores representam 99,1% dos registos bancários, separando malware de clientes da contenção de contas internas.

03

Cinquenta e um incidentes DORA graves em 2025 mostram que a resiliência TIC e de terceiros exige a mesma prioridade executiva que o combate à fraude.

CAPÍTULO 10

10

Regulação, prazos de notificação e resposta nacional

ESTE CAPÍTULO RESPONDE

Que autoridade, portal e prazo legal se aplicam em Portugal perante um incidente em 2026?

3 de abril de 2026

Entrada em vigor do Decreto-Lei n.º 125/2025 (transposição NIS2) em Portugal

10.1 Enquadramento legal português em 2026 77

10.2 Prazos e destinatários distintos em Portugal 78

10.3 Lições práticas de conformidade nos incidentes portugueses de 2026 79

CAPÍTULO 10

Regulação, prazos de notificação e resposta nacional

EM RESUMO

Cinco quadros legais regem as notificações cibernéticas e de privacidade em Portugal em 2026. O Decreto-Lei n.º 125/2025 (NIS2, 3 de abril) e o Regulamento n.º 756/2026 do CNCS (MyCiber, 23 de junho) coexistem com a Lei n.º 73/2025 (DORA sob o Banco de Portugal, CMVM e ASF). O RGPD sob a Lei n.º 58/2019 (CNPD) e as obrigações do Regulamento da Ciber-Resiliência da UE (11 de setembro de 2026) correm em prazos separados. Registe-se no MyCiber, designe os responsáveis obrigatórios e registe separadamente a deteção e a classificação.

10.1 Enquadramento legal português em 2026

Cinco quadros normativos articulados definem a responsabilização executiva, os prazos de notificação e as prioridades de conformidade em Portugal em 2026:

- **Regime Jurídico da Cibersegurança (Decreto-Lei n.º 125/2025, de 4 de dezembro, em vigor desde 3 de abril de 2026):** Transpõe a NIS2 em 17 setores e na administração pública [S22]. Designa o **Centro Nacional de Cibersegurança (CNCS)** como Autoridade Nacional de Cibersegurança [S5][S22]. O artigo 42.º fixa um alerta inicial em **24 horas**, uma atualização em **72 horas** e um relatório final em **1 mês** [S22]. As coimas administrativas máximas atingem EUR 10 milhões ou 2% do volume de negócios mundial para entidades essenciais, e EUR 7 milhões ou 1,4% para entidades importantes [S22].
- **Regulamento de Execução do CNCS (Regulamento n.º 756/2026, em vigor desde 23 de junho de 2026):** Operacionaliza a plataforma **MyCiber**, definindo regras de autoidentificação e qualificação com audiência prévia de 10 dias úteis [S23][S24]. As entidades devem designar um **Responsável de Cibersegurança** e um **Ponto de Contacto Permanente** [S23]. As medidas mínimas alinham-se com o **QNRCS**, com períodos de adaptação faseada até 24 meses [S23][S24].
- **Execução Nacional do DORA (Lei n.º 73/2025) e Regulamento Delegado (UE) 2025/301:** Distribui a supervisão do DORA entre o **Banco de Portugal**, a **CMVM** e a **ASF** [S25]. O Banco de Portugal funciona como ponto único de receção de incidentes TIC graves para instituições de crédito e pagamento [S25]. O artigo 5.º do Regulamento Delegado (UE) 2025/301 fixa prazos estritos de notificação [S27].
- **RGPD e Lei n.º 58/2019 (8 de agosto):** Designa a **Comissão Nacional de Proteção de Dados (CNPD)** como autoridade de controlo, aplicando o prazo de 72 horas para violações de dados pessoais [S26]. Em **15 de janeiro de 2026**, a **CNPD** e o **CNCS** assinaram um protocolo de cooperação criando um canal de emergência 24/7, auditorias conjuntas e um roteiro para um portal interoperável de entrada única [S9]. A cobertura pública assinalou ainda restrições de pessoal na CNPD: abriram-se **472** processos de violação em 2025 (**+42%** homólogo), mas apenas **duas coimas RGPD totalizando EUR 47 000** foram aplicadas no ano [S9][S10][S11].

- **Regulamento da Ciber-Resiliência (UE 2024/2847):** Pelos artigos 14.º e 71.º, a notificação por fabricantes de **vulnerabilidades ativamente exploradas** e **incidentes graves** entrou em vigor em **11 de setembro de 2026** [S28]. Os deveres gerais de conformidade aplicam-se a partir de **11 de dezembro de 2027** [S28].

10.2 Prazos e destinatários distintos em Portugal

Um único ciberincidente aciona frequentemente várias notificações legais em simultâneo. O resumo operacional seguinte sintetiza gatilhos e prazos principais em Portugal (orientação geral, não constitui aconselhamento jurídico):

Regime	Gatilho principal	Sequência principal de notificação	Destinatário competente em Portugal
Regime Jurídico da Cibersegurança (`DL 125/2025` , `Reg. 756/2026`)	Incidente significativo numa entidade essencial ou importante em 17 setores ou administração pública	Alerta inicial em **24 horas** após conhecimento; atualização em **72 horas**; relatório intercalar a pedido e relatório final em **1 mês** (artigo 42.º) [S22][S23]	**CNCS / CERT.PT** via plataforma **MyCiber** e autoridades setoriais designadas [S22] [S23]
RGPD e `Lei n.º 58/2019`	Violação de dados pessoais salvo improbabilidade de risco para direitos e liberdades	Notificar em **72 horas** após conhecimento sempre que viável; avisar titulares sem demora injustificada em caso de elevado risco [S26]	**CNPD** (Comissão Nacional de Proteção de Dados) [S9] [S26]
DORA (`Lei 73/2025` , Reg. UE `2022/2554` , Reg. Del. `2025/301` art. 5.º)	Incidente TIC grave numa entidade financeira abrangida	Notificação inicial em **4 horas** após classificação como grave e no máximo **24 horas** após deteção; intercalar em **72 horas**; final em **1 mês** [S25][S27]	**Banco de Portugal** (ponto único para instituições de crédito e pagamento), **CMVM** ou **ASF** [S25]
Regulamento da Ciber-Resiliência (Reg. UE `2024/2847` , arts. 14.º e 71.º)	Conhecimento pelo fabricante de **vulnerabilidade ativamente explorada** ou **incidente grave** num produto digital (desde **11 de setembro de 2026**)	Alerta inicial em **24 horas**; notificação em **72 horas**; relatório final em **14 dias** (vulnerabilidades após correção) ou **1 mês** (incidentes graves) [S28]	CSIRT coordenador (**CERT.PT**) e **ENISA** em simultâneo via Plataforma Única CRA [S28]
Investigação criminal	Suspeita de acesso ilegítimo, ransomware, sabotagem ou burla informática	Participação criminal célere preservando evidências forenses voláteis e registos [S5][S29][S39]	**Polícia Judiciária (UNC3T)** e **Ministério Público (Gabinete de Cibercrime)** [S5][S8] [S29]

Ao abrigo do artigo 5.º do Regulamento Delegado (UE) 2025/301 do DORA, entidades impossibilitadas de cumprir um prazo devem informar a autoridade antes do termo apresentando razões documentadas [S27]. O diferimento de fim de semana não dispensa instituições de crédito, contrapartes centrais, plataformas de negociação nem entidades financeiras essenciais ou importantes NIS2 das notificações iniciais e intercalares [S27].

10.3 Lições práticas de conformidade nos incidentes portugueses de 2026

Três lições práticas destacam-se nas 20 divulgações confirmadas em Portugal em 2026. Primeiro, **a notificação multiautoridade tornou-se rotina**. **Serpa**, **Santo Tirso**, **Metro Mondego**, **Universidade de Aveiro**, **Grupo Águas de Portugal** e **Worten** notificaram o **CNCS**, a **CNPD** e a **Polícia Judiciária** [S45][S47][S50][S52][S53][S68]. Os **SMAS de Sintra** notificaram a **CNPD** e o **CNCS** [S72].

Segundo, **os fornecedores não eliminam deveres do responsável pelo tratamento**, como mostraram **Canvas** (`Caso I`), o **subcontratado web do SIRP** (`Caso Q`) e o **fornecedor de frio do Intermarché** (`Caso S`) [S37][S58][S64]. Terceiro, **publicações clandestinas não verificadas não são gatilhos automáticos de notificação**: valide o impacto técnico nos sistemas reais e registe a decisão.

PRINCIPAIS CONCLUSÕES

01

O regime NIS2 em Portugal (DL 125/2025 e Reg. 756/2026), o DORA (Lei 73/2025), o RGPD (CNPD) e o CRA da UE correm em prazos distintos.

02

Conclua a qualificação no MyCiber, nomeie o Responsável de Cibersegurança e o Ponto de Contacto Permanente e valide credenciais de reserva agora.

03

Registos clandestinos não verificados exigem triagem forense antes de acionar notificações legais formais.

CAPÍTULO 11

11

Perspetivas e cenários condicionais de planeamento

ESTE CAPÍTULO RESPONDE

Que sinais concretos devem ajustar a postura defensiva em Portugal após 26 de novembro de 2026?

4

cenários condicionais de planeamento assentes em evidência própria

11.1 Juízos principais e limites de evidência 81

11.2 Quatro cenários condicionais de planeamento 82

11.3 O que alteraria esta avaliação 83

CAPÍTULO 11

Perspetivas e cenários condicionais de planeamento

EM RESUMO

A evidência portuguesa de 2026 exige prontidão em quatro frentes: ransomware em autarquias e saúde, proteção de registos nacionais, controladores OT remotos e engenharia social com NIF e IBAN expostos. Não estabelece um ator único coordenado nem prevê probabilidades de ataque. Associe cada cenário condicional seguinte a planos pré-aprovados de isolamento técnico, notificação legal e comunicação pública.

11.1 Juízos principais e limites de evidência

Juízo	Base e confiança	Limite principal	Decisão atribuída
Municípios, universidades e saúde mantêm a exposição operacional mais aguda a ransomware em Portugal	Elevada com base nos ataques confirmados (`Casos H, K, L, N, R`), baixa aplicação DMARC (`48%-56 %`) e RASI 2025 [S3][S5] [S43][S47][S51]	Várias encriptações municipais confirmadas nunca surgiram em sites de extorsão; a maturidade setorial varia amplamente	Partilhar monitorização SOC municipal 24/7 via **FCSAL**, testar restauros offline e aplicar DMARC
A extração em massa de registos e falhas em formulários públicos geram grave fraude secundária	Elevada com base em **SNS 24** (`>100 000`), **ANEPC RNBP** (`~60 000`), **Worten**, **SMAS de Sintra** e **Metro Mondego** [S39][S48][S62] [S70][S72]	As populações expostas sobrepõem-se de forma desconhecida entre responsáveis distintos e não podem ser somadas	Impor limites de consulta, MFA resistente a phishing e correção rápida de formulários
TI de fornecedores externos e controladores OT remotos criam choques transfronteiriços em Portugal	Elevada com base em **Intermarché** (7 lojas), **Instructure Canvas** e subcontratado do **SIRP** [S37][S58][S64]	A exposição de terceiros depende da higiene individual de acesso remoto de cada fornecedor	Retirar controladores OT de terceiros da Internet pública e auditar servidores de testes
A pressão em portais de extorsão acelerou fortemente no 2.º semestre de 2026 (`83,3%` em jun-nov)	Elevada para os **36** registos da Ransompedia em 17 etiquetas (+71,4% face a 21 em 2025) [S2]	**34 de 36** registos permanecem não verificados; uma duplicação da Nova limita entradas únicas a no máximo 35	Validar cada registo face a logs forenses internos antes de negociar ou notificar

Juízo	Base e confiança	Limite principal	Decisão atribuída
Os controlos nos pagamentos reduzem fraude em cartões enquanto crescem burlas cripto e engenharia social	Elevada com base no **Banco de Portugal** (`-40,4%` perdas 1.º sem. 2025; `EUR 6,5M` evitados) vs **PJ** (`EUR 14,7M` burlas cripto), spoofing **ANACOM** e anúncios SMS [S1][S5][S12][S13][S15]	Anúncios clandestinos não medem taxas de conversão nem perdas concretas por banco	Combinar defesa de remetentes SMS e telemetria de trojans Android com alertas direcionados a clientes
A exposição externa de identidade nos 247 domínios avaliados exige triagem separada de colaboradores e clientes	Elevada para o indicador nacional **51/100**, **83** anúncios ativos e **202** domínios com dispositivos de colaboradores [S4]	Sinais acumulados não estabelecem intrusão em 2026 nem prevalência nacional; 3 de 250 domínios permanecem desconhecidos	Validar anúncios ativos em cinco dias úteis e separar filas de colaboradores das de clientes

11.2 Quatro cenários condicionais de planeamento

Cenário A: Uma rede municipal, universitária ou de saúde deteta encriptação ativa ou desfiguração de portal

Caso a monitorização detete encriptação rápida de ficheiros (`Casos H, K, L, N, R`) ou desfiguração de gestor de conteúdos público (`Caso U`), acione de imediato o isolamento de rede pré-autorizado. Mantenha cuidados clínicos ou serviços municipais essenciais em contingência segmentada. Preserve memória volátil e registos de firewall para a **Polícia Judiciária (UNC3T)** e notifique o **CNCS / CERT.PT** em 24 horas sob o **DL 125/2025** se aplicável. Emita despachos de suspensão de prazos municipais quando necessário (`Caso H`) e restaure apenas a partir de cópias imutáveis offline verificadas.

Cenário B: Velocidade anómala de consultas ou exploração de formulário atinge uma base de cidadãos ou clientes

Caso os registos revelem consultas em massa a partir de uma única conta clínica, interna ou API (`Caso J`) ou exploração de formulário web (`Casos R, T`), revogue de imediato as sessões ativas. Bloqueie os pontos de exportação em massa e apure os campos exatos expostos (`NIF` , `CC` , `IBAN`). Submeta notificações paralelas à **CNPD** (72h) e ao **CNCS** consoante aplicável, publicando alertas simples contra phishing, smishing e falsas referências Multibanco com esses dados.

Cenário C: Um anúncio clandestino, combolist ou registo na Ransompedia nomeia uma organização portuguesa

Se a monitorização sinalizar uma base em fórum (`Casos A, B, E`), acesso inicial (`Caso D`) ou extorsão (§7.1), valide primeiro os dados [S1]. Compare esquemas, datas de registo e credenciais face à produção e arquivos históricos. Confirme se reciclagem histórica (`Caso B`), textos-modelo (`Caso A`) ou logs de infostealers de utilizadores explicam a publicação antes de acionar comunicados de crise ou redefinições globais de palavras-passe.

Cenário D: Controladores OT geridos por fornecedores ou ligações internacionais sofrem perturbação súbita

Caso a telemetria local detete desvios anómalos de temperatura ou regulação em controladores de frio, energia ou edifícios (`Caso S` ; §6.2), desligue de imediato as ligações remotas de fornecedores. Passe para controlo manual seguro local e alerte o **CNCS** e a **PJ**. Caso DDoS volumétrico degrade a conectividade externa (`Caso P`), acione mitigação no operador a montante e publique boletins factuais datados sem especular sobre causas cibernéticas em falhas não investigadas (§6.3).

11.3 O que alteraria esta avaliação

Atribuição forense confirmada ligando várias intrusões municipais ou de portais públicos de 2026 (`Casos H, K, R, U`) a um único intermediário de acesso ou cadeia de vulnerabilidades justificaria elevar alertas coordenados multissetoriais. Confirmação de credenciais internas ativas não mitigadas entre os **83 domínios** com anúncios correntes, ou observações de exposição para os **3 domínios não avaliados**, afinaria também a priorização setorial. Inversamente, a adesão alargada ao **MyCiber** e a migração dos **87 domínios sem DMARC restritivo** para DMARC `quarantine` ou `reject` reduziriam materialmente o risco de falsificação. A aprovação das regras contra spoofing telefónico e SMS propostas pela **ANACOM** limitaria ainda mais a fraude doméstica.

PRINCIPAIS CONCLUSÕES

01

Vincule cada juízo estratégico ao respetivo limite de evidência para concentrar orçamentos em lacunas verificadas.

02

Pré-autorize isolamento, bloqueio de consultas em massa, triagem de alegações e controlo manual OT antes de um incidente.

03

Acompanhe a adesão ao MyCiber, a aplicação de DMARC e as regras anti-spoofing da ANACOM como indicadores de progresso nacional.

CAPÍTULO 12

Plano de ação e evidências de conclusão

12

ESTE CAPÍTULO RESPONDE

Quem atua, perante que sinal e o que demonstra que cada controlo funciona na prática?

30 / 60 / 90

marcos de verificação; correções urgentes de perímetro e triagem ativa começam hoje

12.1 Faixas prioritárias de ação e evidências de conclusão 85

12.2 Referência de correção de vulnerabilidades 87

12.3 Apoio à validação externa contínua 88

CAPÍTULO 12

Plano de ação e evidências de conclusão

EM RESUMO

A correção urgente de equipamentos de perímetro e portais PHP, a retirada de controladores OT de fornecedores da Internet pública e a validação de anúncios ativos de credenciais começam hoje. Use os marcos de 30, 60 e 90 dias seguintes para atribuir responsáveis técnicos e executivos em Portugal. Exija evidência operacional testada em vez de políticas em papel para concluir cada medida.

12.1 Faixas prioritárias de ação e evidências de conclusão

1**Imediato (0-7 dias)**

Inventariar todos os gateways expostos, soluções de suporte remoto, portais PHP/CMS e controladores OT/frio de terceiros; aplicar versões corrigidas da §12.2, cortar acesso direto pela Internet a OT de fornecedores e pré-autorizar isolamento rápido de DMZ

RESPONSÁVEL

Infraestrutura, engenharia OT e CISO

EVIDÊNCIA DE CONCLUSÃO

Registo assinado de ativos externos, comprovativos de atualização e manual aprovado de isolamento

Validar qualquer anúncio ativo de credenciais (**83 de 247** domínios avaliados) em cinco dias úteis; auditar Microsoft 365 e inquilinos cloud (`126 de 250` domínios da carteira) para sessões **Tycoon 2FA**, regras de reencaminhamento anómalas e permissões OAuth

RESPONSÁVEL

Identidade e liderança SOC

EVIDÊNCIA DE CONCLUSÃO

Registo datado de triagem de anúncios, logs de sessões revogadas e exportação de políticas MFA

2**30 dias**

Reconciliar associações de dispositivos de colaboradores (**202** domínios avaliados, **38 013** dispositivos) face ao inventário gerido para isolar máquinas internas infetadas, encaminhando dispositivos externos para equipas antifraude

RESPONSÁVEL

Segurança de endpoints e operações antifraude

EVIDÊNCIA DE CONCLUSÃO

Registo reconciliado de triagem com datas de contenção ou encerramento documentado

Migrar domínios sem DMARC restritivo (**87 de 250**, liderados por autarquias, universidades e saúde) para DMARC `quarantine` ou `reject`, corrigir as **20** falhas TLS de raiz e ativar HSTS nos portais públicos restantes

RESPONSÁVEL

Segurança de correio e domínios

EVIDÊNCIA DE CONCLUSÃO

Verificação DNS ao vivo de DMARC e relatório externo limpo de TLS/HSTS nos domínios próprios

Concluir a autoidentificação e qualificação no **MyCiber** sob o **Regulamento n.º 756/2026**, nomear o **Responsável de Cibersegurança** e o **Ponto de Contacto Permanente**, e validar acessos paralelos para **CNCS**, **CNPD**, **Banco de Portugal / CMVM / ASF** (se DORA) e **PJ UNC3T**

RESPONSÁVEL

Jurídico, conformidade e CISO

EVIDÊNCIA DE CONCLUSÃO

Comprovativo datado do MyCiber, nomeações formais e lista testada de acessos aos portais

3**60 dias**

Implementar limites de velocidade de consulta por conta, alertas de exportação anómala e MFA resistente a phishing em registos nacionais, municipais e de saúde (`Casos J, R`); minimizar `NIF` / `IBAN` em formulários web e proibir dados reais em servidores de testes de subcontratados (`Casos Q, T`)

RESPONSÁVEL

Engenharia aplicacional, EPD e risco de terceiros

EVIDÊNCIA DE CONCLUSÃO

Registo de teste de limitação de consultas, revisão de formulários e auditoria assinada de subcontratados

Em plataformas financeiras e de consumo, alinhar bloqueios de spoofing SMS com orientações da **ANACOM**, detetar abuso de Acessibilidade Android dirigido à **Chave Móvel Digital** (`Massiv` / `ToxicPanda`) e reforçar provas de vida e alertas de contas mula recentes

RESPONSÁVEL

Operações antifraude e canais digitais

EVIDÊNCIA DE CONCLUSÃO

Relatório assinado de testes antifraude e revisão de telemetria móvel e de operadoras

4**90 dias**

Realizar exercício conjunto de continuidade e teste real de reposição offline integral (alinhado com **DL 125/2025**, **DORA** ou modelo municipal **CIBER 26**), cobrindo isolamento TI/OT, suspensão legal de prazos e boletins baseados em telemetria

RESPONSÁVEL

Patrocinador executivo, continuidade e CISO

EVIDÊNCIA DE CONCLUSÃO

Relatório pós-exercício datado, tempos medidos de recuperação e registo assinado de risco residual

12.2 Referência de correção de vulnerabilidades

A tabela seguinte reúne versões afetadas e corrigidas verificadas diretamente nos registos **NIST NVD** e **CVE CNA** em **27 de novembro de 2026**. Abrange equipamentos de perímetro, motores web PHP e plataformas destacadas pelo CERT.PT relevantes para Portugal. Atualizações cumulativas posteriores substituem versões mínimas anteriores em ramos suportados:

Produto e CVE	Versões afetadas (NVD / CNA)	Versões corrigidas e ação defensiva	Fontes
BeyondTrust Remote Support / PRA (`CVE-2026-1731` CVSS 3.1 `9.8` ; `CVE-2026-102764` CVSS 3.1 `9.8`)	`CVE-2026-1731` : Remote Support (`RS`) `⩽ 25.3.1` e Privileged Remote Access (`PRA`) `⩽ 24.3.4` . `CVE-2026-102764` : Remote Support `⩽ 26.2.3` .	Atualizar o **Remote Support** para versão posterior a `26.2.3` (cobrindo RCE pré-autenticação de fevereiro e validação de origem de outubro) e o **PRA** para versão posterior a `24.3.4` ; procurar persistência anterior e rodar credenciais de serviço.	[S86][S88]
Citrix NetScaler ADC e Gateway (`CVE-2026-88771` CVSS 3.1 `9.8` ; `CVE-2026-88772` CVSS 3.1 `8.1` ; substituídas por `CVE-2026-120868` CVSS 4.0 `9.3`)	Versões de setembro: `14.1` anterior a `14.1-73.37` , `13.1` anterior a `13.1-64.23` , `14.1` FIPS anterior a `14.1-73.37` FIPS, `13.1` FIPS/NDcPP anterior a `13.1-37.279` . Novembro (`CVE-2026-120868`): `14.1` anterior a `14.1-73.57` , `13.1` anterior a `13.1-64.39` , `14.1` FIPS anterior a `14.1-73.58` FIPS, `13.1` FIPS/NDcPP anterior a `13.1-37.293` .	Atualizar diretamente para `14.1-73.57` , `13.1-64.39` , `14.1-73.58` FIPS ou `13.1-37.293` FIPS/NDcPP (ou posteriores suportadas); migrar equipamentos em fim de vida, procurar persistência pré-correção e rodar segredos de sessão.	[S87][S91]
Ivanti Connect Secure (`CVE-2026-104935` CVSS 3.1 `8.6`)	Versões ICS `22.8R2` a `22.8R2.4` e `25.1.x` anteriores a `25.1.3.0` ; `22.8R2.5` , `22.7R2.14` e anteriores não são afetadas.	Atualizar equipamentos `ICS` expostos para `25.1.3.0` (ou compilações `25.1.3` posteriores) ou `22.8R2.5` (ou posteriores suportadas); verificar MFA na VPN e auditar registos quanto a spoofing.	[S89]

Produto e CVE	Versões afetadas (NVD / CNA)	Versões corrigidas e ação defensiva	Fontes
Motor Web PHP (`CVE-2026-109618` CVSS 3.1 `9.8` ; `CVE-2026-109619` CVSS 3.1 `8.1` ; substituídas em 19 nov por `CVE-2026-115560` e `CVE-2026-129289` CVSS 4.0 `9.2`)	Falhas de outubro: `8.2` anterior a `8.2.35` , `8.3` anterior a `8.3.36` , `8.4` anterior a `8.4.27` , `8.5` anterior a `8.5.12` (mais ramos em fim de vida). Falhas de novembro (`CVE-2026-115560` RCE em serialização de sessão; `CVE-2026-129289` contrabando de pedidos PHP-FPM): `8.2` anterior a `8.2.36` , `8.3` anterior a `8.3.37` , `8.4` anterior a `8.4.28` , `8.5` anterior a `8.5.13` .	Atualizar diretamente para `8.5.13` , `8.4.28` , `8.3.37` ou `8.2.36` (ou correções LTS suportadas); migrar ramos `8.1` e anteriores (o `8.2` atinge fim de vida em 31 de dezembro de 2026). Definir `session.upload_progress.enabled=0` na configuração do servidor/FPM e alinhar serializadores de sessão partilhados.	[S90][S92]
Microsoft SharePoint Server e DNN CMS (`CVE-2025-53770` CVSS 3.1 `9.8` ; `CVE-2025-64095` NVD Primary CVSS 3.1 `9.8` / CNA `10.0`)	Microsoft SharePoint Server local vulnerável a RCE de desserialização (`CVE-2025-53770`); DNN CMS anterior a `10.1.1` (`CVE-2025-64095`). Ambas destacadas pelo **CERT.PT** no **RASI 2025** entre as falhas mais exploradas em Portugal.	Confirmar atualizações cumulativas do Microsoft SharePoint e rotação de chaves de máquina para `CVE-2025-53770` ; atualizar o DNN CMS para `10.1.1` ou posterior e auditar pastas públicas quanto a carregamentos indevidos.	[S5][S93]

12.3 Apoio à validação externa contínua

Organizações que pretendam visibilidade específica sobre exposição de domínios portugueses, alertas de credenciais de infostealers, nomes semelhantes e alegações clandestinas sobre a sua marca podem solicitar uma apresentação em Pedido de demonstração Brandefense [S94].

PRINCIPAIS CONCLUSÕES

01

Corrija gateways expostos e portais PHP, isole controladores OT de fornecedores e valide anúncios ativos de credenciais de imediato.

02

Conclua a qualificação no MyCiber e feche a lacuna de 87 domínios sem DMARC restritivo em 30 dias.

03

Exija evidências datadas de recuperação, limitação de consultas e continuidade para concluir cada marco.

APÊNDICES

Apêndices

A–D

ESTE CAPÍTULO RESPONDE

Apêndice A. Método, âmbito e exclusões · Apêndice B. Registo de evidências · Apêndice C. Fontes · Apêndice D. Glossário

94

fontes

Apêndice A. Método, âmbito e exclusões 90

Apêndice B. Registo de evidências 93

Apêndice C. Fontes 94

Apêndice D. Glossário 100

Apêndice A. Método, âmbito e exclusões

Os países de comparação foram selecionados como exemplos apenas para fornecer contexto; a sua escolha não implica uma classificação nem uma avaliação política.

A.1 Janelas de observação e separação de evidências

Datas de referência distintas aplicam-se ao longo deste relatório sem nunca se confundirem. A **janela de atividade de 2026** decorre de **1 de janeiro a 26 de novembro de 2026** (UTC, data de publicação) [S1][S2]. Abrange observações clandestinas, registos Ransompedia, menções de domínios em 2026 e incidentes públicos [S1][S2][S4]. Dentro dessa janela, o período de **12 a 26 de novembro de 2026** é analisado separadamente na secção §5.3 e não implica vigilância mais longa [S1][S2]. As menções móveis a 365 dias em chats e fontes da dark web decorrem de **27 de novembro de 2025 a 26 de novembro de 2026**, reportadas separadamente do subconjunto de 2026 [S4].

As observações de exposição Brandefense Atlas (**247 de 250** domínios selecionados) e as configurações passivas (**todos os 250** domínios) refletem um retrato de **27 de novembro de 2026** [S3][S4]. Todos os avisos públicos, diplomas, PDF oficiais, registos NVD e fontes jornalísticas foram verificados em **27 de novembro de 2026**. Cada fonte sustenta exclusivamente a sua proposição.

A.2 Volume clandestino e limite da recolha

A população observada com etiqueta Portugal totaliza **744 809 publicações** entre 1 de janeiro e 26 de novembro de 2026 [S1]. Janeiro (`411 861`) e fevereiro (`316 130`) concentram **727 991 publicações (97,7%)**, impulsionadas por tráfego promocional multipaís em turco no Telegram (`723 945` em jan-fev; `724 031` na janela completa) [S1].

De março a novembro somam-se **16 818 publicações** (`16 716` Telegram, `82` fórum, `14` sites de texto, `6` Discord) [S1]. A janela recente (**12 a 26 de novembro**) reúne **715** publicações com etiqueta Portugal e **25** publicações em fóruns que mencionam Portugal em tópicos com e sem etiqueta de país [S1]. Os excertos (`B01` - `B15`) provêm de um acervo retido mais estreito e não representam um censo integral. Novembro é parcial até dia 26.

A.3 Carteira de 250 domínios selecionados e retrato de configuração passiva

A carteira passiva reúne **250 domínios portugueses com resolução DNS**, distribuídos igualmente por dez células setoriais de **25 domínios**, recolhidos em **27 de novembro de 2026** [S3]. A seleção é intencional entre grandes instituições públicas e privadas portuguesas e não constitui censo estatístico dos domínios `.pt` . Os valores de autenticação de correio refletem categorias publicadas (`reject` , `quarantine` , `none` , em falta) e não comportamento verificado dos recetores (`RFC 7489`) [S3][S82]. TLS (`217/237` válidos) e HSTS (`164/212` presentes) preservam denominadores acessíveis; servidores inacessíveis (`13` TLS, `38` HTTP) são contados à parte e não como falhas [S3].

A.4 Avaliações de exposição dos domínios selecionados e menções

As observações de exposição Brandefense Atlas abrangem **247 dos 250 domínios selecionados** no retrato de **27 de novembro de 2026** [S4]. A exposição permanece **desconhecida** em **3 domínios selecionados** (1 em Energia e serviços públicos, 1 em Indústria e manufatura, 1 em Transportes, marítimo e logística); domínios não avaliados nunca são tratados como zero [S4]. Publica-se apenas o indicador nacional Atlas único (**51/100**); não existem pontuações, medianas ou classificações por setor, grupo ou organização neste relatório.

Os sinais incluem **83** domínios com anúncios ativos de credenciais (**2 621** registos históricos) e pelo menos **523 733** associações acumuladas de dispositivos (**38 013** de colaboradores em **202** domínios) [S4]. Os domínios avaliados reúnem ainda **13 777 936** credenciais históricas (**238** domínios), **801** documentos (**137** domínios) e **40 060** nomes semelhantes a 30 dias (**191** domínios) [S4]. Os sinais podem sobrepor-se entre domínios e indivíduos, não representando pessoas únicas, atividade exclusiva de 2026 nem intrusões confirmadas [S4]. O subconjunto estrito de **15** bancos emissores na secção §9.1 preserva o seu denominador dentro da célula de 25 domínios de Banca e finanças [S4].

A.5 Registos de ransomware

Os **36 registos com etiqueta Portugal** na Ransompedia até **26 de novembro de 2026** (vs **21** em 2025 e **104** acumulados) medem alegações criminosas [S2]. Não representam intrusões verificadas nem vítimas únicas [S2]. Uma duplicação no mesmo dia sob `Nova` (24 de junho) limita as entidades distintas alegadas a **no máximo 35** [S2]. Duas entradas coincidem com confirmações públicas (`Casos L e M`), permanecendo **34 não verificadas** com identidades omitidas. Os totais do ano anterior dos comparadores cobrem todo o ano de 2025, enquanto 2026 vai até 26 de novembro [S2].

A.6 Âmbito de cartões de pagamento

ÂMBITO DOS NÚMEROS DE CARTÕES

Estes números descrevem uma população limitada de publicações observadas nos registos clandestinos retidos. Não estimam o furto de cartões em Portugal, perdas nacionais de fraude nem a validade ativa dos cartões.

As publicações clandestinas retidas incluíram **155 ocorrências de cartões de emissores portugueses** cobrindo **132 cartões mascarados distintos** (`114` publicações, `51` BIN de seis dígitos, `6` emissores nomeados omitidos) [S1]. Separadamente, **1 776 publicações de oferta** não continham linhas de cartão em texto claro, incluindo **1 433** listagens de lotes multipaís (mediana **USD 10-25**) [S1]. Nenhum valor confirma emissão ativa, furto, saldo disponível ou intrusão bancária [S1].

A.7 Incidentes públicos, exclusões e disciplina de nomeação

Catorze dossiês de incidentes públicos (`Casos H-U`) documentam **20 incidentes portugueses de 2026 oficialmente confirmados e amplamente noticiados**, a par de sete casos clandestinos (`Casos A-G`). Quatro categorias foram excluídas explicitamente das contagens confirmadas de 2026:

1. **Apagão ibérico de 28 de abril de 2025:** Evento de 2025 atribuído a controlo de tensão no relatório da ENTSO-E de março de 2026, validado pela ACER, sem causa cibernética identificada [S16][S17].
2. **Ciberataques municipais e de águas de 2023:** Incidentes de anos anteriores (incluindo ataques de 2023 a municípios e serviços de águas) ficam fora da janela de 2026.
3. **Alegações não confirmadas e notícias locais isoladas:** Entradas não verificadas da Ransompedia (`34 em 36`), alegações hacktivistas no Telegram (`313 Team` , `Z-Pentest Alliance` , `BNCT`) e notícias isoladas sem confirmação institucional ficam fora da nomeação confirmada.
4. **Avarias informáticas de rotina sem origem de ataque:** Falhas técnicas confirmadas como não cibernéticas, como a falha de atualização de setembro na Universidade de Aveiro [S52] e avarias operacionais separadas pelo Ciberseguranca.PT [S79].

Uma organização só é nomeada quando existem simultaneamente confirmação oficial e ampla cobertura mediática (`public_names.json`). Nenhuma pessoa singular (incluindo o médico no `Caso J`), nenhum subcontratado externo não confirmado (`Caso Q`) e nenhum domínio de vítima omitida figura neste pacote.

Apêndice B. Registo de evidências

Excertos autênticos redigidos do acervo clandestino retido da Brandefense para Portugal figuram nos capítulos abaixo (`B01` – `B15`). As datas refletem carimbos UTC de publicação; nenhuma publicação estabelece por si só intrusão confirmada ou transação concluída.

Ficha	Data (UTC)	Espaço	Alcunha	Idioma	Secção
B01	2026-01-04	Tópico de fórum	Alcunha omitida	Inglês	§4.2
B02	2026-04-03	Tópico de fórum	Alcunha omitida	Inglês	§4.2
B03	2026-09-13	Tópico de fórum	Alcunha omitida	Inglês	§4.2
B04	2026-04-30	Tópico de fórum	Alcunha omitida	Inglês	§4.3
B05	2026-05-01	Retransmissão Telegram	Alcunha omitida	Inglês	§4.3
B06	2026-06-02	Canal Telegram	Alcunha omitida	Inglês	§4.3
B07	2026-03-31	Tópico de fórum	Alcunha omitida	Russo / Inglês	§4.4
B08	2026-06-30	Tópico de fórum	Alcunha omitida	Russo	§4.4
B09	2026-04-05	Tópico de fórum	Alcunha omitida	Inglês	§4.4
B10	2026-11-17	Canal Telegram	Alcunha omitida	Português	§4.4
B11	2026-11-14	Tópico de fórum	Alcunha omitida	Inglês	§4.3
B12	2026-11-21	Tópico de fórum	Alcunha omitida	Inglês	§4.4
B13	2026-11-23	Tópico de fórum	Alcunha omitida	Inglês	§4.2
B14	2026-11-23	Tópico de fórum	Alcunha omitida	Inglês	§4.3
B15	2026-11-23	Tópico de fórum	Alcunha omitida	Inglês	§4.4

Apêndice C. Fontes

S1: Odin by Brandefense. Retained underground observations and publication counts (1 Jan–26 Nov 2026; recent 12–26 Nov 2026). URL omitido (dados próprios). Verificado em 2026-11-27.

S2: Ransompedia. Country-labelled ransomware listings (1 Jan–26 Nov 2026 and full-year 2025). URL omitido (dados próprios). Verificado em 2026-11-27.

S3: Odin by Brandefense. Configuration snapshot of 250 selected Portuguese domains (27 Nov 2026). URL omitido (dados próprios). Verificado em 2026-11-27.

S4: Brandefense Atlas and Odin by Brandefense. Exposure observations for 247 assessed Portuguese domains (27 Nov 2026) and rolling 365-day dark-chat/dark-web mentions across 250 domains (27 Nov 2025 to 26 Nov 2026; 2026 subset 1 Jan to 26 Nov 2026). URL omitido (dados próprios). Verificado em 2026-11-27.

S5: Governo de Portugal / Sistema de Segurança Interna. Relatório Anual de Segurança Interna (RASI) 2025 (including CNCS/CERT.PT, DGPJ, PJ and SIS chapters). https://portugal.gov.pt/api/media/edge/Project/Portal-do-Governo/Portal-do-Governo/gc25/Files/Documentos/rasi-2025-relatorio-anual-de-seguranca-interna/rasi_2025_-_relatorio_anual_de_seguranca_interna.pdf Verificado em 2026-11-27.

S6: Diário de Notícias da Madeira / Lusa. CNCS Riscos & Conflitos 6th edition: CERT.PT recorded 2,758 validated incidents in 2024 (+36%). https://www.dnoticias.pt/2025/9/16/463051-incidentes-de-ciberseguranca-registados-em-2024-sobem-36-para-2758/ Verificado em 2026-11-27.

S7: Pplware. CNCS Riscos & Conflitos 6th edition summary (2024 baseline and emerging risks). https://pplware.sapo.pt/internet/cncs-portugal-registou-aumento-de-incidentes-ciberneticos/ Verificado em 2026-11-27.

S8: Ministério Público - Gabinete de Cibercrime. Cibercrime em 2025: denúncias recebidas por correio eletrónico (+13.16% YoY). https://cibercrime.ministeriopublico.pt/destaque/cibercrime-em-2025-denuncias-recebidas Verificado em 2026-11-27.

S9: Comissão Nacional de Proteção de Dados (CNPD). CNPD and CNCS sign cooperation protocol (15 January 2026) and 2025 breach case statistics (472 cases, +42%). https://www.cnpd.pt/comunicacao-publica/noticias/comissao-nacional-de-protecao-de-dados-e-centro-nacional-de-ciberseguranca-assinam-protocolo-de-cooperacao/ Verificado em 2026-11-27.

S10: Observador / Lusa. Personal-data breach proceedings at CNPD rose 42% in 2025 to 472 (16 January 2026). https://observador.pt/2026/01/16/processos-por-violacao-de-dados-pessoais-aumentaram-42-em-2025/ Verificado em 2026-11-27.

S11: Observador. Staffing constraints slow CNPD GDPR fines: two fines totalling EUR 47,000 in 2025 (17 May 2026). https://observador.pt/2026/05/17/falta-de-pessoal-trava-aplicacao-de-coimas-por-violacao-de-dados-pessoais/ Verificado em 2026-11-27.

S12: Dinheiro Vivo / Diário de Notícias / Lusa. Banco de Portugal 2025 Payment Systems Report: H1 2025 payment fraud losses fell 40.4% to EUR 5.3M; 51 severe DORA incidents (21 May 2026). https://dinheirovivo.dn.pt/economia/perdas-em-fraudes-com-pagamentos-recuam-para-53-milhes-no-1-semestre-de-2025 Verificado em 2026-11-27.

S13: Observador / Lusa. Banco de Portugal beneficiary-confirmation and SPIN tools avoided EUR 6.5M in fraud; launch of Digital Fraud Monitoring Platform (25 May 2026). https://observador.pt/2026/05/25/ferramentas-do-banco-de-portugal-ja-evitaram-65-milhoes-de-euros-em-fraudes-desde-maio-de-2024/ Verificado em 2026-11-27.

S14: CCSL Advogados. Overview of Banco de Portugal Plataforma de Acompanhamento da Fraude Digital (26 May 2026). https://ccsllegal.com/2026/05/26/banco-de-portugal-lanca-plataforma-de-acompanhamento-da-fraude-digital/?lang=pt-pt Verificado em 2026-11-27.

S15: CNN Portugal / Lusa. ANACOM reports caller-ID and SMS spoofing complaints more than doubled in 2025 to mid-July compared with full-year 2024 and proposes legal amendment. https://cnnportugal.iol.pt/telefones/fraude/fraudes-com-numeros-de-telefone-mais-do-que-duplicam-em-2025-e-anacom-quer-nova-lei/20250720/687ca1f7d34e3f0baea0b5ed Verificado em 2026-11-27.

S16: ERSE - Entidade Reguladora dos Serviços Energéticos. ERSE Explica: ENTSO-E Expert Panel Factual Report on the 28 April 2025 Iberian power outage. https://www.erse.pt/media/owjmzbx3/erseexplica_relat%C3%B3rio-factual-vf.pdf Verificado em 2026-11-27.

S17: Governo de Portugal. ENTSO-E technical report validated by ACER on the 28 April 2025 Iberian power outage (20 March 2026). https://portugal.gov.pt/gc25/comunicacao/noticias/apagao-eletrico-relatorio-iliba-portugal-de-responsabilidades Verificado em 2026-11-27.

S18: RTP. Comissão Nacional de Eleições launches disinformation reporting channel ahead of 2026 presidential election. https://www.rtp.pt/noticias/pais/cne-cria-canal-de-denuncia-para-combater-fake-news-a-desinformacao-nao-vota-mas-influencia_n1708395 Verificado em 2026-11-27.

S19: ERC - Entidade Reguladora para a Comunicação Social. ERC and LabCom-UBI publish study on social-media disinformation during the 2026 Presidential Election. https://www.erc.pt/pt/a-erc/noticias/erc-e-labcom-ubi-publicam-estudo-sobre-desinformacao-nas-redes-sociais-durante-as-presidenciais-2026/ Verificado em 2026-11-27.

S20: DataReportal. Digital 2026: Portugal (9.26M internet users, 89.0% penetration at end of 2025; 10.4M population in October 2025). https://datareportal.com/reports/digital-2026-portugal Verificado em 2026-11-27.

S21: ECO. Valongo municipal cybersecurity and emergency response exercise CIBER 26 (28 September 2026). https://eco.sapo.pt/2026/09/28/valongo-testa-resposta-a-ciberataque-com-impacto-na-agua-energia-e-escolas/ Verificado em 2026-11-27.

S22: Procuradoria-Geral Distrital de Lisboa (PGDL). Decreto-Lei n.º 125/2025, de 4 de dezembro - Regime Jurídico da Cibersegurança (NIS2 transposition, in force 3 April 2026). https://www.pgdlisboa.pt/leis/lei_mostra_estrutura.php?tabela=leis&artigo_id=&nid=3985&nversao=&tabela=leis&so_miolo=S Verificado em 2026-11-27.

S23: Diário da República (CNCS). Regulamento n.º 756/2026, de 22 de junho - Implementing regulation of the Cybersecurity Legal Regime and MyCiber platform. https://files.diariodarepublica.pt/2s/2026/06/118000000/0003200120.pdf Verificado em 2026-11-27.

S24: Abreu Advogados. Legal briefing on CNCS Regulation n.º 756/2026 and MyCiber entity qualification procedures. https://abreuadvogados.com/conhecimento/publicacoes/regulamento-de-execucao-do-regime-juridico-da-ciberseguranca/ Verificado em 2026-11-27.

S25: Procuradoria-Geral Distrital de Lisboa (PGDL) / Abreu Advogados. Lei n.º 73/2025, de 23 de dezembro - National execution of EU DORA designating Banco de Portugal, CMVM and ASF. https://abreuadvogados.com/conhecimento/publicacoes/implementacao-do-regulamento-dora/ Verificado em 2026-11-27.

S26: Diário da República. Lei n.º 58/2019, de 8 de agosto - National execution of the GDPR in Portugal. https://files.dre.pt/1s/2019/08/15100/0000300040.pdf Verificado em 2026-11-27.

S27: Official Journal of the European Union (Publications Office). Commission Delegated Regulation (EU) 2025/301 - DORA major ICT incident notification time limits (Article 5). https://publications.europa.eu/resource/cellar/36795cde-ef2b-11ef-981b-01aa75ed71a1.0006.03/DOC_1 Verificado em 2026-11-27.

S28: Official Journal of the European Union (Publications Office). Regulation (EU) 2024/2847 - Cyber Resilience Act (CRA). https://publications.europa.eu/resource/cellar/21b7d4eb-a6e2-11ef-85f0-01aa75ed71a1.0006.03/DOC_1 Verificado em 2026-11-27.

S29: Observador / Lusa. Polícia Judiciária arrests two suspects in Europol LeakBase takedown and participates in Tycoon 2FA disruption affecting over 160 Portuguese organisations (4 March 2026). https://observador.pt/2026/03/04/pj-detem-dois-suspeitos-em-operacao-da-europol-que-desmantela-leakbase-um-dos-maiores-foruns-de-cibercrime-do-mundo/ Verificado em 2026-11-27.

S30: Correio da Manhã / Lusa. Polícia Judiciária UNC3T Operation Cryptoclaim recovers ~EUR 500,000 in stolen digital assets. https://www.cmjornal.pt/portugal/detalhe/pj-recupera-e-devolve-meio-milhao-de-euros-a-vitima-de-burla-informatica Verificado em 2026-11-27.

S31: Observador / Lusa. Polícia Judiciária UNC3T arrests two suspects over fraudulent use of French payment cards in Portugal (17 November 2026). https://observador.pt/2026/11/17/dois-estrangeiros-detidos-pela-pj-por-abuso-de-cartao-bancario-e-fraude-informatica/ Verificado em 2026-11-27.

S32: The Portugal News / Lusa. Polícia Judiciária participates in Europol Operation PowerOFF against DDoS-for-hire services, securing 59 removals (23 November 2026). https://www.theportugalnews.com/pt/noticias/2026-11-23/policia-portuguesa-participa-em-operacao-internacional-contra-ciberataques/1008950 Verificado em 2026-11-27.

S33: Eurojust. International operation disrupts NoName057(16) hacktivist DDoS infrastructure (16 July 2025). https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down Verificado em 2026-11-27.

S34: CNN Portugal / Lusa. Câmara Municipal da Guarda digital services blocked after complex cyber incident on 12 February 2026 (20 February 2026). https://cnnportugal.iol.pt/camara-da-guarda/ataque-informatico/camara-da-guarda-ha-uma-semana-com-varios-servicos-bloqueados-apos-incidente-cibernetico-complexo/20260220/6998d02bd34e6a48f446cb32 Verificado em 2026-11-27.

S35: Correio da Manhã / Lusa. Câmara Municipal da Guarda confirms preventive unavailability of platforms and PJ notification after 12 February cyberattack. https://www.cmjornal.pt/politica/detalhe/camara-da-guarda-continua-sem-acesso-a-plataformas-servicos-digitais-apos-ciberataque-de-12-de-fevereiro Verificado em 2026-11-27.

S36: Jornal o Interior. Câmara Municipal da Guarda suspends administrative deadlines retroactive to 12 February cyberattack. https://www.ointerior.pt/sociedade/camara-da-guarda-suspende-prazos-administrativos-devido-a-ataque-informatico/ Verificado em 2026-11-27.

S37: SOL. Global Instructure Canvas breach affects Portuguese higher-education students and triggers CNPD notifications (8 May 2026). https://sol.iol.pt/sociedade/noticias/ataque-cibernetico-mundial-a-plataforma-canva-ha-estudantes-portugueses-afetados/20260508/69fdeef30cf2d0ed34b84128 Verificado em 2026-11-27.

S38: Pplware. Instructure confirms early-May Canvas security incident affecting Portuguese university users. https://pplware.sapo.pt/internet/tem-conta-no-canvas-a-sua-conta-esta-em-risco/ Verificado em 2026-11-27.

S39: ECO / Lusa. Polícia Judiciária UNC3T reports unauthorised access to SNS patient records reached over 100,000 victims nationwide (25 May 2026). https://eco.sapo.pt/2026/05/25/acesso-indevido-a-dados-do-sns-atinge-mais-de-100-000-vitimas-de-todo-o-pais/ Verificado em 2026-11-27.

S40: Observador / Lusa. CNCS, SPMS and PJ conduct joint forensic investigation into SNS 24 data-access incident notified on 21 May (1 June 2026). https://observador.pt/2026/06/01/centro-de-ciberseguranca-continua-a-realizar-acoes-forenses-sobre-ataque-ao-sistema-nacional-de-saude-com-policia-judiciaria/ Verificado em 2026-11-27.

S41: RTP. PJ investigates unauthorised access to administrative SNS patient records via stolen medical credentials; health regulator ERS statement. https://www.rtp.pt/noticias/pais/pj-investiga-acesso-indevido-a-dados-de-centenas-de-utentes_n1742852 Verificado em 2026-11-27.

S42: ERS - Entidade Reguladora da Saúde. Official ERS statement on unauthorised accesses to health information via SNS 24. https://www.ers.pt/pt/comunicacao/destaques/lista-de-destaques/comunicado-ers-alegados-acessos-indevidos-a-informacao-de-saude-atraves-de-consulta-ao-portal-sns-24/ Verificado em 2026-11-27.

S43: Rádio Pax. Câmara Municipal de Serpa confirms 27 May 2026 cyberattack encrypting files and triggering server rebuild. https://www.radiopax.com/ataque-informatico-paralisou-servicos-da-camara-de-serpa-e-levanta-preocupacoes-de-seguranca/ Verificado em 2026-11-27.

S44: Correio Alentejo. Câmara Municipal de Serpa confirms external cyberattack reported to authorities and investigated by PJ (28 May 2026). https://correioalentejo.com/ataque-a-infraestrutura-informatica-da-camara-de-serpa/ Verificado em 2026-11-27.

S45: Rádio Voz da Planície. Câmara Municipal de Serpa confirms notification to CNCS, Ministério Público, CNPD and PJ. https://www.vozdaplanicie.pt/index.php/noticias/camara-municipal-de-serpa-alvo-de-ataque-informatico Verificado em 2026-11-27.

S46: Observador / Lusa. Santa Casa da Misericórdia de Santo Tirso confirms June 2026 cyberattack disrupting outpatient medical units (9 June 2026). https://observador.pt/2026/06/09/santa-casa-da-misericordia-de-santo-tirso-alvo-de-ciberataque-no-fim-de-semana/ Verificado em 2026-11-27.

S47: TugaTech. Santa Casa da Misericórdia de Santo Tirso reports notifications to CNCS, CNPD and PJ following 8 June intrusion and Qilin listing. https://tugatech.com.pt/t85651-ataque-informatico-expoe-dados-da-misericordia-de-santo-tirso-na-dark-web Verificado em 2026-11-27.

S48: RTP / Lusa. Metro Mondego alerts personalised transit-pass holders of probable personal-data copy in 6 July ransomware attack. https://www.rtp.pt/noticias/economia/dados-pessoais-poderao-ter-sido-copiados-durante-ataque-informatico-a-metro-mondego_n1755936 Verificado em 2026-11-27.

S49: Observador / Lusa. Metro Mondego confirms ransomware on internal systems while transport operations and card terminals remained isolated (26 July 2026). https://observador.pt/2026/07/26/dados-pessoais-poderao-ter-sido-copiados-durante-ataque-informatico-a-metro-mondego/ Verificado em 2026-11-27.

S50: Diário de Notícias / Lusa. Metro Mondego confirms CNCS, CNPD and criminal-investigation notifications following 6 July ransomware. https://www.dn.pt/sociedade/metro-mondego-alerta-que-dados-pessoais-podero-ter-sido-copiados-durante-ataque-informtico Verificado em 2026-11-27.

S51: RTP / Lusa. CNCS/CERT.PT confirms notification on 20 July of Universidade de Aveiro ransomware with email and database exfiltration. https://www.rtp.pt/noticias/economia/equipa-de-resposta-a-incidentes-de-ciberseguranca-notificada-a-20-julho-de-ocorrencia-na-universidade-de-aveiro_n1756821 Verificado em 2026-11-27.

S52: Rádio Ria / Lusa. Universidade de Aveiro confirms collaboration with CNCS, CNPD, PJ and SIS and separates September update outage from July ransomware. https://radioria.pt/noticias/universidade/ua-afasta-ligacao-entre-falhas-na-rede-sentidas-em-setembro-e-ciberataque-de-julho Verificado em 2026-11-27.

S53: ECO. Grupo Águas de Portugal confirms high-complexity cyberattack on administrative IT systems; water supply unaffected (4 August 2026). https://eco.sapo.pt/2026/08/04/aguas-de-portugal-alvo-de-ciberataque-fornecimento-e-qualidade-da-agua-nao-esta-em-causa/ Verificado em 2026-11-27.

S54: Observador / Lusa. Environment Minister confirms Grupo Águas de Portugal attack remained contained to administrative systems (7 August 2026). https://observador.pt/2026/08/07/ciberataque-ao-grupo-aguas-de-portugal-nao-afetou-fornecimento-de-agua-diz-ministra-do-ambiente/ Verificado em 2026-11-27.

S55: Observador. MEO confirms mass attack degrading international network links without system intrusion or customer data access (14 September 2026). https://observador.pt/2026/09/14/meo-foi-alvo-de-ataque-em-massa-que-afetou-servicos-de-telecomunicacoes/ Verificado em 2026-11-27.

S56: ECO / Lusa. MEO technical analysis confirms distributed denial-of-service (DDoS) waves across 14-15 September 2026 (15 September 2026). https://eco.sapo.pt/2026/09/15/incidentes-na-meo-foram-provocados-por-ataque-de-negacao-de-servico/ Verificado em 2026-11-27.

S57: ECO. MEO reports 6,020,686 blocked attack attempts during the first two days of Web Summit 2026 in Lisbon (10 November 2026). https://eco.sapo.pt/2026/11/10/web-summit-foi-alvo-de-seis-milhoes-de-tentativas-de-ciberataque-em-dois-dias/ Verificado em 2026-11-27.

S58: RTP / Lusa. SIRP confirms external web-contractor development server breach exposed non-classified data from public websites; no operational or classified systems affected. https://www.rtp.pt/noticias/pais/ciberataque-expoe-na-internet-dados-nao-classificados-das-secretas-portuguesas_n1770309 Verificado em 2026-11-27.

S59: Diário de Notícias / Lusa. SIRP confirms 8 October 2026 clarification and report to Procuradoria-Geral da República following 120 GB forum listing. https://www.dn.pt/sociedade/ciberataque-expe-na-internet-dados-no-classificados-das-secretas-portuguesas Verificado em 2026-11-27.

S60: Rádio Nova. Câmara Municipal de Ovar confirms October 2026 cyberattack suspending municipal services. https://www.radionova.fm/atualidade/camara-de-ovar-foi-alvo-de-ataque-informatico-e-tera-servicos-encerrados-ate-quarta-feira/ Verificado em 2026-11-27.

S61: Notícias de Ovar. Reporting on Câmara Municipal de Ovar October 2026 cyberattack recovery and cybersecurity measures. https://noticiasdeovar.pt/news/o-ataque-informatico-a-camara-de-ovar-e-os-investimentos-feitos-na-area/ Verificado em 2026-11-27.

S62: Observador / Lusa. ANEPC confirms cyberattack copying personal records from the 60,000-entry National Firefighters Registry (RNBP) and immediate suspension with CNCS and RNSI (24 October 2026). https://observador.pt/2026/10/24/piratas-informaticos-atacam-base-de-dados-dos-bombeiros-e-acedem-a-dados-pessoais/ Verificado em 2026-11-27.

S63: Diário de Notícias / Lusa. ANEPC and Liga dos Bombeiros Portugueses confirm RNBP data copy excluding banking records and issue phishing/smishing/quishing warnings. https://www.dn.pt/sociedade/base-de-dados-dos-bombeiros-foi-alvo-de-ciberataque-comprometendo-dados-pessoais Verificado em 2026-11-27.

S64: RTP. Grupo Mosqueteiros confirms seven Intermarché stores in Portugal affected by European refrigeration-controller supply-chain cyberattack (2 November 2026). https://www.rtp.pt/noticias/mundo/sete-lojas-do-intermarche-atingidas-por-ciberataque-em-portugal_n1776375 Verificado em 2026-11-27.

S65: Observador. APED confirms three of seven affected Intermarché Portugal stores suffered total refrigerated merchandise loss (2 November 2026). https://observador.pt/2026/11/02/ataque-informatico-atinge-frigorificos-e-congeladores-de-supermercados-na-belgica-luxemburgo-e-suecia/ Verificado em 2026-11-27.

S66: Azeméis.Net / Lusa. Câmara Municipal de Santa Maria da Feira confirms 5 November 2026 cyberattack halting IT, email and landlines and notifying CNCS. https://azemeisnet.sapo.pt/ataque-informatico-camara-feira-depois-ovar-servicos-afetados/ Verificado em 2026-11-27.

S67: Rádio Sintonia. Câmara Municipal de Santa Maria da Feira official statement on 5 November 2026 overnight intrusion and CNCS coordination. https://radiosintonia.pt/2026/11/05/camara-municipal-de-santa-maria-da-feira-alvo-de-ataque-informatico/ Verificado em 2026-11-27.

S68: Observador / Lusa. Worten confirms unauthorised access to limited customer and supplier data, patching exploited flaw and notifying CNCS, CNPD and PJ (11 November 2026). https://observador.pt/2026/11/11/worten-alvo-de-ciberataque-que-acedeu-a-dados-de-clientes-e-prestadores-de-servicos/ Verificado em 2026-11-27.

S69: RTP / Lusa. Worten confirms no passwords or payment-card details accessed in November 2026 cyberattack. https://www.rtp.pt/noticias/economia/worten-alvo-de-ciberataque-que-acedeu-a-dados-de-clientes-e-prestadores-de-servicos_n1778556 Verificado em 2026-11-27.

S70: ECO. Worten notifies affected customers on 12 November 2026 that NIF, telephone, email and some order numbers were accessed (12 November 2026). https://eco.sapo.pt/2026/11/12/ciberataque-a-worten-acedeu-a-nif-contactos-telefonicos-e-email-de-clientes/ Verificado em 2026-11-27.

S71: Correio da Manhã. SMAS de Sintra confirms November 2026 cyberattack affecting online customer forms. https://www.cmjornal.pt/portugal/detalhe/ataque-informatico-saca-dados-dos-clientes-dos-smas-de-sintra Verificado em 2026-11-27.

S72: TugaTech. SMAS de Sintra notifies affected customers of web-form data copy including NIF, ID and IBAN and notifies CNPD and CNCS. https://tugatech.com.pt/t94480-smas-de-sintra-sofrem-ataque-informatico-que-expoe-dados-pessoais-e-iban-de-clientes Verificado em 2026-11-27.

S73: Observador. ASAE official source confirms 15 November 2026 website defacement; CNCS confirms outreach (15 November 2026). https://observador.pt/2026/11/15/site-da-asae-indisponivel-apos-ataque-informatico-que-usou-imagem-de-jose-socrates/ Verificado em 2026-11-27.

S74: Executive Digest. IMT confirms consecutive cyberattacks forcing preventive suspension of digital services with no indication of data exfiltration. https://executivedigest.sapo.pt/ciberataques-ao-imt-deixam-servicos-em-dificuldades-atencao-as-possiveis-burlas/ Verificado em 2026-11-27.

S75: Rádio Metropolitana Porto. Câmara Municipal do Porto confirms 21 November 2026 website defacement limited to institutional portal with no personal-data compromise and CNCS notification. https://www.radiometropolitanaporto.pt/website-da-camara-do-porto-alvo-de-ataque-informatico/ Verificado em 2026-11-27.

S76: Ciberseguranca.PT. Technical analysis of Câmara Municipal do Porto CMS modification (21 November 2026) and broader 2026 Portuguese public-portal defacements. https://www.ciberseguranca.pt/camara-do-porto-paginas-oficiais-exibem-assinatura-de-intruso-e-os-seus-dados/ Verificado em 2026-11-27.

S77: ADENE - Agência para a Energia. Official ADENE communiqué confirming 23 November 2026 intrusion, preventive suspension of Portal SCE and notifications to CNCS and PJ. https://www.adene.pt/adene-alvo-de-ataque-informatico-suspende-temporariamente-o-acesso-ao-sce/ Verificado em 2026-11-27.

S78: RTP / Lusa. ADENE suspends Building Energy Certification System (SCE) following unauthorised intrusion (23 November 2026). https://www.rtp.pt/noticias/economia/adene-suspende-acesso-ao-sistema-de-certificacao-energetica-dos-edificios-apos-ciberataque_n1781185 Verificado em 2026-11-27.

S79: Ciberseguranca.PT. Overview of 2026 cyber-incident timeline highlighting 32 public Portuguese cases through 23 November 2026. https://www.ciberseguranca.pt/188-ciberincidentes-em-2026-o-que-a-linha-do-tempo-do-ano-revela/ Verificado em 2026-11-27.

S80: Burlómetro / Tek Notícias (citing CNCS). CNCS/CERT.PT alert on phishing emails impersonating CNCS requesting a critical system update (25 June 2026). https://burlometro.pt/alertas/email-cncs-atualizacao-critica/ Verificado em 2026-11-27.

S81: ThreatFabric. Massiv Android banking trojan masquerading as an IPTV app targeting Portuguese digital identity wallet and Chave Móvel Digital (February 2026). https://www.threatfabric.com/blogs/massiv-when-your-iptv-app-terminates-your-savings Verificado em 2026-11-27.

S82: IETF RFC Editor. RFC 7489 - Domain-based Message Authentication, Reporting, and Conformance (DMARC). https://www.rfc-editor.org/rfc/rfc7489.html Verificado em 2026-11-27.

S83: IETF RFC Editor. RFC 7208 - Sender Policy Framework (SPF). https://www.rfc-editor.org/rfc/rfc7208.html Verificado em 2026-11-27.

S84: IETF RFC Editor. RFC 6376 - DomainKeys Identified Mail (DKIM) Signatures. https://www.rfc-editor.org/rfc/rfc6376.html Verificado em 2026-11-27.

S85: IETF RFC Editor. RFC 6797 - HTTP Strict Transport Security (HSTS). https://www.rfc-editor.org/rfc/rfc6797.html Verificado em 2026-11-27.

S86: NIST NVD. CVE-2026-1731 - BeyondTrust Remote Support / Privileged Remote Access pre-authentication RCE (CVSS 9.8). https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Verificado em 2026-11-27.

S87: NIST NVD. CVE-2026-88771 and CVE-2026-88772 - Citrix NetScaler ADC and Gateway input-validation vulnerabilities (CVSS 9.8 / 8.1). https://nvd.nist.gov/vuln/detail/CVE-2026-88771 Verificado em 2026-11-27.

S88: NIST NVD. CVE-2026-102764 - BeyondTrust Remote Support improper message origin validation (CVSS 9.8). https://nvd.nist.gov/vuln/detail/CVE-2026-102764 Verificado em 2026-11-27.

S89: NIST NVD. CVE-2026-104935 - Ivanti Connect Secure authentication bypass by spoofing (CVSS 8.6). https://nvd.nist.gov/vuln/detail/CVE-2026-104935 Verificado em 2026-11-27.

S90: NIST NVD. CVE-2026-109618 and CVE-2026-109619 - PHP out-of-memory and global-state memory-corruption flaws (CVSS 9.8 / 8.1). https://nvd.nist.gov/vuln/detail/CVE-2026-109618 Verificado em 2026-11-27.

S91: NIST NVD. CVE-2026-120868 - Citrix NetScaler ADC and Gateway packet-processing memory overflow (CVSS 4.0 9.3). https://nvd.nist.gov/vuln/detail/CVE-2026-120868 Verificado em 2026-11-27.

S92: NIST NVD. CVE-2026-115560 and CVE-2026-129289 - PHP session-serializer RCE and PHP-FPM request smuggling (CVSS 4.0 9.2). https://nvd.nist.gov/vuln/detail/CVE-2026-115560 Verificado em 2026-11-27.

S93: NIST NVD. CVE-2025-53770 (Microsoft SharePoint) and CVE-2025-64095 (DNN CMS) - Top vulnerabilities observed by CERT.PT in 2025. https://nvd.nist.gov/vuln/detail/CVE-2025-53770 Verificado em 2026-11-27.

S94: Brandefense. Brandefense demo and advisory contact page. https://brandefense.io/request-a-demo/ Verificado em 2026-11-27.

Apêndice D. Glossário

- **Indicador nacional Atlas.** Valor único de 0 a 100 da Brandefense Atlas para o conjunto da carteira avaliada em Portugal [S4]. Valores mais altos refletem maior exposição externa observada, nunca taxa de intrusão nem classificação setorial [S4].
- **CNCS / CERT.PT.** Centro Nacional de Cibersegurança de Portugal e a respetiva equipa nacional de resposta a incidentes de segurança informática [S5][S22].
- **Decreto-Lei n.º 125/2025.** Regime Jurídico da Cibersegurança em Portugal que transpõe a Diretiva NIS2 da UE, em vigor desde 3 de abril de 2026 [S22].
- **Regulamento n.º 756/2026 e MyCiber.** Regulamento de execução do CNCS (em vigor desde 23 de junho de 2026) e plataforma eletrónica para qualificação de entidades, designação de responsáveis e medidas mínimas [S23][S24].
- **QNRCS.** Quadro Nacional de Referência para a Cibersegurança que define controlos mínimos de segurança em Portugal [S23].
- **CNPD e Lei n.º 58/2019.** Comissão Nacional de Proteção de Dados e diploma nacional de execução do RGPD [S9][S26].
- **DORA e Lei n.º 73/2025.** Regulamento europeu de resiliência operacional digital no setor financeiro e lei nacional de execução que designa o Banco de Portugal, a CMVM e a ASF [S25][S27].
- **PJ UNC3T.** Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica da Polícia Judiciária [S29][S39].
- **RASI 2025.** Relatório Anual de Segurança Interna de Portugal que reúne os capítulos oficiais do CNCS/CERT.PT, PJ, DGPJ e SIS [S5].
- **FCSAL.** Fórum de Cibersegurança da Administração Local, que integra entidades intermunicipais, a Associação Nacional de Municípios Portugueses e autarquias para partilha de alertas e boas práticas [S5].
- **RNSI.** Rede Nacional de Segurança Interna, que apoiou a ANEPC e o CNCS na suspensão imediata do registo RNBP [S62].
- **Chave Móvel Digital (CMD).** Meio nacional de autenticação eletrónica e assinatura digital móvel para serviços públicos e privados em Portugal [S81].
- **Multibanco, MB WAY e SPIN.** Rede interbancária nacional de pagamentos e referências, serviço móvel de transferências instantâneas e ferramenta de identificação de beneficiário do Banco de Portugal [S13].
- **NIF / CC / NISS / SNS.** Número de Identificação Fiscal, Cartão de Cidadão, número da Segurança Social e número do Serviço Nacional de Saúde; identificadores pessoais constituem contexto, nunca autenticação [S39] [S62].
- **DMARC, SPF, DKIM e HSTS.** Normas publicadas em DNS de autenticação de correio eletrónico (`RFC 7489` , `RFC 7208` , `RFC 6376`) e política estrita de transporte HTTPS (`RFC 6797`) [S82][S83][S84][S85].
- **AiTM (adversary-in-the-middle).** Técnica de phishing que interpõe um proxy em tempo real entre o utilizador e o portal de início de sessão para intercetar palavras-passe e sessões MFA ativas (como no Tycoon 2FA) [S29].

- **BIN (número de identificação bancária).** Primeiros seis dígitos de um cartão de pagamento que identificam a rede e a instituição emissora [S1].
- **KYC (Know Your Customer).** Procedimentos de verificação de identidade e diligência de cliente realizados por instituições financeiras antes da abertura de contas [S1].
- **TLP:CLEAR.** Partilhável sem restrições ao abrigo do Traffic Light Protocol, respeitando a privacidade e obrigações legais.

Sobre este relatório

Elaborado por Odin by Brandefense. A versão 1.0 aplica datas de referência distintas. A janela de atividade de 2026 decorre de 1 de janeiro a 26 de novembro de 2026 (UTC, data de publicação), com 12 a 26 de novembro analisados separadamente como atividade recente.

As menções móveis a 365 dias abrangem 27 de novembro de 2025 a 26 de novembro de 2026. As observações de exposição (247 de 250 domínios) e configurações passivas (todos os 250) refletem um retrato de 27 de novembro de 2026, permanecendo 3 domínios desconhecidos na exposição. Todas as fontes externas foram verificadas em 27 de novembro de 2026.

Esta edição em português europeu traduz o original em inglês; em caso de divergência de redação, prevalece a edição em inglês. As recomendações exigem validação face aos ativos, dependências e obrigações legais de cada organização.

© 2026 Brandefense. Todos os direitos reservados.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO