bilingual edition

ptsoc{news}

Primeiro semestre 2026 | First half of 2026

#19

Novo Regime Jurídico da Cibersegurança

New Legal Framework for Cybersecurity

Novas regras de registo em .pt
New .pt registration rules

O impacto da IA no abuso de DNS
The impact of AI on DNS abuse

Cibercrime autónomo e abuso de DNS
Autonomous cybercrime and DNS abuse

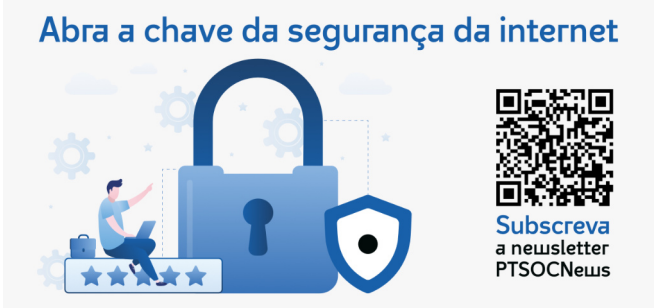
Radiografia da resiliência digital nacional
Evaluation of national digital resilience

Ficha técnica
Credits

Esta publicação é produzida pelo .pt
This publication is produced by .pt

19ª Edição | Primeiro semestre 2026
19th Edition | First half of 2026

Edição e design gráfico: Casa dos Bits – Edições Lda.
Edited and designed by: Casa dos Bits – Edições Lda



Luisa Ribeiro Lopes
Presidente do Conselho Diretivo do .PT

Reforçar a ligação à comunidade com a PTSOC News

A PTSOC News inicia agora uma nova etapa, marcada por uma revisão de design e de conteúdos. Esta evolução reflete o compromisso em tornar a revista uma fonte de informação técnica de referência e um ponto de contacto ativo entre o .pt e a comunidade de cibersegurança. O objetivo é reforçar a proximidade, promover a partilha de conhecimento e consolidar uma rede de colaboração que contribua para um espaço digital mais seguro e resiliente.

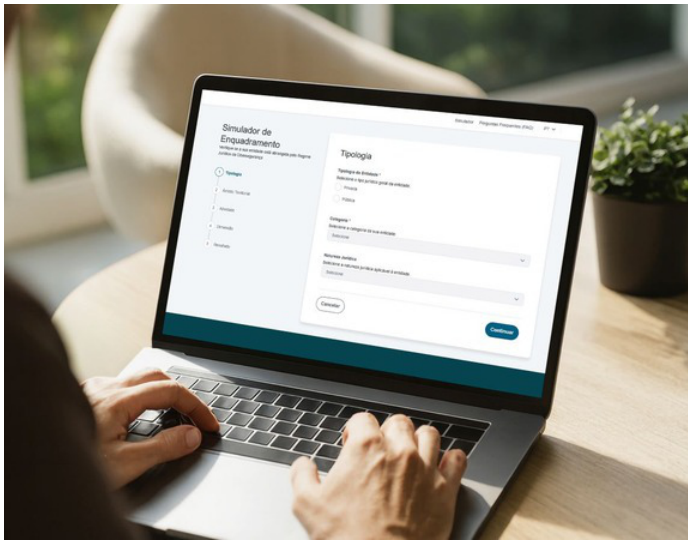
Mais do que uma atualização visual, esta nova fase traduz uma visão estratégica: posicionar a PTSOC News como um hub de informação e cooperação, capaz de acompanhar os desafios crescentes da segurança digital e de apoiar profissionais e organizações na adoção de boas práticas.

Este reforço ganha especial relevância num momento em que o novo Regime Jurídico da Cibersegurança — que transpõe a diretiva europeia NIS2 — impõe novas responsabilidades e exigências a muitas entidades abrangidas. Queremos continuar a contribuir para a capacitação e sensibilização do ecossistema nacional, reforçando o .pt como um domínio de confiança e excelência, e para isso contamos com o compromisso de toda a comunidade.

en pt

Índice

Regime Jurídico da Cibersegurança



a nova linha vital para empresas e a resiliência digital do país

O enquadramento legal está completo para a aplicação do Regime Jurídico da Cibersegurança que transpõe diretiva NIS2, com novos desafios e obrigações para um maior número de entidades e prazos para cumprir.

O tema da cibersegurança já integrou definitivamente a agenda das organizações de diferentes sectores e dimensões, e com a entrada em vigor do Regime Jurídico da Cibersegurança (RJC), que transpõe a diretiva europeia NIS2, há também uma nova fase com desafios para todo o ecossistema. Cerca de seis mil entidades passam a estar sujeitas a regras mais exigentes, responsabilidades reforçadas e prazos apertados, um número que cresce exponencialmente face ao anterior enquadramento legal. Nunca tantas entidades públicas e privadas estiveram obrigadas a cumprir requisitos formais de segurança digital, com medidas que são cada vez mais exigentes, num contexto onde as ameaças se tornam mais globais e sofisticadas com a ajuda da Inteligência Artificial.

"A cibersegurança é um investimento, e isso significa que traz valor acrescentado e melhora o funcionamento das instituições e empresas, aumenta a qualidade dos produtos e serviços e assegura a qualidade de vida das pessoas".

Lino Santos, Coordenador do CNCS

O novo regime foi publicado em dezembro de 2025, entrou oficialmente em vigor a 3 de abril de 2026 e acaba de ser operacionalizado com a publicação do Regulamento e da plataforma de registo MyCiber do Centro Nacional de Cibersegurança (CNCS), que assume o papel de Autoridade de cibersegurança competente. Mas o caminho já estava a ser preparado para o reforço da resiliência das redes de sistemas de informação nacionais, com o objetivo declarado de criar um ecossistema mais seguro e resiliente, preparado para proteger as empresas, as pessoas e o próprio Estado de Direito.

"Com o regime jurídico da cibersegurança, o que nós queremos é mais confiança, mais resiliência e mais responsabilidade naquilo que é a cibersegurança", defendeu Lino Santos, Coordenador do CNCS, durante a conferência C-Days 2026.

Registo na plataforma MyCiber com prazos a ter em conta

No mesmo dia em que entrou em vigor o Regulamento do Regime Jurídico da Cibersegurança o CNCS colocou online **a plataforma MyCiber que funciona como portal de registo das entidades e ponto de contacto com as autoridades nacionais de cibersegurança.** Este é um elemento-chave para que as empresas e organismos façam o seu registo no prazo estipulado, cumprindo os 30 dias obrigatórios para as empresas criadas depois de 4 de dezembro de 2025, quando foi publicado o RJC, ou 60 dias para as criadas em datas anteriores.

Depois de notificadas de que foram qualificadas como essenciais ou importantes, as organizações têm 20 dias para comunicação do responsável de cibersegurança e ponto de contacto permanente. **E há mais prazos a anotar na agenda: até 31 de janeiro de 2027, ou 6 meses após a notificação de qualificação final, consoante o prazo que vença primeiro, deverá ser feito o envio da Lista de Ativos das entidades essenciais, importantes e públicas relevantes**.

De notar ainda que, no prazo de dois anos, em junho de 2028, as entidades essenciais devem começar a apresentar um Relatório anual, e aplicar as medidas de cibersegurança, uma obrigação que também abrange as entidades importantes e públicas.

Se não cumprirem a obrigação de registo as entidades estão sujeitas a sanções com coimas que são definidas consoante a qualificação da entidade e o nível de gravidade da contraordenação.

Impacto transversal em 17 sectores identificados

Para além dos setores tradicionalmente críticos, como energia, transportes ou saúde, o regime inclui agora empresas de setores "importantes", fornecedores essenciais e uma parte significativa da cadeia de abastecimento digital. O impacto faz-se sentir em grandes operadores mas também em PME que nunca se viram envolvidas num enquadramento regulatório de cibersegurança.

O desafio aqui é maior. Muitas empresas partem de níveis baixos, sem equipas dedicadas, processos estruturados ou políticas internas. Outras dependem fortemente de fornecedores externos, o que aumenta a complexidade. E há ainda um défice de literacia que se traduz em decisões tardias ou reativas na preparação e resposta a incidentes.

A responsabilidade da gestão de topo das organizações é uma das mudanças do novo regime. A NIS2 deixa claro que administradores e diretores passam a ter deveres formais de supervisionar políticas, aprovar medidas, garantir recursos e acompanhar riscos. A lógica é simples: a cibersegurança deixa de ser um tema "técnico" e passa a ser um tema de governação.

Hackers vs. Crackers, quais são as diferenças essenciais?

HACKERS
Éticos / White Hat

Objetivo: melhorar segurança, encontrar falhas antes dos criminosos.
Atuação: com autorização, seguindo regras e enquadramento legal.
Contribuição: reforçam sistemas, ajudam empresas e entidades públicas.
Motivação: ética, investigação, proteção.

CRACKERS
Maliciosos / Black Hat

Objetivo: explorar vulnerabilidades para roubo, fraude ou sabotagem.
Atuação: sem autorização, violando sistemas e leis.
Impacto: danos financeiros, interrupção de serviços, extorsão.
Motivação: lucro, vandalismo digital, espionagem.

As consequências do incumprimento podem ser graves já que o regime prevê coimas elevadas, proporcionais à dimensão da organização, e penaliza a negligência. Mesmo assim o Governo tenha deixado claro que procurou implementar um regime "equilibrado e proporcional", procurando evitar "custos de contexto excessivos".

Lino Santos defende também que o CNCS quer ser um parceiro do ecossistema, não apenas um fiscalizador, trabalhando em proximidade com as entidades, partilhando boas práticas e lições aprendidas, e ouvindo as organizações nas suas dificuldades e conquistas. A estratégia passa por capacitar, apoiar e criar condições para que as organizações evoluam.

Planear e melhorar a maturidade

Para as entidades abrangidas, a pergunta é inevitável: o que é preciso fazer agora? O primeiro passo é fazer um diagnóstico e confirmar o enquadramento no MyCiber, identificar funções críticas e nomear o responsável de cibersegurança. Depois, é necessário avaliar riscos, implementar medidas técnicas e organizativas, rever contratos com fornecedores, definir processos de deteção e resposta a incidentes e preparar documentação para auditorias futuras. A formação, da gestão às equipas operacionais, é parte obrigatória deste caminho, apesar da falta de profissionais especializados em cibersegurança que estão entre os mais procurados e podem não ser suficientes para responder à procura.

Hackers éticos com maior proteção legal

A regulação do ethical hacking é uma das grandes novidades do Regime Jurídico da Cibersegurança e uma opção diferenciada na transposição da NIS2 para a legislação portuguesa. **O objetivo é proteger os hackers que estão a avaliar os sistemas e plataformas para identificar falhas que possam ser comunicadas às entidades e solucionadas antes que sejam exploradas por crackers**.
Com a nova legislação os "White hat hackers" passam a ter proteção legal para testar sistemas, aplicações ou redes, partindo de uma autorização explícita para o fazer, e assim conseguir identificar vulnerabilidades antes de serem exploradas por atacantes reais. **Ficam de fora a interrupção de serviços, danos nos sistemas, eliminação ou cópia de dados, ataques DDoS, phishing ou roubo de credenciais, que continuam a ser encarados como crimes.**

Simulador é ponto de partida para cumprir obrigações

Ainda antes da publicação do Regulamento e da disponibilização da plataforma MyCiber para registo das entidades abrangidas pelo Regime Jurídico da Cibersegurança, o **Centro Nacional de Cibersegurança colocou online um simulador onde as empresas e organizações públicas podem testar se fazem parte das entidades abrangidas pelo novo regime.**
Este é um primeiro passo para apoiar o processo de adaptação, embora a ferramenta não seja vinculativa e não abranja alguns casos específicos. **O resultado é apenas indicativo e não está sujeito a uma avaliação formal**, pelo que a sua utilização não dispensa o registo das entidades que se inicia após a publicação do Regulamento.

Quem está abrangido pelo Regime Jurídico da Cibersegurança?

O novo Regime que resulta da transposição da NIS2 alarga de forma muito significativa as entidades abrangidas pelas obrigações de cibersegurança, abarcando 17 setores e a Administração Pública e não fazendo distinção pela dimensão da organização. A legislação estabelece a diferença entre "Setores de importância crítica" e "outros setores críticos", considerando ainda as entidades como essenciais ou importantes, e entidades públicas relevantes.

Sectores de importância crítica

energia; transportes; setor bancário; infraestruturas do mercado financeiro; saúde; gestão da água (potável e residual); infraestruturas digitais; gestão de serviços de TIC; e Espaço.

Outros sectores críticos

serviços postais e de estafetas; gestão de resíduos; produção, fabrico e distribuição de químicos; produção, transformação e distribuição de produtos alimentares; Indústria transformadora; prestação de serviços digitais; e investigação.

Os próximos meses serão decisivos. Com as medidas do RJC a entrarem em vigor no espaço de 24 meses, as organizações têm de acelerar a maturidade da cibersegurança, aplicando políticas de análise dos riscos e de segurança, tratamento de incidentes e práticas básicas de ciber-higiene e formação. No C-Days o coordenador do CNCS deixou o aviso de que "não são 24 meses para deixar tudo para a última da hora. É um tempo para construir e implementar, é um tempo para planear e crescer na maturidade de forma gradual e não deixar tudo para a última hora".

O desafio não é apenas técnico mas cultural. O RJC redefine responsabilidades, eleva exigências e obriga a uma nova forma de pensar o risco digital. Mas também abre espaço para um ecossistema mais robusto, mais preparado e mais competitivo.

Novas Regras de Registo de .pt

uma evolução para reforçar a confiança e a segurança no espaço digital português

Marta Moreira Dias
Vogal do Conselho Diretivo do .PT

A transformação do ambiente digital e as novas exigências legais e regulamentares incluindo o Regime Jurídico da Cibersegurança, estão na base da evolução das regras de Registo de .pt que entram em vigor a 1 de julho de 2026.

O domínio de topo de Portugal (.pt) tem registado, ao longo dos últimos anos, um crescimento sustentado, afirmando-se como um dos ccTLD (country code Top-Level Domain) europeus com melhor desempenho. Paralelamente, mantém níveis muito reduzidos de litigância, um número residual de reclamações e uma taxa extremamente baixa de remoção de domínios por incumprimento das regras de registo. Este contexto demonstra a maturidade do ecossistema .pt e a adequação das regras atualmente em vigor.

É também por este motivo que a revisão das Regras de Registo, cuja entrada em vigor está prevista para 1 de julho de 2026, não surge como resposta a problemas estruturais ou falhas do modelo existente. Trata-se, antes, de uma evolução natural e preventiva, destinada a acompanhar a transformação do ambiente digital, incorporar novas exigências legais e regulamentares e responder a sugestões apresentadas pelos registrars, consumidores finais, stakeholders e restantes intervenientes do mercado.

Porque foi necessário rever as regras de 2021?

Desde a última revisão, realizada em 2021, o enquadramento legislativo e regulatório europeu e nacional sofreu alterações significativas. Entre os principais fatores que justificaram a atualização das Regras de Registo destacam-se a entrada em vigor de novos instrumentos legais, como o Regulamento dos Serviços Digitais (Digital Services Act), o Regime Jurídico da Cibersegurança, o Regulamento das Indicações Geográficas e diversos diplomas nacionais que impactam a gestão e utilização de identificadores digitais.

A revisão procurou igualmente refletir a experiência acumulada pelo .PT na gestão do domínio nacional, incorporar melhorias operacionais sugeridas pelos registrars e alinhar os procedimentos com iniciativas e processos internos entretanto desenvolvidos. Estas novas regras refletem, pois, adequadamente as exigências acrescidas de segurança, fiabilidade e responsabilização que recaem sobre a entidade gestora do domínio nacional.

O objetivo central foi garantir que as regras permanecem claras, atuais, proporcionais e adequadas aos desafios de um ecossistema digital cada vez mais exigente, sem comprometer a simplicidade e a eficiência que têm caracterizado o modelo de registo .pt.

Segurança e cibersegurança: um eixo central da revisão

Entre os fatores que justificam a atualização das Regras de Registo .pt assume particular relevância o reforço das exigências em matéria de segurança e cibersegurança aplicáveis às infraestruturas críticas da Internet. Enquanto entidade responsável pela gestão do domínio de topo correspondente a Portugal, a Associação DNS.pt desempenha um papel essencial na preservação

da estabilidade, resiliência, disponibilidade e confiança do ecossistema digital nacional.

A gestão do ccTLD .pt envolve responsabilidades que transcendem o mero registo de nomes de domínio, abrangendo igualmente a adoção de mecanismos preventivos e reativos destinados a mitigar riscos e comprometimento de serviços e outras ameaças que possam afetar a segurança dos utilizadores e da própria Internet portuguesa.

Neste contexto, a entrada em vigor do novo Regime Jurídico da Cibersegurança assume particular relevância. Ao reconhecer formalmente o .pt como entidade essencial, o legislador veio concretizar e clarificar um conjunto de obrigações já inerentes à gestão de uma infraestrutura crítica digital, estabelecendo um quadro mais robusto de responsabilidades em matéria de gestão de risco, governação da segurança, prevenção de incidentes, monitorização, reporte e cooperação institucional.

A revisão das Regras de Registo surge, assim, também como um instrumento de alinhamento com este novo enquadramento legal, assegurando que os termos e condições aplicáveis ao registo e manutenção de nomes de domínio .pt refletem adequadamente as exigências acrescidas de segurança, fiabilidade e responsabilização que recaem sobre a entidade gestora do domínio nacional.

Importa igualmente salientar que este novo quadro normativo não se limita à Associação DNS.pt. Pelo contrário, promove uma abordagem mais abrangente e integrada da segurança do ecossistema .pt, estendendo de forma clara determinadas obrigações e responsabilidades aos diversos intervenientes da cadeia de valor, nomeadamente aos agentes de registo (registrars). A segurança do espaço digital .pt depende cada vez mais da capacidade de todos os intervenientes atuarem de forma articulada, partilhando responsabilidades, boas práticas e procedimentos que contribuam para a prevenção e mitigação de riscos.

Uma atualização orientada para o futuro

As novas Regras de Registo de .pt representam uma evolução ponderada e alinhada com a realidade atual do ecossistema digital. Não alteram os princípios fundamentais que têm contribuído para o sucesso do domínio nacional, mas introduzem melhorias que reforçam a segurança, a qualidade da informação registada, a conformidade legal e a eficiência operacional. Esta é a nossa aposta, só concretizável com o compromisso de todos.

As principais alterações introduzidas no registo em .pt

Reforço dos mecanismos de validação e verificação de dados

Uma das alterações mais relevantes consiste na criação de um artigo específico dedicado à validação e verificação dos dados associados aos titulares de nomes de domínio. Passa a ficar expressamente previsto que a verificação dos dados constitui condição para o registo de domínios .pt, para a transferência de titularidade e para alterações de contactos essenciais, como o endereço de correio eletrónico ou o número de telefone. Foram ainda introduzidos os conceitos de "validação" e "verificação" no glossário das Regras de Registo.

Novos instrumentos para resolução de litígios e cumprimento legal

A revisão introduz a possibilidade de recurso à mediação no âmbito dos mecanismos de resolução alternativa de litígios relacionados com nomes de domínio. Por outro lado, passa a prever-se a possibilidade de bloqueio ou redirecionamento de nomes de domínio mediante notificação por autoridade legalmente competente, permitindo uma resposta mais eficaz a situações que exijam intervenção urgente ou cumprimento de determinações legais.

Harmonização das condições de registo

Outra novidade importante consiste na aplicação das mesmas condições de registo aos domínios .pt e .com.pt, simplificando o quadro regulamentar e promovendo maior coerência entre as diferentes categorias de nomes de domínio.

Clarificação do regime de pagamentos

As regras revistas estabelecem igualmente que serão cobrados todos os domínios registados, mesmo quando venham posteriormente a ser removidos por incumprimento das condições de admissibilidade previstas nas regras.
É ainda prevista a introdução futura de um valor aplicável ao período de pending delete para domínios renovados nessa fase do ciclo de vida, cuja implementação ocorrerá de forma diferida.

Ajustamento dos prazos procedimentais

As novas regras introduzem também alterações nos prazos aplicáveis aos procedimentos de verificação. O prazo para confirmações, retificações ou aditamentos dos dados fornecidos passa de 5 para 10 dias, proporcionando maior flexibilidade aos titulares e aos registrars. Adicionalmente, prevê-se a suspensão do prazo de análise da conformidade do domínio enquanto decorrem estes pedidos de esclarecimento ou de documentação.

Atualização do serviço WHOIS

As alterações refletem também a evolução das exigências em matéria de proteção de dados pessoais lida em conjunto com o já referido Regime Jurídico da Cibersegurança.
No futuro, no diretório WHOIS deixam de ser publicados dados pessoais, deixando igualmente de ser necessário recolher consentimento para essa publicação.
Para pessoas coletivas continuarão a ser disponibilizados o nome e a morada, mantendo-se simultaneamente mecanismos de contacto.

Cibercrime autónomo e abuso do DNS

Tendências que moldam o futuro dos ataques digitais

O relatório IOCTA 2026 descreve um cenário em rápida mutação, onde o cibercrime se torna mais autónomo, mais invisível e mais difícil de travar.

A Europol alerta que, nos próximos anos, a capacidade das autoridades para responder dependerá da adoção de tecnologias avançadas, do acesso legal a dados críticos e de uma colaboração muito mais estreita com o setor privado.

Uma das tendências mais disruptivas é o surgimento do autonomous cybercrime. Grupos criminosos já utilizam sistemas de IA agentiva capazes de executar fluxos completos de ataque, desde a recolha de informação à intrusão, exfiltração e monetização, com intervenção humana mínima. À medida que estas ferramentas se tornam mais acessíveis, os atacantes conseguem distanciar-se das operações, reduzindo o risco de identificação e transformando o cibercrime numa ameaça cada vez mais intangível.

O relatório destaca também a evolução das ameaças híbridas, onde atores patrocinados por Estados e grupos de cibercrime colaboram de forma fluida. Ataques DDoS continuam a ser usados para minar a confiança pública e gerar instabilidade política, enquanto coligações de hackers combinam intrusões, roubo de dados e esquemas de fraude. O resultado é um ecossistema de ataque dinâmico, onde fronteiras entre espionagem, sabotagem e criminalidade financeira se tornam cada vez mais difusas.

No centro desta nova realidade está o abuso do DNS, que o IOCTA identifica como uma das infraestruturas críticas mais exploradas para ataques e fraude online. O DNS funciona como ponte entre a infraestrutura criminosa e as vítimas, permitindo que ofensores lancem campanhas de phishing, distribuam malware ou controlem botnets através de domínios temporários. Criminosos exploram a ausência de mecanismos automáticos de reporte e a lentidão dos pedidos judiciais internacionais. Quando um domínio malicioso é finalmente bloqueado, muitas vezes o ataque já atingiu escala.

O DNS é igualmente essencial para operações de ransomware e C2, com botnets a recorrerem a proxies residenciais para mascarar tráfego e imitar utilizadores legítimos. Esta técnica dificulta a deteção e torna o desmantelamento das infraestruturas criminosas significativamente mais complexo.

O IOCTA 2026 reforça que o futuro do cibercrime será marcado por infraestruturas distribuídas, criptomoedas opacas, mercados fragmentados e IA autónoma. Para reduzir o "velocity gap" entre atacantes e autoridades, a Europol defende uma resposta baseada em inovação tecnológica, acesso legal a dados essenciais e cooperação internacional contínua. Sem esta adaptação, o cibercrime continuará a ganhar terreno.

O impacto da Inteligência Artificial no abuso de DNS

José Casinha
Vogal do Conselho Diretivo do .PT

A IA não mudou a natureza dos ataques de abuso de DNS mas há um aumento de escala, velocidade e sofisticação.
O impacto dos agentes autónomos ainda é incerto e a resposta defensiva exige uma adaptação sustentada e baseada em evidências.

A IA no contexto do DNS

As duas grandes categorias de tecnologias de Inteligência Artificial, os LLMs e os agentes autónomos, interagem com o abuso de DNS de formas fundamentalmente distintas, e qualquer análise séria deve tratá-las separadamente. O estado atual do abuso é dominado por fluxos de trabalho assistidos por LLMs; o abuso conduzido por agentes autónomos continua a ser uma preocupação de curto-médio prazo, e não uma realidade presente documentada. Uma das constatações mais importantes ao examinar o papel da IA no abuso de DNS é que os vetores de ataque fundamentais não mudaram. Phishing, spoofing de domínios, registos maliciosos, campanhas baseadas em infraestrutura e manipulação de SEO não são fenómenos novos — são ferramentas operacionais dos cibercriminosos há mais de uma década. O que a IA modificou não foi a natureza destes ataques, mas a economia e a eficiência com que podem ser executados.

Esta distinção é extremamente relevante. Significa que os quadros defensivos existentes, os instrumentos de política e as abordagens de deteção permanecem conceptualmente válidos. O desafio não é conceber respostas para categorias de ameaças inteiramente novas, mas garantir que as respostas existentes possam operar à velocidade e escala que os ataques assistidos por IA agora exigem.

Como a IA está a influenciar o panorama dos ataques

Talvez o efeito mais consequente da IA no abuso de DNS a curto prazo seja a democratização das capacidades, ou seja, assistimos a uma clara redução das barreiras à entrada. Tarefas que anteriormente exigiam conhecimentos técnicos significativos são agora acessíveis a atores com muito menos competências. Esta não é apenas uma mudança quantitativa. É uma transformação estrutural em quem pode conduzir abusos sofisticados.

Para além do conteúdo, as ferramentas de IA — em particular os agentes autónomos — têm o potencial de transformar a forma como a infraestrutura de suporte aos ataques de abuso é criada e gerida. Os domínios podem ser registados, os ambientes de alojamento aprovisionados, e campanhas reconfiguradas com reduzida intervenção humana.

Quando a infraestrutura é detetada e eventualmente desativada, infraestrutura substituta pode ser criada e ativada automaticamente sem qualquer intervenção humana.

Isto tem implicações que vão além da eficiência operacional. Começa a desafiar a lógica económica das operações defensivas de desativação: se o custo

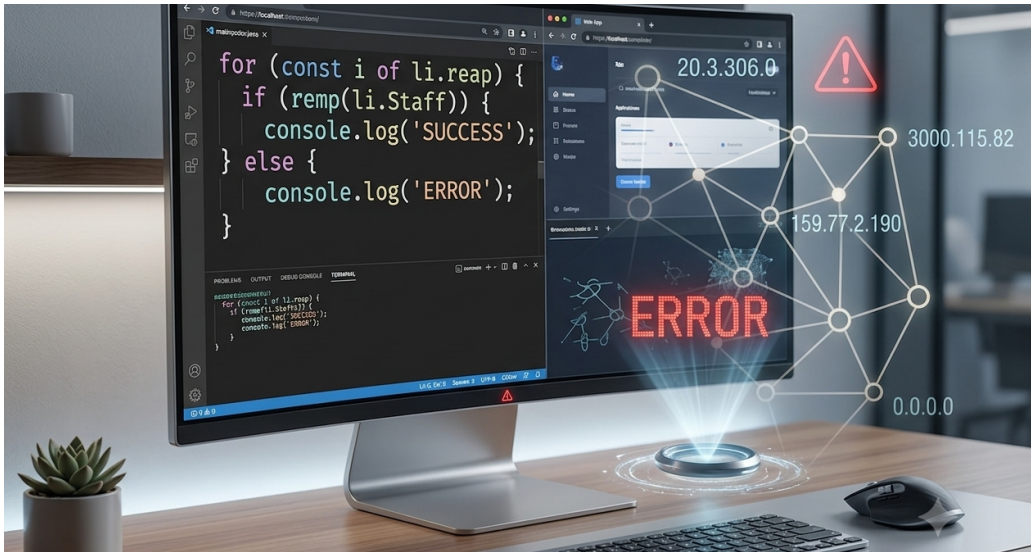
de substituir infraestrutura desativada se aproxima de zero e a substituição pode ser automatizada, o efeito dissuasor da perturbação fica substancialmente enfraquecido. A convergência de escala e personalização com capacidade de conduzir campanhas que são simultaneamente amplas e individualmente adaptadas representa uma mudança qualitativa nas capacidades de ataque que não era praticamente alcançável antes da IA generativa.

O papel da IA já existente na Infraestrutura Defensiva

É importante reconhecer que as defesas alimentadas por IA não são uma aspiração futura, estão já incorporadas em partes do ecossistema DNS. Os sistemas de avaliação de risco de registo que sinalizam registos de domínios potencialmente abusivos antes de se concluírem já incorporam técnicas adjacentes à IA. A questão relevante não é se introduzir IA na estratégia defensiva, mas como alargar e melhorar as capacidades já existentes.

A implantação de IA em contextos defensivos de abuso de DNS comporta os seus próprios riscos que requerem gestão cuidadosa. A alucinação, a geração de outputs confiantes mas incorretos é um modo de falha real dos LLMs que é particularmente perigoso em contextos de mitigação de abuso de alto risco. Um falso positivo que classifica incorretamente um domínio legítimo como malicioso pode causar danos reais; um falso negativo que falha na deteção de atividade maliciosa cria risco contínuo.

Talvez a observação mais estável sobre o abuso de DNS na era da IA seja que este tipo de atividades permanece fundamentalmente dependente de vítimas humanas. O abuso de DNS é eficaz porque consegue persuadir um humano para clicar num link, introduzir credenciais, descarregar um ficheiro ou autorizar um pagamento. A cadeia de ataque termina no comportamento humano, e é esse o objetivo final que confere valor ao abuso.



Esta observação tem uma implicação importante: a evolução do abuso de DNS assistido por IA será reativa à forma como os próprios humanos mudam.

Isto significa que todo o investimento de IA do lado do ataque serve em última análise o objetivo de explorar vulnerabilidades cognitivas humanas: limitações na compreensão da linguagem, suscetibilidade à engenharia social, as heurísticas que guiam a tomada de decisões online, e os níveis variados de literacia digital entre diferentes populações de utilizadores.

À medida que as potenciais vítimas desenvolvem melhores intuições para conteúdo gerado por IA, os atacantes adaptam-se para produzir conteúdo que derrota essas intuições. Isto cria uma dinâmica co-evolutiva em vez de uma mudança de capacidade única.

O único cenário que altera fundamentalmente este quadro é o surgimento do abuso máquina-a-máquina — ataques em que a vítima, bem como o atacante, é automatizada, e o resultado prejudicial é alcançado sem que um humano esteja alguma vez no ciclo. Isto permanece uma possibilidade futura e não uma realidade presente, mas a trajetória do desenvolvimento de agentes de IA torna-o um cenário que a análise prospetiva não pode ignorar.

Trajetória a curto prazo

Olhando em frente, três desenvolvimentos parecem mais prováveis de moldar o impacto da IA no abuso de DNS no curto prazo.

O aumento da escala e velocidade são as consequências a curto prazo mais certas. As capacidades já demonstradas — triagem automatizada de domínios, geração rápida de conteúdo, gestão programática de infraestrutura — continuarão a melhorar e a tornar-se mais amplamente disponíveis. Campanhas que atualmente requerem esforço operacional significativo tornar-se-ão mais acessíveis e mais rápidas de executar.

O aumento da sofisticação é a segunda trajetória. Não porque a IA vá introduzir técnicas de ataque fundamentalmente novas, mas porque a disponibilidade de ferramentas capazes para um conjunto mais alargado de atores significa que padrões de ataque mais sofisticados se tornarão rotineiros em vez de excecionais.

A atividade emergente de agentes autónomos representa a terceira e menos certa trajetória. À medida que as capacidades dos agentes de IA amadurecem, a possibilidade de campanhas que se executam com mínima direção humana torna-se mais realista. As implicações tanto para a deteção como para a dissuasão são significativas.

Conclusão

A IA não está a revolucionar o abuso de DNS da forma dramática que algumas narrativas sugerem, nem é uma preocupação marginal que pode ser seguramente adiada. A caracterização precisa é que é um acelerador — um conjunto de capacidades que torna os padrões de ataque existentes mais rápidos, mais baratos e mais acessíveis, sem alterar a sua natureza fundamental.

Os esquemas são antigos. A escala e a velocidade estão a mudar. A economia do abuso está a deslocar-se de formas que favorecem atores que anteriormente careciam dos recursos ou competências para operar com sofisticação. E as condições estruturais — automação completa do ciclo de vida do ataque, abuso máquina-a-máquina, gestão autónoma de infraestrutura — estão a aproximar-se da viabilidade mesmo que ainda não sejam a norma.

A resposta adequada não é nem o alarme nem a indiferença, mas uma adaptação sustentada e baseada em evidências: melhorar a deteção, fortalecer os quadros de política, implantar a IA defensiva de forma ponderada e com supervisão adequada, e manter a coordenação comunitária que permite ao campo ver claramente o que está realmente a acontecer — por distinção do que é temido ou presumido.

O humano permanece, por agora, tanto o alvo como o elo essencial na cadeia de abuso. Compreender que a ameaça evolui em resposta à forma como os humanos mudam — como interagem com a IA, como a sua calibração de confiança se adapta, como a sua literacia digital se desenvolve — é talvez o quadro analítico mais importante para antecipar o que vem a seguir.

Cooperação para travar o cibercrime

Adesão da UE à Convenção das Nações Unidas reforça capacidade

A adesão formal da União Europeia à Convenção das Nações Unidas contra o Cibercrime dá um passo importante na harmonização das infrações e no reforço da cooperação policial e judiciária e acelera o acesso transfronteiriço a provas eletrónicas, um dos maiores desafios da investigação criminal.

A criminalidade digital deixou de ser um fenómeno técnico para se tornar um problema económico, social e geopolítico. As estimativas da Cybersecurity Ventures indicavam que, em 2025, o cibercrime poderia custar à economia mundial mais de 10 biliões de dólares, com potencial para ultrapassar os 12 a 15 biliões. As organizações e os cidadãos enfrentam ataques mais frequentes, mais rápidos e mais automatizados, impulsionados por ferramentas de IA que reduzem custos para os atacantes e ampliam o impacto.

A cooperação entre as várias entidades e países é apontada como um fator crucial num contexto de cibercrime globalizado, onde a pressão aumenta também com a evolução tecnológica. Em 2024 as Nações Unidas avançaram com uma Convenção das Nações Unidas contra o Cibercrime que cria uma base mínima comum para cooperar, investigar e responder a ataques que atravessam fronteiras em segundos, e agora a União Europeia formalizou uma adesão que já tinha sido aprovada em dezembro do ano passado.

A Convenção define um conjunto de crimes informáticos, estabelece regras para recolha e partilha de prova eletrónica e reforça salvaguardas de direitos fundamentais. A UE sublinha que este acordo reforça a capacidade da UE para combater o cibercrime em conjunto com parceiros internacionais e alarga a cooperação internacional entre os 112 Estados-Membros da ONU que não fazem parte da Convenção de Budapeste sobre o Cibercrime.

Neste sentido, a Convenção da ONU responde a três necessidades centrais:

1

Investigações mais rápidas e eficazes, criando mecanismos mais ágeis para aceder a dados essenciais, sempre com controlo judicial.

2

Regras mínimas comuns, reduzindo as zonas cinzentas e facilitando a ação conjunta, especialmente em ataques coordenados que envolvem múltiplas jurisdições.

3

Proteção de direitos num ambiente digital hostil, incorporando princípios alinhados com a Carta dos Direitos Fundamentais da UE.

Num ecossistema digital onde um ataque pode partir de qualquer lugar e atingir qualquer organização, a União Europeia reconhece que a cooperação é a única estratégia para garantir um combate global, reduzir riscos, acelerar respostas e proteger cidadãos, empresas e democracias.

IberianQCI:

Portugal e Espanha ligam infraestruturas de comunicações quânticas

Os objetivos para o projeto de três anos são ambiciosos e passam por contribuir para o desenvolvimento de um ecossistema europeu de comunicações quânticas escalável.

O projeto IberianQCI, liderado pela Indra Space, foi oficialmente inaugurado como o segmento ibérico da futura rede europeia de comunicações quânticas, EuroQCI, criada para garantir ligações altamente seguras entre os Estados-Membros da União Europeia e proteger infraestruturas críticas e informação sensível contra ameaças futuras.

Com duração prevista de três anos, o IberianQCI pretende interligar as infraestruturas nacionais de comunicações quânticas de Portugal e Espanha, criando uma rede integrada e totalmente interoperável com a arquitetura europeia. A iniciativa soma-se ao trabalho já desenvolvido no âmbito do EuroQCI e de projetos nacionais como o PTQCI (Portuguese Quantum Communication Infrastructure) e o DISCRETION, este último liderado por Portugal para reforçar a segurança das redes militares.

Financiado pelo Connecting Europe Facility (CEF), o projeto é coordenado por Portugal através da Indra Space, em colaboração com entidades científicas, tecnológicas e industriais dos dois países. Entre os parceiros portugueses estão a Infraestruturas de Portugal, IP Telecom, Instituto de Telecomunicações, Altice Labs e o Instituto Superior Técnico. Do lado espanhol participam a Universidade Politécnica de Madrid, a Telefónica, o Consejo Superior de Investigaciones Científicas (CSIC), o Instituto de Ciências Fotónicas de Barcelona, o Centro de Supercomputación de Galiza e a Universidade de Vigo.

O desenvolvimento das comunicações quânticas é vital para garantir a cibersegurança global face à futura capacidade dos supercomputadores quânticos. Estes sistemas de comunicação permitem uma transmissão de dados ultrassegura e quase impenetrável, servindo de pilar para a proteção de infraestruturas críticas, dados governamentais e instituições financeiras. Ao contrário das redes tradicionais, as ligações quânticas permitem a distribuição de chaves criptográficas invioláveis, baseadas em princípios físicos que tornam impossível a sua interceção sem deteção imediata.

Atualmente, a fibra ótica limita a transmissão de chaves quânticas a cerca de 100 quilómetros, mas a utilização de satélites elimina essa barreira, permitindo coberturas globais com menor atenuação de sinal.

A arquitetura híbrida do IberianQCI combina as componentes terrestres e espaciais. Está prevista uma ligação transfronteiriça entre Vigo e Valença, utilizando nós de confiança que reforçam a conectividade entre os dois países e integram as redes nacionais existentes. A componente espacial incluirá três estações óticas, em Madrid, Barcelona e no sul de Portugal, ligadas ao segmento terrestre em Lisboa. Estas estações permitirão comunicações seguras com o satélite demonstrador EAGLE-1, em baixa órbita terrestre, e com a futura constelação SAGA, garantindo a distribuição de chaves quânticas mesmo entre países sem fronteiras comuns.

Radiografia da resiliência digital nacional: Literacia, boas práticas e capacitação têm de ser reforçadas

A 7ª edição do Relatório Cibersegurança em Portugal, tema Sociedade, traça o retrato do nível de prontidão da sociedade portuguesa para responder aos riscos do ciberespaço e aponta fragilidades e a necessidade de reforçar competências.

O documento complementa o Relatório Cibersegurança em Portugal, tema Riscos & Conflitos, que foi publicado em 2025 pelo Centro Nacional de Cibersegurança (CNCS), e procura oferecer uma visão integrada do panorama dos riscos no ciberespaço de interesse nacional, abordando comportamentos, maturidade tecnológica e vulnerabilidades num contexto em que as ameaças evoluem rapidamente.

À medida que indivíduos e empresas intensificam a utilização de serviços digitais, cresce também a exposição aos riscos, em particular nos domínios da engenharia social e da fraude. O relatório identifica as principais tendências dos incidentes que têm afetado infraestruturas nacionais e confirma que a grande maioria continua concentrada no setor privado, representando cerca de 78% do total, mas é observada uma mutação tática perigosa nos alvos dos atacantes.

Os dados revelam um agravamento significativo na Administração Pública, onde os incidentes aumentaram 67% no espaço de um ano, entre 2023 e 2024. A administração local destaca-se como um dos alvos mais vulneráveis, com cerca de um quarto das câmaras municipais a reportarem ciberataques ativos nos seus ecossistemas durante 2024 — um sinal claro de fragilidades estruturais.

No que diz respeito às tipologias de vetores de ataque, mantém-se o predomínio das técnicas que exploram o erro humano e a manipulação psicológica. O phishing, o smishing e o vishing continuam a ser as portas de entrada preferenciais para esquemas criminosos, agora acompanhados por formas mais sofisticadas de engenharia social. Burlas online, roubo e comprometimento de contas e ataques de ransomware, que paralisam serviços operacionais e exigem resgates avultados, permanecem entre as ameaças mais frequentes. O relatório destaca ainda o crescimento do CEO Fraud, das campanhas de falso recrutamento e dos incidentes envolvendo infostealers, que representaram mais de 80% da atividade de malware observada no terceiro trimestre de 2025.

Empresas ainda pouco preparadas para responder a ameaças

Apesar do aumento de incidentes registado pelo CERT.pt em 2024, uma análise comparativa com dados do Eurostat indica que a percentagem de empresas portuguesas afetadas por incidentes com impacto na disponibilidade de serviços TIC, destruição ou modificação de dados, ou divulgação de informação confidencial, foi inferior à média europeia.

Portugal surge como o quinto país com menor percentagem de incidentes entre empresas de pequena dimensão (10–49 trabalhadores), sugerindo que a digitalização tem sido acompanhada por alguma adoção de medidas de segurança.

Ainda assim, a maioria das organizações não atingiu níveis elevados de maturidade. Firewalls avançadas, sistemas de deteção de intrusão e políticas rigorosas de gestão de acessos continuam a ser sobretudo uma realidade das grandes empresas, deixando cadeias de abastecimento e parceiros mais pequenos expostos a riscos indiretos. A Administração Pública enfrenta desafios semelhantes: apesar dos progressos na digitalização e da adoção de medidas de segurança, estas revelam-se insuficientes para evitar incidentes com impacto nacional.

Reduzir a superfície de ataque e reforçar a ciber-resiliência

O relatório sublinha que, embora exista um reconhecimento crescente da importância da cibersegurança, esse avanço ainda não se traduz numa redução efetiva dos impactos negativos. A perceção de risco é elevada e as organizações estão a reforçar o investimento, nomeadamente através da contratação de serviços especializados. No entanto, o recrutamento de profissionais qualificados continua a ser um obstáculo generalizado, criando fragilidades devido à escassez de recursos internos.

A falta de sensibilização e formação contínua é outro ponto crítico. A maioria das empresas portuguesas não promove ações regulares de capacitação em cibersegurança, nem integra formação obrigatória para colaboradores. Também permanece reduzido o uso de campanhas de grande alcance dirigidas ao público em geral, limitando a disseminação de práticas básicas de ciber-higiene.

Face às vulnerabilidades identificadas, o relatório recomenda reforçar a literacia digital e associá-la, desde cedo, a uma literacia específica para a cibersegurança. Defende ainda a capacitação intensiva dos recursos humanos, com especial foco na Administração Pública, sobretudo no nível autárquico, e nas pequenas e médias empresas, que continuam a carecer de orçamento dedicado à proteção digital. O aumento do alcance e eficácia das ações de sensibilização pública é igualmente apontado como essencial para dotar os cidadãos de competências que permitam mitigar fraudes e burlas antes de estas atingirem redes domésticas ou empresariais.

78%

dos incidentes ocorrem em empresas do setor privado

+67%

de crescimento nos ataques contra a Administração Pública entre 2023 e 2024

25%

das Câmaras Municipais reportaram deteção de ciberataques em 2024

Luisa Ribeiro Lopes
Chair Of The Board Of Directors at .PT

Strengthening the community connection with PTSOC News

PTSOC News is now entering a new phase, marked by a design and content review. This evolution reflects the commitment to making the magazine a source of reference technical information and an active point of contact between .pt and the cybersecurity community. The goal is to strengthen proximity, promote knowledge sharing, and consolidate a collaborative network that contributes to a safer and more resilient digital space.

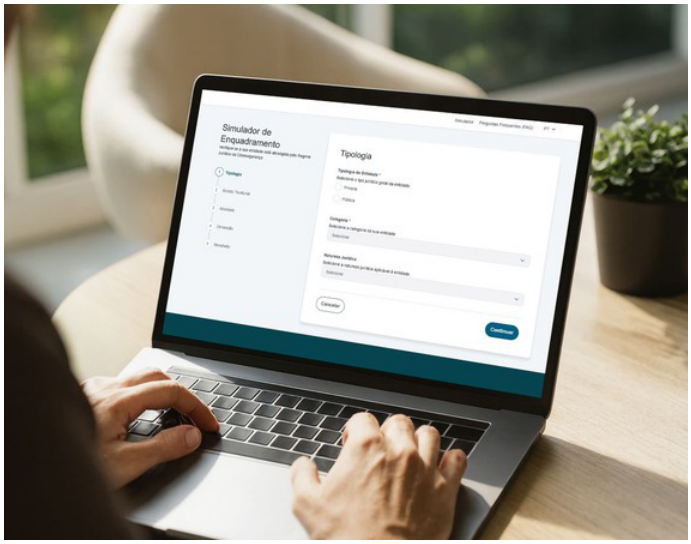
More than a visual update, this new phase reflects a strategic vision: to position PTSOC News as an information and cooperation hub, capable of keeping up with the growing challenges of digital security and supporting professionals and organizations in adopting best practices.

This reinforcement gains special relevance at a time when the new Cybersecurity Legal Regime — which transposes the European NIS2 directive — imposes new responsibilities and requirements on many covered entities. We want to continue contributing to the empowerment and awareness of the national ecosystem, reinforcing .pt as a domain of trust and excellence, and for this we count on the commitment of the entire community.

en pt

Índex

Cybersecurity Legal Framework



The new lifeline for companies and the country's digital resilience

The legal framework is ready for the application of the Cybersecurity Legal Regime, which transposes the NIS2 directive, with new challenges and obligations for a larger number of entities and deadlines to meet.

The topic of cybersecurity has definitively become part of the agenda of organizations of different sectors and sizes, and with the entry into force of the Cybersecurity Legal Framework, which transposes the European NIS2 directive, there is also a new phase with challenges for the entire ecosystem. Around six thousand entities are now subject to more demanding rules, reinforced responsibilities and tight deadlines, a number that is growing exponentially compared to the previous legal framework. Never before have so many public and private entities been required to comply with formal digital security requirements, with measures that are increasingly demanding, in a context where threats are becoming more global and sophisticated with the help of Artificial Intelligence.

"Cybersecurity is an investment, and that means it brings added value and improves the functioning of institutions and companies, increases the quality of products and services, and ensures the quality of life of people."

Lino Santos, Coordinator of the CNCS

The new regime was published in December 2025, officially came into effect on April 3, 2026, and has just been operationalized with the publication of the Regulation and the MyCiber registration platform of the National Cybersecurity Center (CNCS), which assumes the role of competent cybersecurity authority. But the path was already being prepared for strengthening the resilience of national information systems networks, with the stated objective of creating a safer and more resilient ecosystem, prepared to protect companies, people, and the rule of law itself.

"With the cybersecurity legal regime, what we want is more trust, more resilience, and more responsibility in cybersecurity," argued Lino Santos, Coordinator of the CNCS, during the C-Days 2026 conference.

Registration on MyCiber platform: Timeline and compliance steps

On the same day the new Legal Regime of Cybersecurity came into force, Portugal's National Cybersecurity Centre (CNCS) launched the MyCiber platform online - the official portal where organizations must register and maintain contact with national cybersecurity authorities. **The platform is now a central compliance step, as entities are required to register within the legal deadlines: 30 days for companies created after December 4, 2025, the date the legal framework was published, and 60 days for those established before that.**

After being notified that they have been qualified as essential or important, organizations have 20 days to communicate the name of the cybersecurity manager and permanent point of contact. And there are more deadlines to be noted on the agenda: by January 31, 2027, or 6 months after the notification of final qualification, whichever comes first, the List of Assets of essential, important and relevant public entities must be submitted.

Also note that, **within two years, in June 2028, essential entities must begin submitting an annual report and implementing cybersecurity measures, an obligation that also covers important and public entities.**

Non-compliance with the registration obligation results in the imposition of sanctions. The applicable fines are set based on the nature of the entity and the severity of the infringement.

Cross-cutting impact across 17 identified sectors

In addition to traditionally critical sectors, such as energy, transport, or health, the regime now includes companies from "important" sectors, essential suppliers, and a significant part of the digital supply chain. The impact is felt by large operators but also by SMEs that have never been involved in a cybersecurity regulatory framework.

The challenge here is deeper. Many companies start from low levels, without dedicated teams, structured processes, or internal policies. Others rely heavily on external suppliers, which increases complexity. And there is still a literacy deficit that translates into late or reactive decisions in incident preparation and response.

The responsibility of senior management in organizations is one of the changes in the new regime. NIS2 makes it clear that administrators and directors now have formal duties to oversee policies, approve measures, ensure resources, and monitor risks. The logic is simple: cybersecurity ceases to be a "technical" issue and becomes a governance issue.

The consequences of non-compliance can be serious. The system stipulates high fines, proportional to the size of the organization, and penalizes negligence, although the Government has made it clear that it sought to implement a "balanced and proportionate" system, seeking to avoid "excessive contextual costs."

Lino Santos also argues that the CNCS wants to be a partner of the ecosystem, not just an inspector, working closely with the entities, sharing good practices and lessons learned, and listening to the organizations in their difficulties and achievements. The strategy involves empowering, supporting, and creating conditions for organizations to evolve.

Planning and improving maturity

For the organizations covered, the question is inevitable: what needs to be done now? The first step is to conduct a diagnosis and confirm eligibility under MyCiber, identify critical functions, and appoint a cybersecurity manager. Then, it is necessary to assess risks, implement technical and organizational measures, review contracts with suppliers, define incident detection and response processes, and prepare documentation for future audits. Training, from management to operational teams, is a mandatory part of this path, even with the lack of cybersecurity specialists, who are among the most sought after and may not be sufficient to meet the demand.

Hackers vs. Crackers: What are the essential differences?

HACKERS
Ethical / White Hat

Goal: Improve security by identifying vulnerabilities before malicious actors can exploit them.
Approach: Operate with authorization, following rules, standards and legal frameworks.
Contribution: Strengthen systems, support companies and public entities, and help prevent incidents
Motivation: Ethics, research, protection and enhancing digital resilience.

CRACKERS
Malicious / Black Hat

Goal: Exploit vulnerabilities for theft, fraud, sabotage or extortion.
Approach: Act without authorization, breaking into systems and violating laws.
Impact: Cause financial losses, service disruption, data breaches and blackmail.
Motivation: Profit, digital vandalism, espionage or organized criminal objectives.

Ethical hackers get stronger legal protection

The regulation of ethical hacking is one of the major innovations introduced by the new Cybersecurity Legal Framework and represents a distinctive approach in Portugal's transposition of the NIS2 Directive. **The idea is to protect hackers who assess systems and platforms to identify vulnerabilities that can be reported to organisations and resolved before they are exploited by malicious actors.**
Under the new legislation, white hat hackers are granted legal protection when testing systems, applications or networks, provided they have explicit authorisation to do so. However, **they must not act with the intention of obtaining economic advantage, although they may be remunerated as part of their professional activity.**
Excluded from this protection are actions such as service interruption, system damage, deletion or copying of data, DDoS attacks, phishing or credential theft, all of which continue to be treated as criminal offences.

Simulator as a starting point for meeting obligations

Even before the publication of the Regulation and the launch of the MyCiber, the **National Cybersecurity Centre made available an online simulator that allows companies and public organisations to test whether they fall within the scope of the new regime.**

This is a first step to support the adaptation process, although the tool is not binding and does not cover certain specific cases. The result is merely indicative and is not subject to formal assessment, meaning that its use does not replace the mandatory registration of entities, which begins after the Regulation is published.

Who is covered by the Cybersecurity Legal Framework?

The new framework resulting from the transposition of NIS2 significantly expands the range of entities subject to cybersecurity obligations, now encompassing 17 sectors as well as Public Administration. The legislation differentiates between "sectors of critical importance" and "other critical sectors", and further classifies entities as essential, important, or relevant public entities.

Sectors of critical importance

energy; transport; banking; financial market infrastructures; healthcare; water management (drinking and wastewater); digital infrastructure; ICT service management; and space.

Other critical sectors

postal and courier services; waste management; production, manufacturing and distribution of chemicals; production, processing and distribution of food products; manufacturing industry; provision of digital services; and research.

The coming months will be decisive. With the new measures coming into effect within 24 months, organizations must accelerate their cybersecurity maturity by applying risk analysis and security policies, incident handling, and basic cyber hygiene and training practices. At C-Days, the CNCS coordinator warned that "these are not 24 months to leave everything to the last minute. It is a time to build and implement, a time to plan and grow in maturity gradually, and not leave everything to the last minute."

The challenge is not only technical but also cultural. The framework redefines responsibilities, raises demands, and forces a new way of thinking about digital risk. But it also opens up space for a more robust, better prepared, and more competitive ecosystem.

New .pt Registration Rules:

An evolution to strengthen trust and security in the portuguese digital space

Marta Moreira Dias
Member of the Board of Directors of .PT

The transformation of the digital environment and new legal and regulatory requirements, including the Legal Regime for Cybersecurity, are behind the evolution of the .pt Registration rules that will come into effect on July 1, 2026.

The Portuguese top-level domain (.pt) has registered sustained growth over the last few years, establishing itself as one of the best-performing European ccTLDs (country code Top-Level Domains). At the same time, it maintains very low levels of litigation, a residual number of complaints, and an extremely low rate of domain removal due to non-compliance with registration rules. This context demonstrates the maturity of the .pt ecosystem and the adequacy of the rules currently in force.

This is also why the revision of the Registration Rules, scheduled to come into effect on July 1, 2026, does not arise as a response to structural problems or flaws in the existing model. On the contrary, it is a natural and preventive evolution, intended to keep pace with the transformation of the digital environment, incorporate new legal and regulatory requirements, and respond to suggestions submitted by registrars, end consumers, stakeholders, and other market players.

Why was it necessary to revise the 2021 rules?

Since the last revision, carried out in 2021, the European and national legislative and regulatory framework has undergone significant changes. Among the main factors that justified the update of the Registration Rules are the entry into force of new legal instruments, such as the Digital Services Act, the Legal Regime for Cybersecurity, the Geographical Indications Regulation, and various national regulations that impact the management and use of digital identifiers.

The review also sought to reflect the experience accumulated by .PT in managing the national domain, incorporate operational improvements suggested by registrars, and align procedures with internal initiatives and processes developed in the meantime. These new rules therefore adequately reflect the increased demands for security, reliability, and accountability placed on the entity managing the national domain.

The central objective was to ensure that the rules remain clear, up-to-date, proportionate, and adequate to the challenges of an increasingly demanding digital ecosystem, without compromising the simplicity and efficiency that have characterized the .pt registration model.

Security and cybersecurity: a central axis of the review

Among the factors justifying the update of the .pt Registration Rules, the strengthening of security and cybersecurity requirements applicable to critical Internet infrastructures is particularly relevant.

As the entity responsible for managing the top-level domain corresponding to Portugal, the DNS.pt Association plays an essential role in preserving the stability, resilience, availability, and trust of the national digital ecosystem.

The management of the .pt ccTLD involves responsibilities that transcend the mere registration of domain names, also encompassing the adoption of preventive and reactive mechanisms aimed at mitigating risks and service compromise and other threats that may affect the security of users and the Portuguese Internet itself.

In this context, the entry into force of the new Legal Regime for Cybersecurity is particularly relevant. By formally recognizing .pt as an essential entity, the legislator has concretized and clarified a set of obligations already inherent in the management of a critical digital infrastructure, establishing a more robust framework of responsibilities regarding risk management, security governance, incident prevention, monitoring, reporting, and institutional cooperation.

The revision of the Registration Rules therefore also serves as an instrument for aligning with this new legal framework, ensuring that the terms and conditions applicable to the registration and maintenance of .pt domain names adequately reflect the increased demands for security, reliability, and accountability placed on the managing entity of the national domain.

It is also important to emphasize that this new regulatory framework is not limited to the DNS.pt Association. On the contrary, it promotes a more comprehensive and integrated approach to the security of the .pt ecosystem, clearly extending certain obligations and responsibilities to the various actors in the value chain, particularly registrars.

The security of the .pt digital space increasingly depends on the ability of all those involved to act in a coordinated manner, sharing responsibilities, best practices, and procedures that contribute to the prevention and mitigation of risks.

An update focused on the future

The new .pt Registration Rules represent a thoughtful evolution aligned with the current reality of the digital ecosystem. They do not alter the fundamental principles that contributed to the success of the national domain, but introduce improvements that reinforce security, the quality of registered information, legal compliance, and operational efficiency. This is our commitment, only achievable with the effort of all.

The main changes introduced in the .pt domain registration

Strengthening of data validation and verification mechanisms

One of the most relevant changes is the creation of a specific article dedicated to the validation and verification of data associated with domain name holders. It is now expressly stipulated that data verification is a condition for the registration of .pt domains, for the transfer of ownership, and for changes to essential contact information, such as email address or telephone number. The concepts of "validation" and "verification" have also been introduced into the Registration Rules glossary.

Adjustment of procedural deadlines

The new rules also introduce changes to the deadlines applicable to verification procedures. The deadline for confirmations, corrections, or additions to the data provided is extended from 5 to 10 days, providing greater flexibility for holders and registrars. Additionally, the deadline for analysing domain compliance is suspended while these requests for clarification or documentation are in progress.

Harmonization of registration conditions

Another important novelty is the application of the same registration conditions to .pt and .com.pt domains, simplifying the regulatory framework and promoting greater consistency between the different categories of domain names.

Clarification of the payment regime

The revised rules also establish that all registered domains will be charged, even when they are subsequently removed for not meeting the admissibility conditions stipulated in the rules. The future introduction of a fee applicable to the pending delete period for domains renewed at this stage of the lifecycle is also foreseen, with implementation occurring in a deferred manner.

New instruments for dispute resolution and legal compliance

The revision introduces the possibility of resorting to mediation within the framework of alternative dispute resolution mechanisms related to domain names. On the other hand, the possibility of blocking or redirecting domain names upon notification by a legally competent authority is now foreseen, allowing for a more effective response to situations requiring urgent intervention or compliance with legal requirements.

WHOIS Service Update

The changes also reflect the evolving requirements regarding the protection of personal data, addressed in conjunction with the aforementioned Cybersecurity Legal Regime. In the future, personal data will no longer be published in the WHOIS directory, and it will no longer be necessary to collect consent for this publication.
For legal entities, the name and address will continue to be available, while contact mechanisms will remain.

Autonomous cybercrime and DNS abuse

Trends shape the future of digital attacks

The IOCTA 2026 report describes a rapidly changing scenario where cybercrime becomes more autonomous, more invisible, and more difficult to stop.

Europol warns that, in the coming years, the ability of authorities to respond will depend on the adoption of advanced technologies, lawful access to critical data, and much closer collaboration with the private sector.

One of the most disruptive trends is the emergence of autonomous cybercrime. Criminal groups already use agentive AI systems capable of executing complete attack flows, from information gathering to intrusion, exfiltration, and monetization, with minimal human intervention. As these tools become more accessible, attackers are able to distance themselves from operations, reducing the risk of identification and transforming cybercrime into an increasingly intangible threat.

The report also highlights the evolution of hybrid threats, where state-sponsored actors and cybercrime groups collaborate fluidly. DDoS attacks continue to be used to undermine public trust and generate political instability, while hacker coalitions combine intrusions, data theft, and fraud schemes. The result is a dynamic attack ecosystem, where boundaries between espionage, sabotage, and financial crime become increasingly blurred.

At the heart of this new reality is DNS abuse, which IOCTA identifies as one of the most exploited critical infrastructures for online attacks and fraud. DNS acts as a bridge between criminal infrastructure and victims, allowing offenders to launch phishing campaigns, distribute malware, or control botnets through temporary domains. Criminals exploit the absence of automatic reporting mechanisms and the slowness of international judicial requests. By the time a malicious domain is finally blocked, the attack has often already reached scale.

DNS is similarly essential for ransomware and C2 operations, with botnets using residential proxies to mask traffic and mimic legitimate users. This technique makes detection difficult and dismantling criminal infrastructure significantly more complex.

The IOCTA 2026 reinforces that the future of cybercrime will be marked by distributed infrastructure, opaque cryptocurrencies, fragmented markets, and autonomous AI. To reduce the "speed gap" between attackers and authorities, Europol advocates a response based on technological innovation, lawful access to essential data, and continuous international cooperation. Without this adaptation, cybercrime will continue to gain ground.

The impact of Artificial Intelligence on DNS abuse

José Casinha
Member of the Board of Directors of .PT

AI has not changed the nature of DNS abuse attacks, but there has been an increase in scale, speed, and sophistication. The impact of autonomous agents is still uncertain, and a defensive response requires sustained, evidence-based adaptation.

The two major categories of Artificial Intelligence technologies, LLMs and autonomous agents, interact with DNS abuse in fundamentally distinct ways, and any serious analysis must treat them separately. The current state of abuse is dominated by LLM-assisted workflows; abuse driven by autonomous agents remains a short- to medium-term concern, not a documented present reality.

One of the most important findings when examining the role of AI in DNS abuse is that the fundamental attack vectors have not changed. Phishing, domain spoofing, malicious records, infrastructure-based campaigns, and SEO manipulation are not new phenomena—they have been operational tools of cybercriminals for over a decade. What AI has changed is not the nature of these attacks, but the economics and efficiency with which they can be executed.

This distinction is extremely relevant. It means that existing defensive frameworks, policy instruments, and detection approaches remain conceptually valid. The challenge is not to design responses for entirely new threat categories, but to ensure that existing responses can operate at the speed and scale that AI-assisted attacks now demand.

How AI is influencing the attack landscape

Perhaps the most consequential effect of AI on DNS abuse in the short term is the democratization of capabilities, that is, we are seeing a clear reduction in barriers to entry. Tasks that previously required significant technical knowledge are now accessible to actors with far fewer skills.

This is not just a quantitative change. It is a structural transformation in who can conduct sophisticated abuses.

Beyond content, AI tools — particularly autonomous agents — have the potential to transform how infrastructure supporting abuse attacks is created and managed. Domains can be registered, hosting environments provisioned, and campaigns reconfigured with reduced human intervention. When infrastructure is detected and eventually disabled, replacement infrastructure can be automatically created and activated without any human intervention.

This has implications that go beyond operational efficiency. It begins to challenge the economic logic of defensive takedown operations: if the cost of replacing disabled infrastructure approaches zero and the replacement can be automated, the deterrent effect of disruption is substantially weakened.

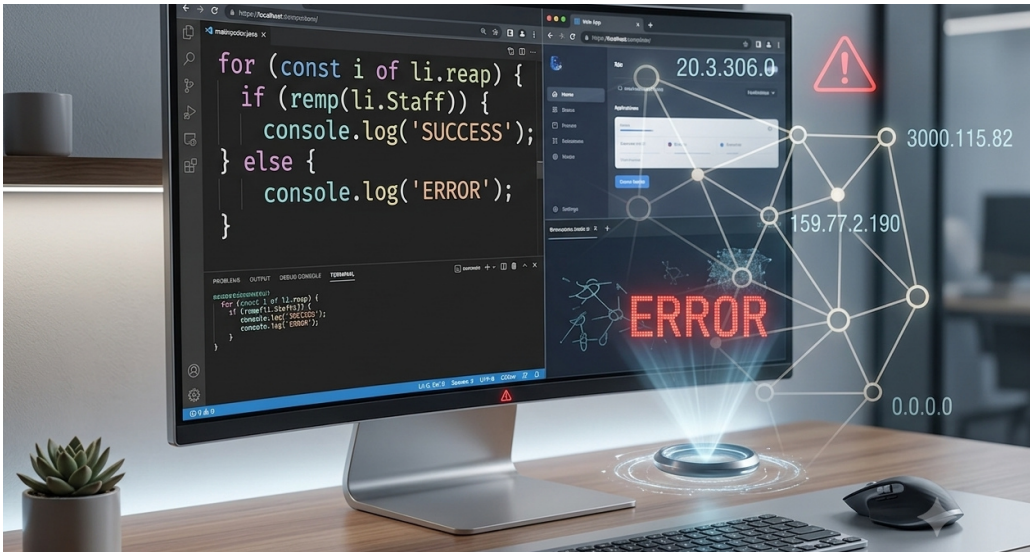
The convergence of scale and personalization with the ability to conduct campaigns that are simultaneously broad and individually tailored represents a qualitative shift in attack capabilities that was virtually unattainable before generative AI.

The role of existing AI in defensive infrastructure

The same capabilities that enable AI-assisted abuse are available for defense activities, with AI defensive applications in the context of DNS abuse playing a key role.

It is important to recognize that AI-powered defenses are not a future aspiration; they are already embedded in parts of the DNS ecosystem. Record risk assessment systems that flag potentially abusive domain registrations before they are completed already incorporate AI-adjacent techniques. The relevant question is not whether to introduce AI into the defensive strategy, but how to extend and improve existing capabilities.

Deploying AI in DNS abuse defensive contexts carries its own risks that require careful management. Hallucination, the generation of confident but incorrect outputs, is a real failure mode of LLMs that is particularly dangerous in high-risk abuse mitigation contexts. A false positive that incorrectly classifies a legitimate domain as malicious can cause real harm; a false negative that fails to detect malicious activity creates ongoing risk.



Perhaps the most consistent observation about DNS abuse in the age of AI is that this type of activity remains fundamentally dependent on human victims. DNS abuse is effective because it can persuade a human to click a link, entering credentials, downloading a file, or authorizing a payment. The attack chain ends with human behaviour, and that is the ultimate goal that gives value to the abuse.

This observation has an important implication: the evolution of AI-assisted DNS abuse will be reactive to how humans themselves change.

This means that all the AI investment on the attack side ultimately serves the purpose of exploiting human cognitive vulnerabilities: limitations in language comprehension, susceptibility to social engineering, the heuristics that guide online decision-making, and the varying levels of digital literacy among different user populations.

As potential victims develop better intuitions for AI-generated content, attackers adapt to produce content that defeats those intuitions. This creates a co-evolutionary dynamic rather than a one-time capability shift.

The only scenario that fundamentally alters this picture is the emergence of machine-to-machine abuse — attacks in which both the victim and the attacker are automated, and the harmful outcome is achieved without a human ever being involved in the cycle. This remains a future possibility and not a present reality, but the trajectory of AI agent development makes it a scenario that forward-looking analysis cannot ignore.

Short-term trajectory

Looking ahead, three developments seem most likely to shape the impact of AI on DNS abuse in the short term.

Increased scale and speed are the most certain short-term consequences. Already demonstrated capabilities — automated domain screening, rapid content generation, programmatic infrastructure management — will continue to improve and become more widely available. Campaigns that currently require significant operational effort will become more accessible and faster to execute.

Increased sophistication is the second trajectory. Not because AI will introduce fundamentally new attack techniques, but because the availability of capable tools for a wider range of actors means that more sophisticated attack patterns will become routine rather than exceptional.

The emerging activity of autonomous agents represents the third and less certain trajectory. As the capabilities of AI agents mature, the possibility of campaigns running with minimal human direction becomes more realistic. The implications for both detection and deterrence are significant.

Conclusion

AI is not revolutionizing DNS abuse in the dramatic way some narratives suggest, nor is it a fringe concern that can be safely postponed. The accurate characterization is that it is an accelerator—a set of capabilities that makes existing attack patterns faster, cheaper, and more accessible, without altering their fundamental nature.

The plots are old. The scale and speed are changing. The abuse economy is shifting in ways that favour actors who previously lacked the resources or skills to operate with sophistication. And the structural conditions—complete automation of the attack lifecycle, machine-to-machine abuse, autonomous infrastructure management—are approaching viability even if they are not yet the norm.

The appropriate response is neither alarm nor indifference, but sustained, evidence-based adaptation: improving detection, strengthening policy frameworks, deploying defensive AI thoughtfully and with adequate oversight, and maintaining community coordination that allows the field to clearly see what is really happening — as opposed to what is feared or assumed.

The human remains, for now, both the target and the essential link in the abuse chain. Understanding that the threat evolves in response to how humans change — how they interact with AI, how their trust calibration adapts, how their digital literacy develops — is perhaps the most important analytical framework for anticipating what comes next.

Cooperation to combat cybercrime

EU ratification of UN cybercrime convention boosts collective capabilities

The European Union's formal adoption and consent to the United Nations Convention against Cybercrime is an important step in harmonizing offenses and strengthening police and judicial cooperation, and accelerates cross-border access to electronic evidence, one of the biggest challenges in criminal investigation.

Digital crime is no longer a technical phenomenon and has become an economic, social and geopolitical problem. Cybersecurity Ventures estimates indicated that, by 2025, cybercrime could cost the global economy more than $10 trillion, with the potential to exceed $12 to $15 trillion. Organizations and citizens face more frequent, faster and more automated attacks, driven by AI tools that reduce costs for attackers and amplify the impact.

Cooperation between various entities and countries is highlighted as a crucial factor in a context of globalized cybercrime, where pressure also increases with technological evolution. In 2024, the United Nations moved forward with a United Nations Convention against Cybercrime that creates a common minimum basis for cooperating, investigating, and responding to attacks that cross borders in seconds, and now the European Union has formalized an accession that had already been approved in December of last year.

The Convention defines a set of digital crimes, establishes rules for the collection and sharing of electronic evidence, and strengthens safeguards for fundamental rights. The EU underlines that this agreement strengthens the EU's capacity to combat cybercrime together with international partners and expands international cooperation among the 112 UN Member States that are not party to the Budapest Convention on Cybercrime.

In this sense, the UN Convention responds to three central needs:

1

Faster and more effective investigations, creating more agile mechanisms to access essential data, always with judicial oversight.

2

Common minimum rules, reducing grey areas and facilitating joint action, especially in coordinated attacks involving multiple jurisdictions.

3

Protection of rights in a hostile digital environment, incorporating principles aligned with the EU Charter of Fundamental Rights.

In a digital ecosystem where an attack can originate from anywhere and target any organization, the European Union recognizes that cooperation is the only strategy to ensure a global fight, reduce risks, accelerate responses, and protect citizens, businesses, and democracies.

IberianQCI:

Portugal and Spain connect Quantum Communications Infrastructures

The goals for the three-year project are ambitious and include contributing to the development of a scalable European quantum communications ecosystem.

The IberianQCI project, led by Indra Space, was officially launched as the Iberian segment of the future European quantum communications network, EuroQCI, created to ensure highly secure connections between the Member States of the European Union and protect critical infrastructure and sensitive information against future threats.

With a planned extent of three years, IberianQCI aims to interconnect the national quantum communications infrastructures of Portugal and Spain, creating an integrated network that is fully interoperable with the European architecture. The initiative adds to the work already developed within the scope of EuroQCI and national projects such as PTQCI (Portuguese Quantum Communication Infrastructure) and DISCRETION, the latter led by Portugal to strengthen the security of military networks.

Funded by the Connecting Europe Facility (CEF), the project is coordinated by Portugal through Indra Space, in collaboration with scientific, technological and industrial entities from both countries. Among the Portuguese partners are Infraestruturas de Portugal, IP Telecom, Instituto de Telecomunicações, Altice Labs and Instituto Superior Técnico. On the Spanish side, the Polytechnic University of Madrid, Telefónica, the Consejo Superior de Investigaciones Científicas (CSIC), the Instituto de Ciências Fotónicas de Barcelona, the Centro de Supercomputación de Galiza and the University of Vigo are participating.

The development of quantum communications is vital to ensuring global cybersecurity in the face of the future capabilities of quantum supercomputers. These communication systems allow for ultra-secure and nearly impenetrable data transmission, serving as a pillar for the protection of critical infrastructure, government data and financial institutions. Unlike traditional networks, quantum connections allow the distribution of tamper-proof cryptographic keys, based on physical principles that make it impossible to intercept them without immediate detection.

Currently, fiber optics limits the transmission of quantum keys to about 100 kilometers, but the use of satellites eliminates this barrier, allowing global coverage with less signal attenuation.

The IberianQCI hybrid architecture combines terrestrial and space components. A cross-border link is planned between Vigo and Valença, using trusted nodes that strengthen connectivity between the two countries and integrate existing national networks. The space component will include three optical stations, in Madrid, Barcelona and southern Portugal, connected to the terrestrial segment in Lisbon. These stations will allow secure communications with the EAGLE-1 demonstrator satellite, in low Earth orbit, and with the future SAGA constellation, ensuring the distribution of quantum keys even between countries without common borders.

Evaluation of national digital resilience: Literacy, good practices and training need to be reinforced

The 7th edition of the Cybersecurity Report in Portugal, under the theme Society, outlines the readiness of Portuguese society to respond to cyber risks, identifying key weaknesses and emphasizing the need to enhance digital skills.

The document complements the Cybersecurity Report in Portugal, theme Risks & Conflicts, which was published in 2025 by the National Cybersecurity Center (CNCS), and seeks to offer an integrated view of the risk landscape in cyberspace of national interest, addressing behaviours, technological maturity and vulnerabilities in a context in which threats evolve quickly.

As individuals and companies increase their use of digital services, exposure to risks also increases, particularly in the areas of social engineering and fraud. The report identifies the main trends in incidents that have affected national infrastructures and confirms that the vast majority continue to be concentrated in the private sector, representing around 78% of the total, but a dangerous tactical mutation is observed in the attackers' targets.

The data reveals a significant worsening in Public Administration, where incidents increased by 67% in the space of one year, between 2023 and 2024. Local administration stands out as one of the most vulnerable targets, with around a quarter of municipal councils reporting active cyberattacks on their ecosystems during 2024 — a clear sign of structural weaknesses.

With regard to the types of attack vectors, the predominance of techniques that exploit human error and psychological manipulation remains. Phishing, smishing and vishing continue to be the preferred entry points for criminal scams, now combined with more sophisticated forms of social engineering. Online scams, account theft and compromise, and ransomware attacks, which paralyze operational services and demand large ransoms, remain among the most frequent threats. The report also highlights the growth of CEO Fraud, false recruitment campaigns and incidents involving infostealers, which accounted for more than 80% of malware activity observed in Q3 2025.

Companies still unprepared to respond to threats

Portugal appears as the fifth country with the lowest percentage of incidents among small businesses (10–49 workers), suggesting that digitalization has been accompanied by some adoption of security measures.

Despite the increase in incidents recorded by CERT.pt in 2024, a comparative analysis with Eurostat data indicates that the percentage of Portuguese companies affected by incidents impacting the availability of ICT services, destruction or modification of data, or disclosure of confidential information, was lower than the European average.

Still, most organizations have not reached high levels of maturity. Advanced firewalls, intrusion detection systems and strict access management policies continue to be primarily a reality for large enterprises, leaving smaller supply chains and partners exposed to indirect risks. Public Administration faces similar challenges: despite progress in digitalization and the adoption of security measures, these prove to be insufficient to prevent incidents with national impact.

Reduce the attack surface and strengthen cyber resilience

The report highlights that, although there is growing recognition of the importance of cybersecurity, this progress has not yet translated into an effective reduction in negative impacts. The perception of risk is high and organizations are reinforcing investment, particularly through hiring specialized services. However, recruiting qualified professionals remains a widespread obstacle, creating weaknesses due to a shortage of internal resources.

The lack of awareness and ongoing training is another critical point.

Most Portuguese companies do not promote regular cybersecurity training actions, nor do they integrate mandatory training for employees. The use of long-range campaigns targeted at the general public also remains small, limiting the dissemination of basic cyber hygiene practices.

Given the vulnerabilities identified, the report recommends strengthening digital literacy and associating it, from an early age, with specific cybersecurity literacy. It also advocates for intensive human resource training, with a special focus on Public Administration, especially at the municipal level, and on small and medium-sized enterprises, which continue to lack a budget dedicated to digital protection. Increasing the reach and effectiveness of public awareness actions is also pointed out as essential to equip citizens with skills that allow them to mitigate fraud and scams before they reach home or business networks.

78%

of incidents occur in private sector companies

+67%

growth in attacks against Public Administration between 2023 and 2024

25%

of local administrations reported detecting cyberattacks in 2024

19ª Edição | Primeiro semestre 2026

19th Edition | First half of 2026