

bilingual edition

ptsoc {news}

Primeiro semestre 2026 | First half of 2026

#19

Novo Regime Jurídico da Cibersegurança

Novas regras de registo em .pt

Cibercrime autónomo e abuso de DNS

O impacto da IA no abuso de DNS

Radiografia da resiliência digital nacional

Ficha técnica

Esta publicação é produzida pelo .pt

19ª Edição | Primeiro semestre 2026

Edição e design gráfico: Casa dos Bits – Edições Lda.



Abra a chave da segurança da internet



Subscreva
a newsletter
PTSOCNews



Conteúdos deste documento ao abrigo da Licença Creative Commons - Atribuição-Não Comercial 4.0 Internacional. Ele pode ser copiado e redistribuído por qualquer meio ou formato, misturado, transformado e usado para a elaboração de outro material que deverá ser distribuído usando a mesma licença. Para mais detalhes consultar as condições de uso em <http://creativecommons.org/licenses/by/4.0/>
Todos os direitos reservados PTSOC News.



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.

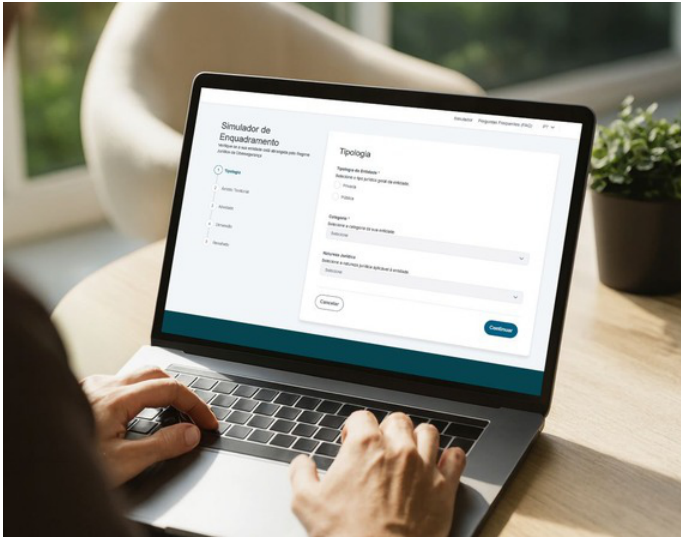
Mais do que uma atualização visual, esta nova fase traduz uma visão estratégica: posicionar a PTSOC News como um hub de informação e cooperação, capaz de acompanhar os desafios crescentes da segurança digital e de apoiar profissionais e organizações na adoção de boas práticas.

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.

Índice

Novo Regime Jurídico da Cibersegurança	2
Novas Regras de Registo de .pt	6
Cibercrime autónomo e abuso de DNS	9
O impacto da IA no abuso de DNS	10
Convenção das Nações Unidas contra o cibercrime	13
IberianQCI: Portugal e Espanha ligam infraestruturas	14
Radiografia da resiliência digital nacional	15

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, abrangendo 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 autônomo 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 autônomo, 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

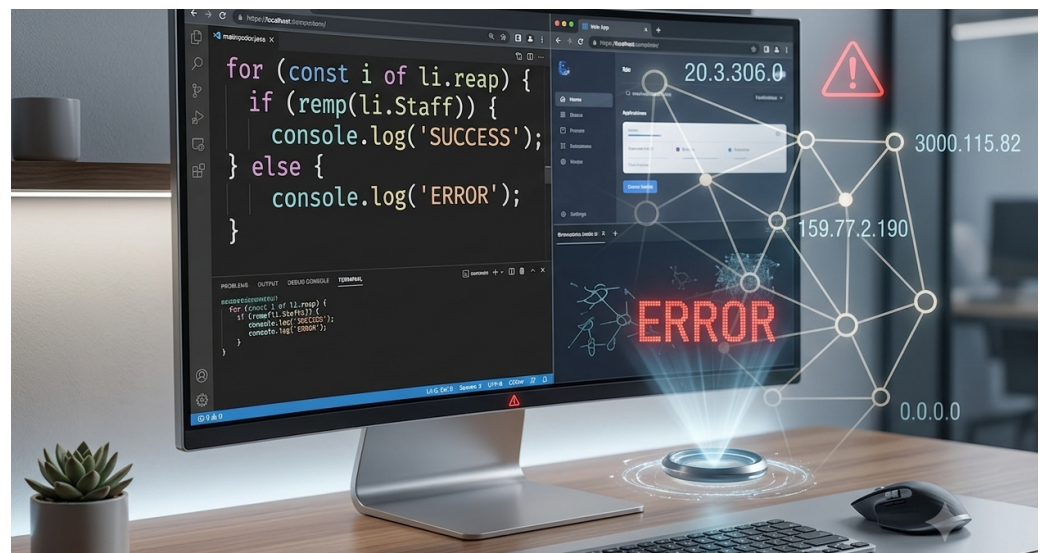
de substituir infraestrutura desativada se aproxima de zero e a substituição pode ser automatizada, o efeito dissuasor da perturbação fica substancialmente enfraquecido. A convergência de escala e personalização com capacidade de conduzir campanhas que são simultaneamente amplas e individualmente adaptadas 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 prospectiva não pode ignorar.

Trajетória 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.

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.

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.

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

.pt



19ª Edição | Primeiro semestre 2026