

ICANN
POLICY FORUM

86

SEVILHA, ESPANHA

8 a 11 de junho de 2026



ÍNDICE

- 1 Introdução
- 2 Nova ronda do Programa de Novos gTLD
- 3 Exatidão dos dados de registo e prevenção de abuse
- 3 Principais temas debatidos no ccNSO
- 4 O papel dos ccTLD na transformação digital
- 4 Transformação digital em África: o caso do .KE
- 5 Resiliência dos ccTLD: as lições da Ucrânia
- 6 Continuidade operacional e Business Continuity
- 6 Exatidão dos registos públicos da IANA
- 7 Cibersegurança e evolução do quadro regulamentar
- 8 Evolução do modelo regulatório da Rússia
- 9 Modernização do .tr e reforço do combate ao DNS Abuse
- 10 Considerações finais



INTRODUÇÃO

Entre os dias **8 e 11 de junho de 2026**, realizou-se, em Sevilha, a **ICANN86 Policy Forum**, uma das três reuniões públicas anuais da Internet Corporation for Assigned Names and Numbers (ICANN). Ao contrário da Community Forum e da Annual General Meeting (AGM), a Policy Forum é predominantemente dedicada ao desenvolvimento de políticas, constituindo um espaço privilegiado para o trabalho entre as diferentes comunidades que integram o modelo *multistakeholder* da ICANN.

A reunião decorreu num momento particularmente relevante para o ecossistema do Sistema de Nomes de Domínio (DNS), marcado pelo arranque da nova ronda do Programa de Novos gTLD, pelo aprofundamento das discussões sobre a resiliência das infraestruturas críticas da Internet e pelo crescente impacto da evolução do quadro regulamentar internacional na atividade dos operadores de registos de nomes de domínio.

Os trabalhos do Governmental Advisory Committee (GAC) e do Country Code Names Supporting Organization (ccNSO) centraram-se, em larga medida, na preparação da nova ronda de novos gTLD, na continuidade operacional dos ccTLD, na cibersegurança e na adaptação do ecossistema DNS aos novos desafios regulatórios e geopolíticos.



NOVA RONDA DO PROGRAMA DE NOVOS GTLD

Um dos principais temas da ICANN86 foi o ponto de situação sobre a nova ronda do Programa de Novos gTLD, cuja fase de candidaturas decorre entre 30 de abril e 12 de agosto de 2026, mediante o pagamento de uma taxa de candidatura de 227 000 dólares norte-americanos. Foi igualmente confirmado que a divulgação pública das candidaturas recebidas ("Reveal Day") ocorrerá durante os meses de outubro e novembro.

A sessão permitiu esclarecer diversos aspetos relacionados com o processo de avaliação das candidaturas, incluindo os mecanismos destinados a evitar conflitos entre novas strings e domínios de topo já existentes ou reservados.

Neste contexto, suscitou-se uma questão particularmente relevante relacionada com a eventual similaridade fonética entre novos gTLD candidatos e TLD's já delegados ou nomes reservados. Em resposta, foi explicado que o processo de avaliação contemplará expressamente a análise da similaridade visual, fonética e conceptual das strings candidatas, podendo igualmente ser apresentados mecanismos de oposição ("String Confusion Objection") pelas partes interessadas sempre que entendam existir risco de confusão para os utilizadores.

A discussão demonstrou a preocupação da comunidade em assegurar que a expansão do espaço de nomes de domínio continua a ser compatível com a estabilidade, previsibilidade e segurança do DNS.

O "GAC Communiqué – Seville, Spain" pode ser consultado [aqui](#).



EXATIDÃO DOS DADOS DE REGISTO E PREVENÇÃO DE ABUSE

No âmbito dos trabalhos do Governmental Advisory Committee (GAC), foi igualmente debatida a problemática da exatidão dos dados de registo dos nomes de domínio e a sua relação com a prevenção do abuso no DNS.

Durante a sessão dedicada ao tema foram apresentados os requisitos atualmente previstos no WHOIS Accuracy Program Specification do Registrar Accreditation Agreement (RAA) de 2013, que impõem aos registrars a validação e verificação de determinados elementos dos dados dos titulares após o registo do nome de domínio.

Foi igualmente apresentada a análise desenvolvida no âmbito do estudo INFERMAL sobre dns abuse, cujos resultados indicam que a verificação apenas após o registo poderá estar associada a um aumento significativo de registos maliciosos, por permitir que agentes maliciosos utilizem o domínio antes da conclusão dos procedimentos de validação.

Neste contexto, encontra-se em discussão, no âmbito de um grupo de trabalho do GAC, a possibilidade de recomendar ao ICANN a revisão dos atuais requisitos aplicáveis aos registrars, passando a exigir que a verificação da identidade do titular seja concluída antes da efetivação do registo do domínio, procurando

reforçar as medidas preventivas de combate ao dns abuse e aumentar a fiabilidade dos dados de registo.

PRINCIPAIS TEMAS DEBATIDOS NO CCNSO

Como habitualmente, as reuniões do ccNSO centraram-se na partilha de experiências entre operadores de ccTLD's e na discussão dos principais desafios técnicos, operacionais e estratégicos que atualmente afetam estes registries.



O PAPEL DOS CCTLD NA TRANSFORMAÇÃO DIGITAL

Destacamos a apresentação realizada pelo .rw (Ruanda), que apresentou a integração do registo de nomes de domínio na plataforma governamental IremboGov, através da qual os cidadãos podem aceder a um vasto conjunto de serviços públicos digitais, como a emissão de certidões de nascimento, cartas de condução ou outros atos administrativos.

Esta plataforma permite igualmente o registo de nomes de domínio sob .rw, constituindo um exemplo de integração entre a infraestrutura nacional da Internet e os serviços públicos digitais. Foi ainda referido que cerca de 31% do valor pago pelo registo dos domínios reverte diretamente para a plataforma governamental, tendo já sido registados mais de 300 domínios através deste mecanismo.

O exemplo apresentado demonstra como os operadores de ccTLD assumem muitas vezes, e independentemente do modelo de governação, um papel ativo nas estratégias nacionais de transformação digital, atuando como parceiros do setor público na disponibilização de serviços digitais aos cidadãos. Neste caso, em particular, a entidade responsável pela gestão do registry integra, ela própria, o setor público. Este modelo de governação, embora relativamente comum no continente africano, afasta-se daquele que é habitualmente adotado no contexto europeu e, que é seguido nas tendências mundiais. A relevância deste tipo de

parcerias tem-se revelado no ecossistema global como de sucesso e nunca dependentes dos modelos de governação de cada registry.

TRANSFORMAÇÃO DIGITAL EM ÁFRICA: O CASO DO .KE

A apresentação realizada pelo registry do .ke destacou a evolução do ecossistema digital africano e o papel que os ccTLDs podem desempenhar na promoção da transformação digital.

Foi referido que o Quénia apresenta uma das populações mais jovens do mundo, sendo os dispositivos móveis o principal meio de acesso à Internet, persistindo, contudo, desafios significativos ao nível da inclusão digital e da presença online das pequenas e médias empresas.

O registry apresentou um crescimento aproximado de 30% no número de registos sob .ke, contando atualmente com uma rede superior a 200 registrars acreditados e beneficiando de uma estreita colaboração com entidades como o ICANN, a KENIC e a AFRALTI.

Entre as iniciativas em desenvolvimento destaca-se a intenção de integrar o processo de constituição de empresas com o registo do respetivo nome de domínio, permitindo que novas empresas estabeleçam desde o início uma presença digital, contribuindo para acelerar a digitalização das PME e o desenvolvimento da economia digital.

RESILIÊNCIA DOS CCTLD: AS LIÇÕES DA UCRÂNIA

A apresentação realizada pelo .ua (Ucrânia) constituiu um dos momentos mais marcantes das reuniões do ccNSO.

Partindo da experiência acumulada desde o início da guerra, foi defendido que a resiliência das infraestruturas críticas não resulta da capacidade de resposta à crise, mas sim da preparação efetuada muito antes da sua ocorrência.

Entre os principais fatores identificados destacaram-se:

- ▶ a distribuição geográfica da infraestrutura DNS;
- ▶ a adoção de elevados padrões de segurança e confiança;
- ▶ a definição de procedimentos internos robustos;
- ▶ a preparação das equipas;
- ▶ a manutenção de relações de confiança entre registry, registrars e restante comunidade técnica.

A apresentação evidenciou igualmente que a resiliência constitui hoje um elemento estrutural da gestão dos ccTLD, deixando de ser encarada apenas como uma componente tecnológica para assumir igualmente uma dimensão organizacional e estratégica.



CONTINUIDADE OPERACIONAL E BUSINESS CONTINUITY

Os debates realizados no âmbito do ccNSO centraram-se igualmente no desenvolvimento do estudo sobre o eventual papel da IANA em cenários de desastre que afetem operadores de ccTLD. Utilizando a metodologia "Double Diamond", o grupo de trabalho constituído para realizar esta análise encontra-se atualmente na fase de desenvolvimento de cenários de crise, procurando identificar de que forma a IANA poderá prestar apoio a um operador sem comprometer a autonomia do respetivo ccTLD ou interferir com os procedimentos formais de transferência de gestão. Os primeiros resultados apontam para a necessidade de distinguir claramente a responsabilidade primária do operador pela continuidade do serviço de um eventual papel complementar da IANA, devidamente estruturado e preparado antecipadamente. Foi igualmente sublinhado que a diversidade de modelos de governação, enquadramentos legais, infraestruturas técnicas e dimensão dos diferentes ccTLD's impede a adoção de uma solução uniforme para todos os registos.

O estudo pretende analisar o eventual papel que a IANA poderá desempenhar em situações extremas de interrupção prolongada da operação de um ccTLD, procurando identificar princípios orientadores que permitam assegurar a continuidade do serviço sem comprometer a autonomia dos operadores nacionais.

Embora ainda numa fase exploratória, esta iniciativa reflete a crescente preocupação da comunidade internacional com a continuidade operacional das infraestruturas críticas da Internet, sobretudo num contexto marcado pelo aumento das ameaças de cibersegurança, dos conflitos armados e da crescente dependência dos serviços digitais.

EXATIDÃO DOS REGISTOS PÚBLICOS DA IANA

Outro dos temas estratégicos abordados foi a exatidão da informação constante dos registos públicos da IANA relativos aos ccTLD's. Os trabalhos em curso procuram identificar mecanismos que permitam melhorar a atualização e fiabilidade destes registos, uma vez que foram identificados diversos casos de informação desatualizada ou incorreta, não existindo atualmente mecanismos formais que assegurem a respetiva correção. A discussão assume particular relevância atendendo ao papel que os registos da IANA desempenham na identificação oficial dos gestores dos ccTLD's e na aplicação dos princípios constantes da RFC 1591. O grupo de trabalho prevê elaborar um documento com propostas de mecanismos graduais de conformidade e atualização de informações, que será posteriormente submetido a consulta da comunidade.

CIBERSEGURANÇA E EVOLUÇÃO DO QUADRO REGULAMENTAR

As reuniões do ccNSO confirmaram igualmente que o enquadramento regulamentar europeu continua a assumir uma influência crescente sobre a atividade dos operadores de registos.

Foram abordados diversos instrumentos legislativos recentemente aprovados ou em desenvolvimento, designadamente a **Diretiva NIS2**, o **Cybersecurity Act** e o **Cyber Resilience Act**, todos eles com impacto direto ou indireto sobre a gestão das infraestruturas DNS.

Foi igualmente destacada a publicação das **ENISA Technical Implementation Guidance**, que clarificam diversos aspetos relacionados com a implementação das medidas de cibersegurança previstas na legislação europeia, incluindo referências específicas à utilização de software open source e à ausência de relações contratuais típicas quando este é utilizado.

Outro aspeto relevante foi a crescente valorização do **DNSSEC**, cuja implementação surge recomendada no Regulamento de Execução (UE) 2024/2690 enquanto mecanismo essencial para reforçar a autenticidade e integridade das respostas DNS.

Durante as discussões foi ainda deixado um alerta que merece particular atenção: embora uma única iniciativa legislativa dificilmente constitua um fator de fragmentação da Internet, a acumulação de múltiplos regimes jurídicos nacionais poderá, no futuro, comprometer a interoperabilidade global do DNS. Esta preocupação foi transversal a várias intervenções e evidencia a importância de preservar uma abordagem harmonizada à governação da Internet.



EVOLUÇÃO DO MODELO REGULATÓRIO DA RÚSSIA

O registry dos domínios .RU e .РФ apresentou as alterações decorrentes da Lei Federal n.º 569-FZ, cuja entrada em vigor está prevista para 1 de setembro de 2026. Esta legislação introduz uma alteração relevante no modelo de registo de nomes de domínio, passando a exigir a verificação obrigatória da identidade dos titulares através do sistema governamental USIA, tanto para novos registos como para determinadas operações sobre domínios já existentes.

A nova lei reforça igualmente a intervenção do Estado na definição das regras de registo e no processo de acreditação dos registrars, que passam a estar sujeitos a requisitos formais definidos por legislação governamental. Para os registrars, esta alteração implica a necessidade de integração técnica dos seus sistemas com o USIA, a adaptação dos procedimentos de atendimento aos clientes, a atualização dos dados dos titulares e a realização de um novo processo de acreditação.

Foram também identificados desafios relevantes na implementação deste modelo, designadamente nos casos em que os dados constantes dos registrars não coincidam com os registos governamentais, bem como no tratamento de titulares estrangeiros, que poderão não conseguir cumprir os mesmos mecanismos de verificação. Do ponto de vista do registry, a lei

atribui ainda novas responsabilidades operacionais, incluindo a possibilidade de atuar como registrar para entidades governamentais.

A apresentação evidenciou, assim, uma evolução para um modelo de verificação de identidade mais centralizado e associado a infraestruturas públicas nacionais, reforçando o controlo regulatório sobre o registo de domínios, mas criando simultaneamente desafios técnicos, operacionais e comerciais para registrars, titulares e para o próprio registry.



MODERNIZAÇÃO DO .TR E REFORÇO DO COMBATE AO DNS ABUSE

O registry turco apresentou igualmente os resultados da implementação da plataforma TRABIS, responsável pela modernização da gestão do domínio .tr. Desde a entrada em funcionamento do novo sistema foram registados cerca de 988 mil novos domínios, ultrapassando atualmente os 1,3 milhões de domínios ativos.

A apresentação incidiu sobretudo sobre as medidas adotadas para prevenção de DNS Abuse, destacando-se o desenvolvimento do sistema AZAD, baseado em inteligência artificial para deteção de phishing e domínios maliciosos, bem como da plataforma KULE, destinada à gestão coordenada de incidentes com as autoridades competentes.

Foi igualmente apresentada uma política de nomes reservados para setores considerados sensíveis, como banca, serviços financeiros e organismos públicos, exigindo procedimentos adicionais de verificação para reduzir fenómenos de fraude e usurpação de identidade. O registry salientou ainda que a definição das respetivas políticas resulta de um modelo participativo ("bottom-up"), envolvendo registrars, especialistas técnicos, entidades públicas e outras partes interessadas.



CONSIDERAÇÕES FINAIS

A ICANN86 confirmou várias tendências que se têm vindo a consolidar nos últimos anos.

Desde logo, ficou evidente que os operadores de ccTLD são hoje reconhecidos como infraestruturas críticas essenciais ao funcionamento da economia digital, assumindo responsabilidades crescentes em matéria de cibersegurança, continuidade operacional e confiança dos utilizadores.

Paralelamente, verificou-se que a evolução legislativa internacional — em particular no contexto europeu — está a exercer uma influência cada vez mais significativa sobre a gestão dos nomes de domínio, exigindo aos operadores uma adaptação contínua dos seus processos técnicos, operacionais e jurídicos.

A nova ronda do Programa de Novos gTLD representa igualmente um marco importante para o ecossistema do DNS, cuja implementação continuará a ser acompanhada de perto pela comunidade internacional ao longo dos próximos meses.

Para o **.PT**, os temas debatidos em Sevilha apresentam particular relevância, não apenas pelo alinhamento com os processos atualmente em curso ao nível da implementação do Regime Jurídico da Cibersegurança e da revisão das Regras de Registo, mas também pela preparação da **ICANN88**, que terá lugar em

Lisboa, em março de 2027. Neste contexto, a participação ativa do .PT nos diferentes fóruns da ICANN continua a revelar-se essencial para acompanhar a evolução das políticas internacionais, antecipar desafios futuros e reforçar a sua posição enquanto operador de referência no panorama europeu dos ccTLD.

Ainda no âmbito da preparação da ICANN 88 Lisboa, reunimos com a equipa de eventos da ICANN para alinhar os detalhes da organização do evento. Esta reunião foi de extrema importância para garantir o bom desenvolvimento dos preparativos e reforçou a nossa convicção de que a ICANN 88 Lisboa será um sucesso.



pt.pt
facebook.com/dns.pt
pt.linkedin.com/in/dnspt

.pt

