ICANN86 em Sevilha: por que acompanhar a governança da Internet é essencial para todos
ICANN 86 7 de junho de 2026
*Por Nivaldo Cleto**

Cheguei a Sevilha, na Espanha, para participar da ICANN86, que acontece entre os dias 8 e 11 de junho de 2026. O encontro internacional reúne governos, empresas, comunidade técnica, academia e sociedade civil para discutir os rumos da governança da Internet. Para muitos, esses debates parecem distantes do dia a dia. Mas a verdade é que decisões tomadas nesses fóruns influenciam diretamente a segurança, a estabilidade, a liberdade e o funcionamento da Internet que todos usamos.

A ICANN é uma das organizações centrais no sistema global de nomes de domínio, os conhecidos endereços da Internet. É graças a essa coordenação técnica e política que conseguimos acessar sites, enviar e-mails, usar serviços digitais e conectar pessoas e empresas em escala mundial. Por trás de algo aparentemente simples, como digitar um endereço no navegador, existe uma complexa estrutura internacional de cooperação.

Esse modelo é chamado de multissetorial. Ele não pertence apenas a governos, nem somente a empresas ou técnicos. A Internet foi construída com base na participação conjunta de diferentes setores da sociedade. E é justamente essa diversidade que ajuda a garantir equilíbrio, inovação, transparência e proteção contra decisões centralizadas que poderiam limitar o acesso, a liberdade e a interoperabilidade da rede.

Minha missão nesse ambiente não é defender isoladamente o setor empresarial brasileiro, mas acompanhar as tendências, os debates e as políticas discutidas na ICANN para levar ao CGI.br as preocupações, oportunidades e alertas que surgem nesse ecossistema global. O papel de quem

participa é observar, dialogar, compreender os impactos e contribuir para que o Brasil esteja atento às mudanças que podem afetar usuários, empresas, governos e toda a sociedade conectada.

Um dos grandes temas desta ICANN86 é o combate ao abuso no DNS. O DNS é o sistema que traduz nomes de domínio em endereços técnicos compreendidos pelos computadores. Quando criminosos utilizam domínios para golpes, phishing, fraudes, disseminação de malware ou outras práticas ilícitas, toda a sociedade é afetada. Mitigar esses abusos é essencial para proteger usuários, empresas e instituições.

Esse desafio se tornou ainda mais complexo com a inteligência artificial. A IA pode ajudar a identificar padrões de abuso, automatizar respostas e fortalecer mecanismos de proteção. Mas também pode ser usada de forma prejudicial, facilitando a criação em massa de ataques, golpes mais convincentes e operações maliciosas em velocidade muito maior. Por isso, o debate precisa ser técnico, político e responsável.

Mitigar abusos na Internet não é simples. A rede é global, distribuída e atravessa diferentes jurisdições, culturas, legislações e regimes políticos. Alguns países impõem regras duras, muitas vezes sob o argumento de segurança, mas que podem restringir liberdades fundamentais. Outros têm modelos mais abertos, baseados em cooperação e transparência. O desafio é combater abusos sem comprometer a liberdade, a inovação e a natureza global da Internet.

Outro tema relevante é a nova rodada de domínios genéricos de primeiro nível, os chamados gTLDs. São extensões que aparecem depois do ponto em um endereço da Internet, como ocorre com .com, .org ou .net, mas que agora podem abrir novas possibilidades para marcas, cidades, comunidades, setores econômicos e instituições. Essa nova rodada representa uma oportunidade estratégica para organizações que desejam construir identidade digital própria, aumentar confiança, reforçar segurança e criar novos espaços de presença na rede. Ao mesmo tempo, exige atenção a custos, governança, proteção de marcas, infraestrutura técnica e impactos concorrenciais.

O grande lema que deve orientar esse esforço é simples e poderoso: uma Internet, um mundo para todos. A Internet precisa continuar sendo um espaço de conexão, oportunidade e desenvolvimento. Para isso, é necessário engajamento político, participação qualificada e defesa permanente do modelo multissetorial.

Participar da ICANN86 é, portanto, mais do que acompanhar uma reunião técnica. É contribuir para que a Internet continue aberta, segura, interoperável e acessível. É defender que decisões sobre o futuro da rede sejam tomadas com equilíbrio, ouvindo todos os setores envolvidos. É garantir que as preocupações brasileiras sejam levadas a um ambiente global onde se discutem as políticas que moldam o presente e o futuro da Internet.

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

Abuso de DNS: por que o tema deve estar no radar das empresas brasileiras
ICANN 86 8 de junho de 2026
*Por Nivaldo Cleto**

O segundo dia de acompanhamento da ICANN86, em Sevilha, reforçou um tema que deveria estar no radar de qualquer empresário que depende da Internet para vender, se comunicar, receber pagamentos, proteger sua marca ou atender clientes: o combate ao abuso de DNS.[1]

Para quem não acompanha esse debate de perto, o DNS é uma espécie de "agenda de endereços" da Internet. É ele que permite que um nome de domínio, como o endereço de um site, seja encontrado pelos computadores. Quando criminosos usam domínios para aplicar golpes, enviar mensagens falsas, instalar programas maliciosos ou enganar consumidores, a confiança no ambiente digital é afetada. E essa confiança é essencial para pequenos, médios e grandes negócios.

Nas discussões da ICANN86, o foco principal foi o avanço de um processo de desenvolvimento de política dentro da GNSO,[2] chamado DNS Abuse Mitigation PDP 1.[3] O tema central desse trabalho são as chamadas verificações de domínios associados. Em termos simples, a pergunta é: quando um domínio é identificado como parte de uma campanha abusiva, o registrador deveria verificar se existem outros domínios relacionados ao mesmo agente malicioso?

Esse ponto é importante porque golpes digitais raramente acontecem de forma isolada. Muitas vezes, criminosos registram vários domínios parecidos, usam contas diferentes, mudam de fornecedor ou distribuem a operação para dificultar a identificação. A proposta em debate busca criar regras mais claras para que os registradores possam investigar padrões e agir com mais eficiência.

Mas a discussão mostrou que não basta “sair derrubando domínios”. É preciso equilíbrio. Um dos temas mais debatidos foi como medir se uma política contra abuso realmente funciona. Não adianta contar apenas quantos domínios foram suspensos. Também é necessário avaliar se houve falsos positivos, se algum titular legítimo foi prejudicado, se a investigação foi proporcional, se a ação foi documentada e se a campanha criminosa foi de fato interrompida ou apenas mudou de lugar.

Esse cuidado é fundamental para o empresário honesto. Imagine uma pequena empresa que teve seu site invadido, sem saber, por uma falha técnica. Ela não é criminosa, mas seu domínio pode ter sido usado por terceiros para hospedar conteúdo malicioso. Nesses casos, a política precisa permitir resposta rápida contra o abuso, mas também proteger quem foi vítima de invasão.

Outro ponto relevante foi a preocupação com a evolução dos ataques. A inteligência artificial pode ajudar a identificar padrões suspeitos e acelerar respostas. Mas também pode ser usada por criminosos para automatizar fraudes, criar campanhas em grande escala e registrar domínios de forma mais sofisticada. Por isso, a comunidade discutiu a necessidade de uma política que seja clara, aplicável e, ao mesmo tempo, flexível para acompanhar novas formas de abuso.

Também foi debatida a diferença entre política, guia de implementação e boas práticas. A tendência é que a política traga princípios mais duradouros, como razoabilidade, proporcionalidade, documentação e uso de informações disponíveis. Já os detalhes técnicos, que mudam com mais rapidez, podem ficar em orientações de implementação ou boas práticas revisáveis.

Na reunião inaugural do GAC,[4] o abuso de DNS também apareceu como uma preocupação relevante para governos. Isso mostra que o tema deixou de ser apenas técnico. Ele envolve segurança pública, proteção de consumidores, privacidade, acesso a dados de registro e cooperação internacional.

Além do abuso de DNS, outras discussões importantes marcaram o dia. A nova rodada de domínios genéricos de primeiro nível, os gTLDs,[5] continua chamando atenção. Ela pode abrir oportunidades para marcas, cidades, comunidades e setores econômicos criarem novas identidades digitais. Ao mesmo tempo, exige atenção a custos, proteção de marcas e governança.

Também foram discutidos temas como Universal Acceptance,[6] que busca garantir que nomes de domínio e e-mails em diferentes idiomas funcionem corretamente; melhoria dos processos internos da ICANN;[7] resiliência do DNS; e avanços técnicos ligados à segurança da infraestrutura da Internet. Para pequenos e médios empresários, a mensagem principal é simples: a governança da Internet não é um assunto distante. Ela influencia a segurança do comércio eletrônico, a proteção da marca, a confiança dos consumidores, a entrega de e-mails, a estabilidade dos sites e a capacidade de combater fraudes digitais.
A participação nesses debates é importante porque a Internet precisa continuar sendo global, interoperável, segura e aberta. Ao acompanhar a ICANN86, minha missão é observar essas tendências, entender seus impactos e levar ao Comitê Gestor da Internet no Brasil preocupações e oportunidades que ajudem o país a participar de forma qualificada da construção das políticas globais da rede.

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

Notas de rodapé

[1] DNS — Domain Name System: sistema que traduz nomes de domínio, como endereços de sites, em endereços técnicos usados pelos computadores para localizar serviços na Internet.

[2] GNSO — Generic Names Supporting Organization: estrutura da ICANN responsável pelo desenvolvimento de políticas para nomes de domínio genéricos, como .com, .org, .net e novos gTLDs.

[3] PDP — Policy Development Process: processo formal de desenvolvimento de políticas dentro da ICANN.

[4] GAC — Governmental Advisory Committee: comitê da ICANN que reúne governos e organizações intergovernamentais para tratar de temas com impacto em políticas públicas.

[5] gTLD — Generic Top-Level Domain: domínio genérico de primeiro nível, isto é, a parte final de um endereço na Internet, como .com, .org, .net ou novas extensões que podem surgir em rodadas da ICANN.

[6] Universal Acceptance: princípio segundo o qual todos os nomes de domínio e endereços de e-mail válidos devem funcionar corretamente em sistemas, aplicativos e plataformas, inclusive aqueles em diferentes idiomas e alfabetos.

[7] ICANN — Internet Corporation for Assigned Names and Numbers: organização global responsável por coordenar elementos essenciais do sistema de identificadores únicos da Internet, como nomes de domínio e números IP.

A visão da Business Constituency sobre segurança, confiança e negócios na Internet
ICANN 86 9 de junho de 2026
*Por Nivaldo Cleto**

Nesta terça-feira, 9 de junho, participei da reunião aberta da Business Constituency, a BC[1], durante a ICANN86[2], em Sevilha. A BC é o grupo da ICANN (foto acima) que representa os usuários comerciais da Internet, ou seja, empresas e organizações que dependem da rede para vender, se comunicar, proteger suas marcas, atender clientes e operar com segurança no ambiente digital.

A reunião começou em clima de grande emoção, com uma homenagem à memória de Arinola Akinyemi, importante integrante da Business Constituency, falecida recentemente. Sua partida causou profundo pesar entre os membros da BC, que destacaram sua gentileza, bom humor, espírito colaborativo e dedicação à comunidade da Internet.

Arinola teve atuação relevante na própria BC, inclusive como representante no NomCom[3], o Comitê de Nomeações da ICANN. Também foi lembrada por sua trajetória na indústria de tecnologia da informação na Nigéria e na África, por sua contribuição à AfICTA[4] e por seu compromisso com inclusão, participação e fortalecimento da presença africana nos espaços de governança da Internet. Foi um momento que mostrou que a governança global da rede é feita não apenas de políticas e tecnologia, mas também de pessoas que dedicam tempo, energia e vida à construção de uma Internet melhor.

Na sequência, um dos principais temas técnicos do dia foi a apresentação da Netcraft sobre bulletproof hosting. Em linguagem simples, trata-se de provedores de hospedagem que oferecem abrigo, direta ou indiretamente, para atividades maliciosas na Internet, como phishing, lojas falsas, fraudes digitais e distribuição de malware. São estruturas que muitas vezes ignoram denúncias de abuso, mudam rapidamente de infraestrutura e dificultam a retirada de conteúdos criminosos do ar.

Para pequenos e médios empresários, esse tema é muito relevante. Muitas fraudes usam nomes de domínio parecidos com marcas legítimas, páginas falsas de venda, boletos falsos, campanhas de phishing e sites que simulam empresas reais. O prejuízo não é apenas financeiro. Há também perda de reputação, desconfiança dos clientes e aumento do custo de proteção digital.

A apresentação mostrou que os criminosos não atuam de forma isolada. Eles usam padrões: registram vários domínios, mudam de servidor, utilizam diferentes fornecedores, reaproveitam infraestrutura e exploram canais de denúncia ineficientes. Por isso, apenas derrubar um site falso pode não ser suficiente. É preciso identificar a campanha inteira.

Esse ponto se conecta diretamente ao debate sobre Associated Domain Checks[5]. A ideia é que, quando um domínio é identificado como abusivo, seja possível investigar se existem outros domínios ligados ao mesmo agente, à mesma infraestrutura ou ao mesmo padrão de ataque. Esse tipo de inteligência pode ajudar a interromper campanhas fraudulentas antes que atinjam mais consumidores e empresas.

Também foi discutido o papel dos registrars[6]. Alguns participantes destacaram que o problema não está apenas em quem comete abuso, mas também em quem não procura abuso de forma ativa. A preocupação é que a fiscalização da ICANN não dependa apenas de denúncias pontuais, mas conte com dados, registros, padrões mínimos e capacidade de auditoria.

Dentro da BC, houve debate sobre o processo de desenvolvimento de política para mitigação de abuso de DNS[7]. O grupo acompanha de perto esse trabalho e defende que as futuras regras sejam claras, proporcionais e úteis para a segurança do ecossistema. Ao mesmo tempo, há uma preocupação prática: regras excessivamente vagas dificultam a fiscalização; regras excessivamente rígidas podem se tornar obsoletas rapidamente.

Outro ponto importante foi a discussão sobre relatórios, registros e métricas. Para saber se uma política funciona, não basta dizer que um domínio foi suspenso. É necessário verificar se a investigação foi feita, se houve documentação adequada, se os dados podem ser auditados, se houve falsos positivos e se a campanha criminosa foi de fato interrompida.

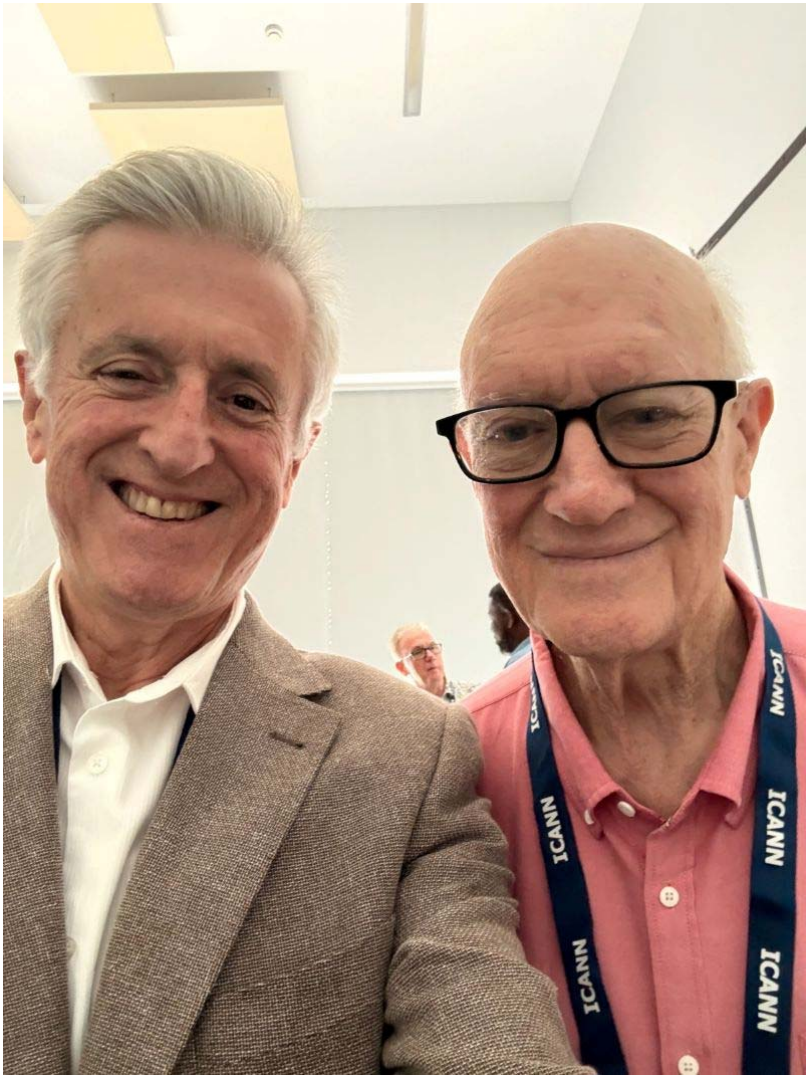
A reunião também tratou de temas internos da BC, como finanças, governança, adesão de novos membros e atividades de divulgação. Foi informado que a BC está em boa condição financeira e mantém reservas para cobrir despesas futuras. Também houve incentivo para que os membros compartilhem experiências e expliquem por que vale a pena participar desse grupo dentro da ICANN.

Na parte de política, foram apresentadas atualizações sobre o trabalho do Conselho da GNSO[8], que é a estrutura responsável por políticas de domínios genéricos, como .com, .org, .net e os novos domínios de primeiro nível. Entre os temas discutidos estiveram processos internos da ICANN, revisão

de decisões, novas rodadas de domínios e a forma como determinados assuntos devem ser encaminhados dentro da comunidade.

Outro tema relevante foi o acesso a dados de registro de domínios. Esse debate é essencial para empresas, titulares de marcas, autoridades e especialistas em segurança que precisam identificar responsáveis por fraudes, abusos ou violações. Ao mesmo tempo, é necessário equilibrar esse acesso com regras de privacidade e proteção de dados.

A reunião também abordou a colaboração entre grupos comerciais e não comerciais da ICANN, incluindo o diálogo no CSG[9]. Mesmo quando há visões diferentes, o diálogo é importante para construir políticas equilibradas, que protejam usuários, empresas, direitos fundamentais, segurança e estabilidade da Internet.



Com Steve Crocker, o pai da internet

Nesse contexto, faço um convite especial às grandes marcas brasileiras: acompanhem mais de perto os debates da Business Constituency. Empresas que investem em reputação, comércio eletrônico, canais digitais, relacionamento com consumidores e proteção de suas marcas precisam estar presentes nos

espaços onde as políticas globais sobre nomes de domínio são discutidas. A filiação à BC permite participar diretamente dos debates sobre abuso de DNS, acesso a dados de registro, proteção contra fraudes, uso indevido de marcas, lojas falsas, phishing e responsabilidade dos agentes que operam a infraestrutura de domínios na Internet.

Para o Brasil, ampliar a presença empresarial na BC é também uma forma de fortalecer nossa voz na governança global da rede. Grandes marcas brasileiras têm muito a contribuir, porque enfrentam diariamente desafios reais de proteção de identidade digital, reputação online, fraudes contra consumidores e uso indevido de seus nomes na Internet.

Para o empresário brasileiro, a principal mensagem da reunião da BC é clara: segurança na Internet não depende apenas de antivírus, firewall ou boas práticas internas. Ela também depende de políticas globais sobre nomes de domínio, dados de registro, responsabilidades de registradores, resposta a abusos e cooperação internacional.

A Internet é hoje infraestrutura essencial para qualquer empresa. Quando há abuso de DNS, phishing, lojas falsas ou uso malicioso de domínios, todos perdem: consumidores, empresas, governos e a própria confiança no ambiente digital.

Minha missão ao acompanhar a ICANN86 é observar esses debates, entender seus impactos práticos e levar ao Comitê Gestor da Internet no Brasil preocupações e oportunidades que ajudem o país a participar de forma qualificada da construção das políticas globais da Internet.

Fica, portanto, o convite: que mais empresas brasileiras, especialmente nossas grandes marcas, conheçam a Business Constituency e participem desse debate. Proteger a identidade digital das marcas brasileiras também passa por estar presente nos fóruns globais onde as regras da Internet são construídas.

(*) Nivaldo Cleto é empresário de contabilidade e de certificação digital, conselheiro do Comitê Gestor da Internet no Brasil CGI.br e membro da ICANN Business Constituency – BC

Notas explicativas dos acrônimos e termos técnicos

1. BC – Business Constituency: grupo da ICANN que representa usuários comerciais da Internet, incluindo empresas, associações empresariais e organizações que dependem da rede para suas atividades.
2. ICANN – Internet Corporation for Assigned Names and Numbers: organização global responsável por coordenar elementos essenciais do sistema de nomes de domínio e identificadores únicos da Internet.
3. NomCom – Nominating Committee: comitê da ICANN responsável por selecionar pessoas para determinadas posições de liderança dentro da organização.

4. AfICTA – Africa ICT Alliance: aliança africana de entidades e lideranças ligadas ao setor de tecnologia da informação e comunicação.

5. Associated Domain Checks – Verificações de domínios associados a uma campanha, infraestrutura ou agente malicioso já identificado.

6. Registrar – Empresa credenciada para registrar nomes de domínio em nome de clientes.

7. DNS – Domain Name System: sistema que traduz nomes de domínio em endereços técnicos usados pelos computadores para localizar sites e serviços na Internet.

8. GNSO – Generic Names Supporting Organization: estrutura da ICANN responsável por desenvolver políticas para domínios genéricos, como .com, .org, .net e novos gTLDs.

9. CSG – Commercial Stakeholders Group: grupo que reúne comunidades comerciais dentro da GNSO.

ICANN86: quando governos, empresas e a comunidade técnica discutem os limites da proteção na Internet
ICANN 86 10 de junho de 2026
*Por Nivaldo Cleto**

Depois de acompanhar a reunião da Business Constituency no dia anterior, o foco do diário de hoje muda de eixo. Desta vez, o debate central veio da reunião do GAC[1] com o Conselho da ICANN[2], uma sessão que mostrou como a governança da Internet envolve muito mais do que tecnologia. Ela também passa por políticas públicas, segurança, dados de registro, proteção contra abusos, financiamento de novos projetos e riscos de fragmentação da rede.

A reunião foi estruturada em torno de quatro prioridades: o Programa de Apoio ao Candidato, os dados de registro de domínios, a governança dos registros regionais de Internet e os riscos sistêmicos associados ao uso de bloqueios no DNS[3].

O primeiro tema foi o Programa de Apoio ao Candidato, conhecido pela sigla ASP[4]. Esse programa busca facilitar a participação de organizações com menor capacidade financeira na próxima rodada de novos domínios de primeiro nível. O GAC questionou o Conselho da ICANN sobre a possibilidade de ampliar o financiamento de terceiros, especialmente para candidatos de países menos desenvolvidos.

A resposta do Conselho foi clara: para a rodada atual, a estrutura de financiamento não será reaberta. O apoio previsto será aplicado conforme as regras já definidas, com descontos que podem chegar a 85% ou 75%, dependendo do número de candidatos qualificados. Também foi explicado que a ICANN pode estimular contatos com organizações e agências interessadas, mas não pode atuar diretamente como intermediária entre financiadores e candidatos.

Para o Brasil, esse ponto merece atenção. A próxima rodada de novos domínios pode abrir oportunidades para entidades, comunidades, setores econômicos, cidades, marcas e projetos de interesse público. Mas a mensagem prática é que não basta ter uma boa ideia. Será necessário planejamento financeiro, capacidade técnica, governança e visão estratégica.

Delegação do CGI.br na 86ICANN: Nivaldo Cleto (Setor empresarial), José Roberto Fernandes (Setor governamental), Marcelo Salomão Martinez (Representante do Itamaraty), Renata Mielli (Setor governamental), Laurianne-Marie Schippers (Assessora Técnica do CGI.br), Jean Carlos Ferreira dos Santos (Coordenador da Assessoria Técnica ao CGI.br) e Flávio Rech Wagner (Consultor)

Outro tema relevante foi o acesso a dados de registro de domínios. Esse debate é sensível porque envolve, ao mesmo tempo, combate a fraudes, proteção de dados pessoais, privacidade, segurança pública e responsabilidade dos agentes que operam nomes de domínio.

O GAC cobrou avanços sobre mecanismos de autenticação para solicitações feitas por autoridades de aplicação da lei. O Conselho explicou que já existe a previsão de resposta em até 24 horas para solicitações urgentes autenticadas, mas que o mecanismo de autenticação ainda depende de amadurecimento e está ligado ao trabalho mais amplo de revisão das recomendações do SSAD[5], com previsão de relatório final em 2027.

Esse tema tem impacto direto para empresas e consumidores. Quando há phishing, golpe financeiro, loja falsa, uso indevido de marca ou fraude digital, muitas vezes é necessário identificar rapidamente quem está por trás de um domínio ou de uma infraestrutura abusiva. Mas esse acesso não pode ser desorganizado ou arbitrário. Ele precisa respeitar critérios, autenticação, finalidade legítima e segurança jurídica.

A reunião também tratou da governança dos registros regionais de Internet, responsáveis pela distribuição de recursos numéricos essenciais, como endereços IP[6]. Embora esse tema seja menos visível para o usuário comum, ele é fundamental para a estabilidade da rede. Sem governança confiável desses recursos, a Internet perde previsibilidade, coordenação e segurança operacional.

O Conselho informou que haverá novas etapas de revisão, circulação entre os registros regionais e consulta pública. O ponto importante é que governos e demais partes interessadas terão oportunidade de contribuir com observações de política pública antes da conclusão do processo.

O tema mais forte da reunião, porém, foi o risco de bloqueios excessivos no DNS. O GAC perguntou sobre os impactos de bloqueios privados, bloqueios geográficos e medidas desproporcionais que podem afetar a estabilidade global da Internet.

A resposta do Conselho foi equilibrada. Bloqueios podem fazer sentido em ambientes limitados, como uma rede doméstica, uma escola ou uma empresa. Mas quando aplicados em larga escala, por provedores de acesso ou por mecanismos amplos de filtragem, podem gerar danos colaterais, atingir usuários legítimos e contribuir para a fragmentação da Internet.

Esse ponto é essencial para o Brasil. Todos queremos combater fraudes, pirataria, malware, phishing e outros abusos. Mas soluções simplistas podem criar novos problemas. Bloquear demais, bloquear errado ou bloquear sem mecanismos de revisão pode prejudicar empresas legítimas, usuários comuns, liberdade de acesso e a própria interoperabilidade global da rede.

A discussão mostrou que segurança e abertura precisam caminhar juntas. A Internet é valiosa justamente porque funciona como uma rede global, interoperável e acessível. Se cada país, provedor ou agente privado começar a aplicar bloqueios de forma isolada, sem coordenação e sem transparência, o risco é criar várias “Internets” separadas, com regras incompatíveis entre si.

Outro ponto importante veio da cobrança por mais transparência no combate ao abuso de DNS. Representantes governamentais defenderam que é preciso ter dados melhores, relatórios mais claros e evidências mais consistentes para avaliar se as políticas realmente funcionam.

Esse é um dilema complexo. De um lado, sem dados não há como medir o problema, fiscalizar resultados ou melhorar políticas. De outro, divulgar informações sensíveis demais pode ajudar agentes maliciosos a entender os mecanismos de defesa e adaptar suas estratégias. A solução, portanto, deve equilibrar transparência, segurança operacional e responsabilidade.

A reunião também mencionou o apoio da ICANN ao Fórum de Governança da Internet, o IGF[7], com uma doação de um milhão de dólares. Esse gesto reforça a importância do modelo multissetorial, no qual governos, setor privado, comunidade técnica, sociedade civil e academia participam da construção das políticas da Internet.

Na parte final, o GAC iniciou a redação de seu comunicado, tratando de temas como abuso de DNS, revisão dos processos internos da ICANN e preocupação com duplicação de esforços. Também foi registrada a confirmação de Ian Sheldon como novo presidente do GAC para mandato futuro.

O que fica desse dia é uma mensagem clara: a governança da Internet está entrando em uma fase em que decisões técnicas têm consequências políticas, econômicas e sociais cada vez mais visíveis. Dados de registro, bloqueio de domínios, abuso de DNS, novos domínios de primeiro nível e governança de recursos críticos não são temas distantes. Eles afetam governos, empresas, consumidores e cidadãos.

Para o empresário brasileiro, a lição é direta. A segurança digital da empresa não depende apenas de ferramentas internas. Ela também depende de políticas globais sobre nomes de domínio, acesso a dados, combate a abusos, proteção contra fraudes e preservação de uma Internet única e interoperável.

Para o Brasil, o desafio é participar desses debates de forma qualificada. É preciso defender segurança, mas sem abrir mão da abertura da rede. É preciso combater abusos, mas sem criar mecanismos desproporcionais. É preciso proteger marcas e consumidores, mas também preservar direitos, inovação e interoperabilidade.

Minha missão ao acompanhar a ICANN86 é justamente observar esses debates, compreender seus impactos práticos e levar ao Comitê Gestor da Internet no Brasil preocupações e oportunidades para que o país esteja presente na construção das políticas globais da Internet.

**Nivaldo Cleto*

Representante do Setor Empresarial Usuários de Internet do Comitê Gestor da Internet no Brasil

Membro da ICANN Business Constituency

Notas explicativas

1. GAC — Governmental Advisory Committee: comitê consultivo da ICANN formado por governos e organizações intergovernamentais, responsável por apresentar preocupações de política pública ao Conselho da ICANN.

2. ICANN — Internet Corporation for Assigned Names and Numbers: organização global responsável pela coordenação de elementos essenciais do sistema de nomes de domínio e identificadores únicos da Internet.

3. DNS — Domain Name System: sistema que permite localizar nomes de domínio na Internet, transformando endereços como "exemplo.com" em informações técnicas compreendidas pelos computadores.

4. ASP — Applicant Support Program: Programa de Apoio ao Candidato da ICANN, criado para reduzir barreiras financeiras e operacionais para determinados candidatos na próxima rodada de novos domínios de primeiro nível.

5. SSAD — System for Standardized Access/Disclosure: sistema discutido na ICANN para estruturar pedidos padronizados de acesso e divulgação de dados de registro não públicos.

6. IP — Internet Protocol: protocolo que permite a identificação e comunicação entre dispositivos conectados à Internet. Os endereços IP são recursos numéricos essenciais para o funcionamento da rede.

7. IGF — Internet Governance Forum: Fórum de Governança da Internet, espaço global de diálogo multissetorial promovido no âmbito das Nações Unidas.

O que fica de Sevilha e o caminho até a ICANN87 em Bali
ICANN 86 14 de junho de 2026
*Por Nivaldo Cleto**

A ICANN86 chegou ao fim em Sevilha, depois de quatro dias intensos de debates sobre políticas globais da Internet. Foi uma reunião marcada por temas técnicos, mas com consequências muito concretas para empresas, governos, consumidores e usuários.

Ao longo da semana, acompanhei discussões sobre abuso de DNS[1], proteção de marcas, dados de registro, novos domínios de primeiro nível, participação empresarial, atuação dos governos, estabilidade da infraestrutura crítica da Internet e os desafios trazidos pela inteligência artificial.

O principal aprendizado é que a governança da Internet não é um assunto distante. Ela influencia diretamente a segurança do comércio eletrônico, a confiança dos usuários, a proteção das marcas, a investigação de fraudes digitais, a entrega de e-mails, a estabilidade dos nomes de domínio e a forma como empresas e cidadãos se relacionam no ambiente online.

Um dos grandes fios condutores da ICANN86 foi o combate ao abuso de DNS. O tema apareceu em diversas sessões e avançou especialmente no trabalho da GNSO[2] sobre verificações de domínios associados. A ideia é simples de explicar, mas complexa de implementar: quando um domínio é identificado como parte de uma campanha abusiva, é preciso verificar se existem outros domínios ligados ao mesmo agente, à mesma conta, à mesma infraestrutura ou ao mesmo padrão de ataque.

Esse debate é importante porque os criminosos digitais não atuam mais de forma isolada. Muitas campanhas de phishing, malware, lojas falsas e fraudes usam vários domínios ao mesmo tempo, registrados em sequência, espalhados por diferentes fornecedores e, muitas vezes, apoiados por automação.

Mas a discussão em Sevilha mostrou que combater abuso exige equilíbrio. Não basta retirar domínios do ar. É preciso criar regras proporcionais, documentadas, fiscalizáveis e capazes de proteger usuários e empresas legítimas contra falsos positivos.

A última sessão do grupo de trabalho sobre abuso de DNS deixou isso muito claro. O debate não foi apenas sobre como agir contra domínios maliciosos, mas também sobre quais dados os registradores devem usar, que tipo de investigação é razoável, como evitar auditorias excessivas sobre contas de clientes e como impedir que pessoas inocentes sejam prejudicadas quando seus dados forem usados indevidamente por criminosos.

A palavra-chave foi proporcionalidade. A investigação precisa ser séria, mas não ilimitada. Precisa ser eficaz, mas não arbitrária. Precisa proteger consumidores, mas sem criar danos colaterais contra empresas, usuários legítimos ou a abertura da rede.

Outro ponto forte da semana foi a atuação do GAC[3], o comitê de governos da ICANN. Na reunião com o Conselho da ICANN, os governos trouxeram preocupações de política pública sobre dados de registro, acesso por autoridades, governança dos registros regionais de Internet, apoio a candidatos de países com menos recursos e riscos sistêmicos de bloqueios no DNS.

Esse último tema merece destaque. Bloqueios podem ser úteis em alguns contextos restritos, como redes domésticas ou ambientes corporativos. Mas, quando aplicados em larga escala, por provedores ou por mecanismos amplos de filtragem, podem gerar danos colaterais, afetar usuários legítimos e contribuir para a fragmentação da Internet.

Essa é uma discussão essencial para o Brasil. Todos queremos combater fraudes, pirataria, phishing, malware e abusos digitais. Mas soluções simplistas podem prejudicar a própria Internet que queremos proteger. A rede precisa continuar aberta, global, interoperável e confiável.

Também foi discutido o acesso a dados de registro de domínios. Esse tema é sensível porque envolve, ao mesmo tempo, combate a crimes digitais, proteção de marcas, segurança pública, privacidade e proteção de dados pessoais. Para empresas e consumidores, o ponto prático é claro: quando ocorre uma fraude digital, muitas vezes é necessário identificar rapidamente quem está por trás de um domínio abusivo. Mas esse acesso precisa ter regras, autenticação, finalidade legítima e segurança jurídica.

Nesse ponto, o Brasil tem uma experiência importante a apresentar. No nosso país, o domínio .br é coordenado pelo NIC.br[4], por meio do Registro.br. Uma característica relevante do modelo brasileiro é que, ao registrar um domínio sob o .br, o titular é identificado por CPF ou CNPJ. Essa identificação não elimina totalmente o risco de abuso, mas aumenta a rastreabilidade, dificulta o anonimato abusivo e contribui para que os domínios brasileiros estejam entre os ambientes com menor incidência relativa de abuso de DNS.

Esse exemplo brasileiro é especialmente relevante porque muitos dos debates da ICANN86 trataram justamente da dificuldade de identificar responsáveis por domínios usados em phishing, malware, lojas falsas e fraudes digitais. A experiência do .br mostra que políticas de registro bem estruturadas, com identificação do titular e governança técnica confiável, podem ajudar a proteger usuários, empresas e marcas sem romper a abertura da Internet.

A ICANN86 também reforçou a importância da participação de diferentes setores. Governos, empresas, comunidade técnica, sociedade civil, academia, registradores, registros, especialistas em segurança e usuários precisam estar presentes. A construção de políticas globais da Internet não acontece por decreto. Ela exige diálogo, negociação, evidências, participação contínua e disposição para construir consenso.

Para as empresas brasileiras, especialmente aquelas que dependem da Internet para vender, atender clientes, proteger marcas e manter reputação, a mensagem é direta: participar desses debates é cada vez mais importante. As políticas discutidas na ICANN podem afetar a forma como domínios são registrados, como abusos são tratados, como dados podem ser acessados e como fraudes digitais são combatidas.

Para o Comitê Gestor da Internet no Brasil, a ICANN86 reforça a necessidade de acompanhamento permanente. O Brasil precisa levar aos fóruns internacionais sua experiência, suas preocupações e suas propostas. Temos um ecossistema digital relevante, empresas fortes, comunidade técnica qualificada e uma trajetória reconhecida no modelo multissetorial.

Sevilha também mostrou que muitos temas ainda não terminaram. O trabalho sobre abuso de DNS continuará depois da ICANN86, com novas reuniões do grupo de trabalho e preparação de relatório inicial para consulta pública. As discussões sobre dados de registro, acesso legítimo, transparência, métricas, inteligência artificial, novos domínios e riscos de fragmentação continuarão evoluindo.

A próxima etapa será a ICANN87, em Bali, na Indonésia, prevista para outubro de 2026. Será a reunião anual geral da ICANN e deverá servir como novo ponto de encontro para avaliar os avanços dos trabalhos iniciados ou aprofundados em Sevilha.

Saio da ICANN86 com uma convicção ainda mais forte: a Internet é uma infraestrutura global essencial, mas sua estabilidade e confiança dependem de participação. Não basta usar a Internet. É preciso ajudar a construir as regras que mantêm a rede segura, aberta e interoperável.

Para o Brasil, o desafio é seguir presente, qualificado e atento. As decisões tomadas nesses fóruns globais afetam nossas empresas, nossos usuários, nossas marcas, nossas políticas públicas e nossa soberania digital.

A ICANN86 termina em Sevilha, mas os temas debatidos aqui continuam vivos. O combate aos abusos digitais, a proteção de marcas, a segurança dos usuários, a preservação da privacidade, a valorização de modelos responsáveis como o .br e a defesa de uma Internet única e global seguirão na agenda até Bali — e muito além.

**Nivaldo Cleto, representante do Setor Empresarial Usuários de Internet do Comitê Gestor da Internet no Brasil*

Membro da ICANN Business Constituency

Imagens: icannphotos

Notas explicativas

1. DNS — Domain Name System: sistema que permite localizar nomes de domínio na Internet, transformando endereços como "exemplo.com" em informações técnicas compreendidas pelos computadores.

2. GNSO — Generic Names Supporting Organization: estrutura da ICANN responsável pelo desenvolvimento de políticas para domínios genéricos, como .com, .org, .net e novas extensões de domínio.

3. GAC — Governmental Advisory Committee: comitê consultivo formado por governos e organizações intergovernamentais, responsável por apresentar preocupações de política pública ao Conselho da ICANN.

4. NIC.br — Núcleo de Informação e Coordenação do Ponto BR: entidade criada para implementar as decisões e projetos do Comitê Gestor da Internet no Brasil. Atua como braço executivo do CGI.br e, entre suas atribuições, realiza o registro e manutenção dos domínios .br por meio do Registro.br, distribui números de Sistema Autônomo e endereços IPv4 e IPv6 no país, responde a incidentes de segurança por meio do CERT.br, apoia a infraestrutura da Internet brasileira por meio de iniciativas como o IX.br, produz indicadores sobre o uso da Internet pelo Cetic.br e promove estudos, normas e padrões técnicos para a segurança e o desenvolvimento da rede no Brasil.