Relatório de participação

Evento: ICANN 64
Datas: 10 a 15 de Março de 2019
Local: Kobe / Japão

Conselheiro: Thiago Tavares Nunes de Oliveira
Representante do Terceiro Setor no CGI.br

Nota introdutória: o presente relatório pretende destacar os temas de maior interesse para o CGI.br. Procura-se evitar redundâncias e sobreposições com o relatório da delegação, consolidado pela assessoria do CGI.br, como também pelos demais conselheiros que participaram do mesmo evento e disponibilizaram seus respectivos relatórios.

Sumário:

A reunião de número 64 da ICANN discutiu uma ampla gama de tópicos em suas diferentes *constituencies.* O relato pormenorizado consta do relatório da delegação[1]. Desse modo, neste relatório individual, pretendo 3 tópicos relevantes que não foram detalhados em outros relatórios, a saber: a) planejamento estratégico da ICANN para o quinquênio 2021-2025; b) atualizações sobre o Domain Abuse Activity Reporting (DAAR); c) nomes geográficos

a) Planejamento Estratégico da ICANN para o quinquênio 2021-2025

O Plano Estratégico da ICANN para os Anos Fiscais de 2021 a 2025 estabelece cinco objetivos estratégicos e metas estratégicas relacionadas. Os objetivos estratégicos estão diretamente relacionados às principais tendências identificadas pela comunidade da ICANN, pela diretoria da ICANN e pela organização da ICANN. Eles representam áreas de desafio e oportunidade para a ICANN moldar seu futuro com sucesso. São eles:

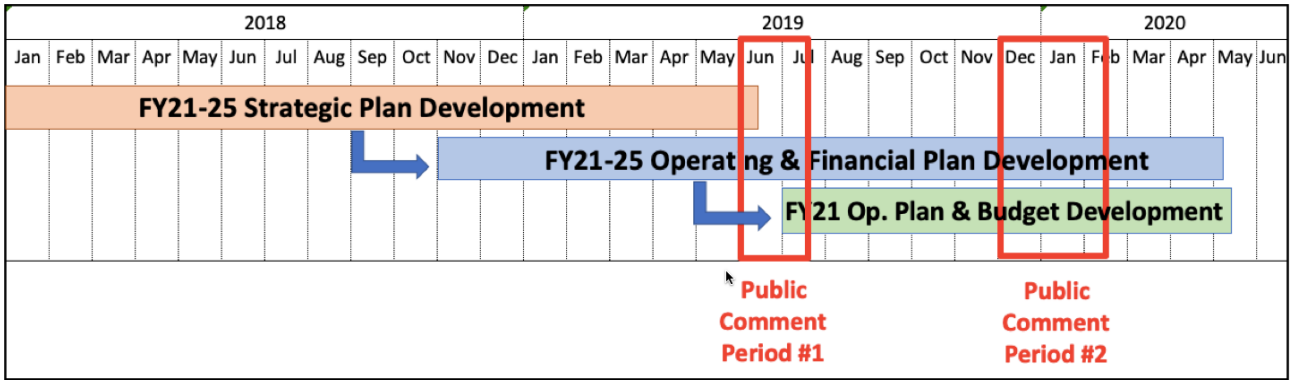
- Strengthen the security of the Domain Name System and the DNS Root Server System.

1 Disponível em: https://observatoriodainternet.br/post/relato-da-icann-64-em-kobe

- Improve the effectiveness of ICANN's multistakeholder model of governance.
- Evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.
- Address geopolitical issues impacting ICANN's mission to ensure a single and globally interoperable Internet.
- Ensure ICANN's long-term financial sustainability.

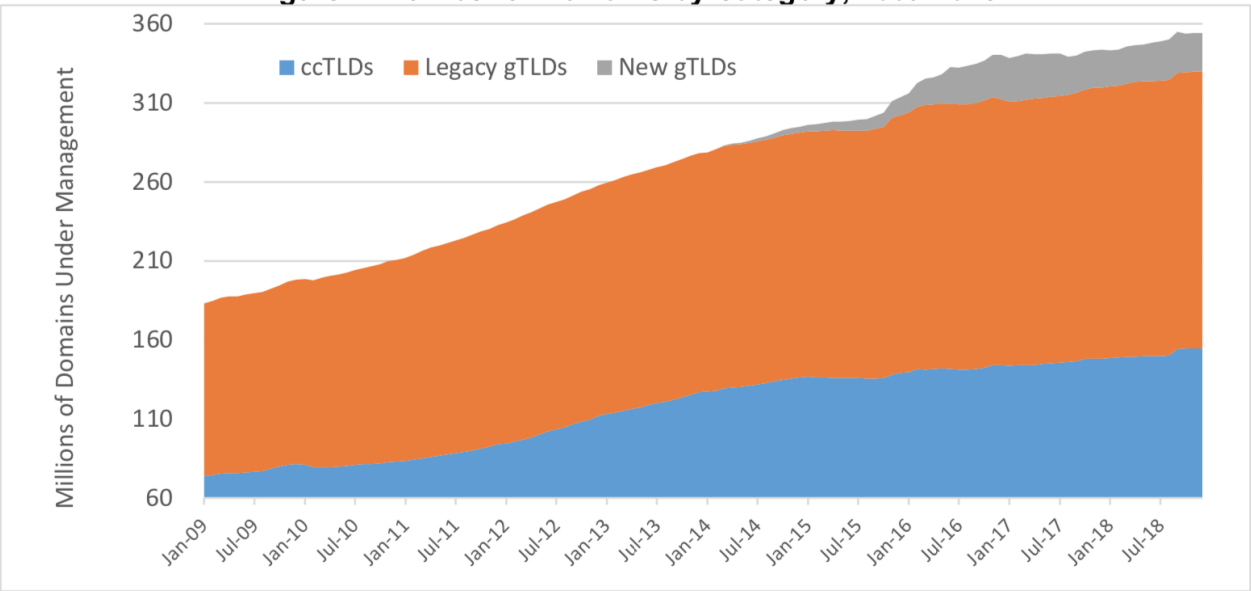
O Plano Estratégico Preliminar será complementado por um Plano Operacional e Financeiro de cinco anos que descreve as Iniciativas Operacionais e Atividades Operacionais da ICANN. Iniciativas operacionais são iniciativas importantes que a ICANN fará para atingir os objetivos e metas estabelecidos no Plano Estratégico. Atividades operacionais são as atividades do dia a dia que apóiam a missão da organização.

Com base no feedback desse período de comentários públicos, a ICANN desenvolverá um esboço abrangente do plano que será publicado para comentários públicos em dezembro de 2019. O Plano operacional e o orçamento do ano fiscal de 2021 também será publicado para comentários do público em dezembro de 2019. A publicação de ambos os planos ao mesmo tempo permitirá que a comunidade da ICANN analise o plano do primeiro ano no contexto do plano quinquenal.



A nova estratégia quinquenal da ICANN privilegiará a ampliação do espaço de nomes geográficos e de marcas. A figura a seguir ilustra a linha de tendência para registros de nomes de domínio após a introdução de novos gTLDs no mercado. Esse segmento de mercado expandiu-se rapidamente após sua implantação inicial e, posteriormente, sofreu volatilidade em 2017 antes de se estabilizar em 2018. Durante 2018, todos os três setores da indústria de nomes de domínio, quais sejam: Legacy gTLDs, os domínios de primeiro nível com código de país (ccTLDs) e os novos gTLDs tiveram crescimento.

Figure 1: Number of Domains by Category, 2009-2018



Source: ZookNIC Domain Counts for Legacy gTLDs, ccTLDs and New gTLDs

Em seu draft[2], a ICANN lista uma série de riscos estratégicos que podem comprometer seus objetivos no quinquênio 2021-2025. São eles:

Strategic Objective 1: Strengthen the security of the Domain Name System and the DNS Root Server System.

STRATEGIC RISKS

- Successful cyberattacks and information warfare undermine trust in the DNS.
- Stronger control over the Internet and cybersecurity by governments changes how security and stability of the DNS can be addressed.
- Stronger control over the Internet and cybersecurity by governments could influence DNS root server governance structures.
- Creation of alternative DNS root infrastructures could facilitate the creation of alternative DNS root name spaces.
- The lack of an accountable governance structure could impact DNS root service delivery and reduce trust in the root server operators and the DNS more generally.
- National or regional regulations cause unintended consequences, which threaten the security and stability of the single, interoperable Internet.
- Inability to mitigate security threats undermines confidence in institutions responsible for the security and stability of the DNS.

2 Fonte: https://www.icann.org/en/system/files/files/revised-strategic-plan-2021-2025-draft-23may19-en.pdf

- Competing priorities -- such as public safety, personal security, privacy, and socioeconomic concerns -- raise challenges in mitigating DNS security threats.
- Domain name abuse continues to grow.
- Successful cyberattacks and information warfare undermine trust in the DNS.
- Failure of the DNS root key signing service would threaten Internet operations.
- Lack of improved root zone distribution service could lead to the overloading of the existing root zone distribution mechanisms.

Strategic Objective 2: Improve the effectiveness of ICANN's multistakeholder model of governance.

STRATEGIC RISKS

- The cost to implement ICANN's multistakeholder model becomes unaffordable.
- Unclear community and organizational priorities compete for scarce resources.
- Polarized positions or agendas that do not represent the collective interest impede progress and waste resources.
- Increased workload for the ICANN community, Board, and org impact the ability to effectively support ongoing work, resulting in community fatigue or stakeholder disengagement.
- Process complexity impedes ICANN's ability to keep pace with the speed of external events that impact its future.
- Perceived or actual delays in decision-making fuel doubts about ICANN's ability to address serious global issues in a timely fashion.
- Limited resources could impact the ability for stakeholders to participate, which could compromise the credibility and integrity of the multistakeholder model.
- Trends toward multilateralism, as well as changing economic, societal, and governmental interests, result in increased pressures on the ICANN multistakeholder model.
- Stakeholder-specific interests preempt Internet policy or governance discussions, impairing the ICANN multistakeholder model.
- Divergence of interests inherent to the multistakeholder model and a perceived lack of global representation fuel doubts about ICANN's effectiveness.

Strategic Objective 3: Evolve the unique identifier systems in coordination and collaboration with relevant parties to continue to serve the needs of the global Internet user base.

STRATEGIC RISKS

- Insufficient readiness for Universal Acceptance, IDN implementation, and IPv6 could result in a failure to serve Internet users' needs.

- Lack of coordination among technical bodies on policy development and standard-setting processes could impact use and adoption of IDNs.
- Failure of the DNS to evolve threatens the single, interoperable Internet, and technical coordination becomes more complex.
- New layers added to a stagnant DNS core technology and the growing viability of alternate DNS roots and alternative infrastructures add more complexity to the Internet ecosystem.
- The complexity of the Internet ecosystem makes technological change difficult.
- Unsuccessful delivery of the IANA functions undermines ICANN's ability to fulfill its mission.
- Increase in security threats raises concerns about the stability of the DNS root and erodes confidence in its dependability.
- A new gTLD round may not achieve its objectives.
- Technical failures within the domain name space expansion could affect the stability of the unique identifier systems and underlying infrastructure.

Strategic Objective 4: Address geopolitical issues impacting ICANN's mission to ensure a single, globally interoperable Internet.

STRATEGIC RISKS

- ICANN's inability to establish itself as a key player in Internet governance results in increased external interventions by nation states or other entities.
- Failure to anticipate legislative efforts force ICANN into a reactive mode.
- Lack of understanding of ICANN's remit interferes with ICANN's ability to participate in relevant arenas.
- Internet infrastructure, security, and government control continue to vary by region or nation.
- Threats to a single, interoperable Internet – such as alternative DNS roots or diminished commonality within networks – fuel doubt in ICANN's ability to serve a global Internet.

Strategic Objective 5: Ensure ICANN's long-term financial sustainability

STRATEGIC RISKS

- ICANN is unable to adjust to changes in the domain name marketplace that impact funding, and becomes unable to fulfill its mission.
- Inefficient financial planning results in an inability to address essential requirements of ICANN's mission.
- The DNS industry evolves in a manner or at a speed that makes it difficult for ICANN to make reliable predictions about the future of the marketplace.

- The relevance and reliability of ICANN org’s funding projections could be affected by a lack of understanding about the evolution of the DNS and how it may impact the perceived or actual value of domain names to the public, therefore impacting the domain name registrations.
- Lack of alignment or consensus on priorities and goals among ICANN stakeholders results in conflicts about resource allocation.
- Expenditures grow faster than funding, eroding ICANN’s reserves.

b) DAAR

O Domain Abuse Activity Reporting System (DAAR) realizou reuniões de trabalho e sessões de update sobre o andamento da implementação do sistema que é usado para rastrear abusos em domínios genéricos, agregando vários dados de várias fontes públicas, abertas e comerciais (dados da zona DNS, dados WHOIS, listas de bloqueio de reputação comercial, etc). O escopo do DAAR coleta dados sobre abuso de DNS nas seguintes categorias: phishing, malware, spam e botnet command & control.

O DAAR deve permitir uma tomada de decisões e formulação de políticas de segurança mais robustas e melhor informadas.No entanto, alguns participantes (Tucows Inc., Verisign) alertaram que a ICANN deve ficar longe do conteúdo e que este exercício estava beirando a avaliação do conteúdo de um site. A ICANN respondeu que eles são muito seletivos na escolha de feeds de dados (principalmente em termos de ficar longe do conteúdo do site).

Outras preocupações expressas foram que domínios inexistentes (excluídos) ainda aparecem nos feeds de reputação. Isso significa que os registros que tomam medidas para tratar do abuso relatado ainda veem um impacto negativo em sua reputação, mesmo depois que o problema foi resolvido. A ICANN confirmou que o modelo de governança dos feeds de abuso é de fato um importante fator decisivo para inclusão no DAAR ou não. Não havia uma resposta clara sobre como se pode fazer a distinção entre domínios comprometidos versus domínios maliciosos.

O relatório com dados consolidados até 28 de fevereiro de 2019 do sistema DAAR considerou 194.076.739 nomes ativos de 1204 domínios genéricos de primeiro nível (gTLDs), em comparação com 193.080.798 domínios ativos em 1153 gTLDs relatados em 31 de janeiro de 2019.

O sistema DAAR detectou pelo menos uma ameaça de segurança em 394 dos 1204 gTLDs em 28 de fevereiro de 2019 em comparação com 357 dos 1153 gTLDs identificados em 31 de janeiro de 2019.

Aproximadamente 88% dos nomes de domínio em resolução estavam em gTLDs lançados antes de 2010 (doravante denominados "Legacy gTLDs"). Dos 1.556.524

domínios identificados como ameaças à segurança, 756.162 ou 48,58% estavam em Legacy gTLDs. Os outros 800.362 ou 51,42% estavam nos novos gTLDs.

Dados relativos a códigos de países (ccTLDs) ainda não são coletados pelo DAAR. A inclusão de registros de DPNs de ccTLDs, nos quais as informações de registros de ccTLDs são voluntariamente fornecidas pelo administrador de ccTLDs, está prevista para futuras atualizações.

A tabela abaixo fornece uma listagem dos fornecedores e feeds de reputação usados no sistema DAAR, juntamente com seus tipos de ameaças correspondentes.

Reputation provider	Feed used	Threat type
SURBL [3]	JwSpamSpy + Prolocation Sa-blacklist SpamCop AbuseButler Phishing domains Malware domains	Spam Spam Spam Spam Phishing Malware
Spamhaus [4]	Domain Block List (DBL) [5]	Spam - Phishing - Malware - Botnet C&C
Anti-Phishing Working Group [6]	Phishing URLs	Phishing
PhishTank [7]	Phishing URLs	Phishing
Malware Patrol [8]	Malware URLs Ransomware URLs Botnet C&C URLs	Malware Malware Botnet C&C
Abuse.ch [9]	FeodoTracker [10] Ransomware Tracker [11]	Malware Malware

Os slides com a excelente apresentação sobre o DAAR na ICANN64 está disponível em: https://static.ptbl.co/static/attachments/200862/1552396738.pdf?1552396738

c) nomes geográficos

A linha de trabalho 5 (WT5) é um subgrupo do Grupo de Trabalho de Processo de Desenvolvimento de Políticas (PDP) de Procedimentos Subsequentes de novos gTLDs. O GT geral é encarregado de determinar se e quais mudanças são necessárias para as recomendações existentes da política em vigor desde 2007. O WT5 procura revisar a política e a implementação existentes relacionadas ao tópico de nomes geográficos no nível superior, e determinar se são necessárias mudanças e recomendar diretrizes revisadas ou novas de políticas e/ou de implementação.

O escopo do WT5 inclui questões que dizem respeito a nomes geográficos no nível superior, incluindo combinações de letra alfabética ASCII de dois caracteres em nível superior, nomes de países e territórios, nomes de cidades, capitais, nomes regionais, província, estado, etc.), regiões protegidas pela UNESCO e outros nomes geográficos (por exemplo: nomes de rios, montanhas, etc.) e termos culturalmente significativos relacionados à geografia.

Havia aproximadamente 50 novos gTLDs geográficos em operação e 1,3 milhão de domínios sob gerenciamento no final de 2018. Embora os marcadores geográficos existissem há muito tempo na forma de ccTLDs, os novos gTLDs geográficos representam uma mudança de escala do nível do país para os níveis locais, principalmente centros urbanos como .london e .tokyo. Essa abordagem se baseia na capacidade de os registrantes estabelecerem identidades associadas às suas cidades de origem e expandirem a especialização em categorias geográficas. Também destaca a flexibilidade dos novos gTLDs em fornecer pontos importantes para a criatividade empreendedora na formação de identidades on-line.

Para os ccTLDs, a Recomendação Preliminar 2, que sugere “continuar reservando todas as combinações ASCII de letras maiúsculas de dois caracteres no nível superior para códigos de países existentes e futuros”, é de particular importância. É aí que a questão de permitir sequências de 1 letra / 1 dígito foi levantada na rodada de consulta pública, pois há um risco de similaridade entre os códigos de país existentes e combinações novas similares (por exemplo, .f1 e .fi, ou. n1 e .nl etc). O WT5 determinou que esse problema está fora do escopo, devido ao fato de essas combinações não serem nomes geográficos. Ainda não está decidido se o problema das seqüências de 1 letra / 1 dígito pode ser movido para WT2. O WT2 é referenciado a esse respeito porque algumas considerações do processo de *application* analisam a confusão de cadeias de caracteres. Como resultado, combinações de 1 letra / 1 dígito podem ser colocadas em um teste de confusão, em vez de serem completamente restritas.

Outras questões divergentes que são relevantes para os ccTLDs também incluíram a questão dos códigos alfa-3 na norma ISO-3166-1, que devem ser disponibilizados para registro. Alguns participantes apoiam a disponibilidade geral para qualquer candidato, enquanto outros apenas com a aprovação do governo ou autoridade pública. Durante a reunião, o direito de um país ao seu código de país foi questionado. No entanto, os participantes foram lembrados de que, qualquer que seja a conclusão do WT5, isso significaria pouco para os ccTLDs na prática. Nenhuma regra inter-jurisdicional pode ser estabelecida como resultado de um trabalho da WT5, pois cada país pode anular essas práticas com uma decisão judicial respectiva. Essa hipótese é exemplificada pelo caso “france.com”, em que o estado da França reivindicou com sucesso o direito soberano do país à palavra “França” e exigiu que o nome de domínio privado france.com fosse transferido para a República Francesa como um resultado.