ICANN | GAC
Governmental Advisory Committee

ICANN 65 POLICY FORUM
MARRAKECH
24–27 June 2019

# Mitigação de abusos do DNS

## Sessão 5.1

## Índice


Histórico 2
Assuntos 3
Proposta da liderança para ação do GAC 5
Acontecimentos relevantes 6
Definição de abuso do DNS: Consenso sobre a infraestrutura de abuso? 6
Definição de Abuso do DNS: Diálogo com a equipe de Proteções do Consumidor 7
Conhecimento e transparência: conversa com a Comunidade liderada pelo GAC 8
Conhecimento e transparência: estudos sobre Abuso do DNS 9
Conhecimento e transparência: DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) 10
Eficiência: atuais proteções contra abusos do DNS em contratos de Registros e Registradores 11
Eficiência: estrutura não vinculativa para Registros responderem a ameaças à segurança 12
Eficiência: medidas proativas e prevenção contra abusos sistêmicos 13
Posições atuais 13
Documentos de referência importantes 14


## Objetivos da sessão

- Analisar os recentes acontecimentos e discussões sobre a definição, a detecção e a mitigação de abuso do DNS, bem como o impacto da conformidade de WHOIS no trabalho do GDPR.
- Debater sobre posições e possíveis próximas etapas para o PSWG (Public Safety Working Group, Grupo de Trabalho sobre Segurança Pública) do GAC e o próprio GAC.

## Histórico

As atividades maliciosas na Internet ameaçam e afetam os registrantes de nomes de domínio e usuários finais aproveitando as vulnerabilidades em todos os aspectos dos ecossistemas da Internet e do DNS (protocolos, sistemas de computadores, transações pessoais e comerciais, processos de registro de domínios etc.). Algumas dessas atividades inescrupulosas ameaçam a segurança, a estabilidade e a resiliência das infraestruturas do DNS, e do DNS como um todo.

Essas ameaças e atividades maliciosas geralmente são chamadas de "Abuso do DNS" na Comunidade da ICANN. Em geral, entende-se que Abuso do DNS refere-se a atividades inteiras ou parte delas, como ataques de DDoS (Distributed Denial of Service, Negação de Serviço Distribuída), spam, phishing, malware, botnets e a distribuição de materiais ilegais. Embora todos concordem que o abuso é um problema que precisa ser resolvido, existem opiniões diferentes sobre a quem atribuir essa responsabilidade. Os Registros e os Registradores, em particular, estão preocupados que seja solicitado que eles façam mais, já que isso afeta o modelo de negócios e o escopo deles.

Como parte desta discussão, é importante observar que até mesmo a definição exata de "Abuso do DNS" é um assunto para debate[1].

Ainda assim, a discussão progrediu nos últimos anos. Este é um resumo dos trabalhos realizados anteriormente pela Comunidade da ICANN para solucionar o Abuso do DNS, e alguns deles contaram com a participação do GAC:

- A **GNSO (Generic Names Supporting Organisation, Organização de Apoio a Nomes Genéricos)** da ICANN organizou um Grupo de Trabalho sobre Políticas de Abuso de Inscrições em 2008. Ele identificou um conjunto de assuntos específicos, mas não gerou resultados de políticas nem realizou uma discussão posterior sobre práticas recomendadas não vinculativas para Registradores (inclusive workshops durante o ICANN41 e o ICANN42).

- **Como parte do Programa de Novos gTLDs,** uma série de novos requisitos[2] adotados pela Organização ICANN de acordo com seu memorando sobre como mitigar condutas maliciosas (3 de outubro de 2009). A eficiência deles foi avaliada nas Relatório da ICANN sobre as proteções do Programa de Novos gTLDs (18 de julho de 2016), em preparação para a Revisão prevista no Estatuto (Revisão de CCT).

- Antes da criação do PSWG (Public Safety Working Group, Grupo de Trabalho sobre Segurança Pública) do GAC, os **representantes de LEAs (Law Enforcement Agencies, Agências Legais Fiscalizadoras)** tiveram uma posição de liderança na negociação do

[1] Conforme evidenciado na discussão sobre as Proteções do consumidor e Abuso do DNS durante a Cúpula da GDD (7 e 8 de maio de 2019).

[2] Investigar os operadores de registro, exigir um plano demonstrado para a implementação de DNSSEC, proibir o uso de caracteres curinga, remover registros glue órfãos quando uma entrada no servidor de nomes for removida da zona, exigir a manutenção dos registros de WHOIS thick, a centralização do acesso de arquivos de zona, exigir procedimentos e contatos de abuso no nível do registro documentados.

Contrato de Credenciamento de Registradores de 2013[3], bem como na elaboração do Conselho do GAC relacionado a Ameaças à Segurança, que resultou em novas disposições no Contrato Básico de Novos gTLDs que descrevia as responsabilidades dos registros. Posteriormente, essas disposições foram complementadas por estrutura para operadores de registros responderem a ameaças à segurança não vinculativas (20 de outubro de 2017) negociadas entre a **Organização ICANN, os Registros e o PSWG**.

- O **SSAC (Security and Stability Advisory Committee, Comitê Consultivo de Segurança e Estabilidade)** emitiu recomendações para a Comunidade da ICANN, em particular no SAC038: ponto de contato de abuso de registrador (26 de fevereiro de 2009) e no SAC040: medidas para proteger os serviços de registro de domínios contra a exploração ou o mau uso (19 de agosto de 2009).

- A **Organização ICANN**, pela **equipe de SSR (Security and Stability Review, Revisão de Segurança e Estabilidade)**, treina regularmente as comunidades de segurança pública e ajuda a responder a incidentes cibernéticos de grande escala, inclusive por meio do ERSR (Expedited Registry Security Request Process, Processo de Solicitação Expressa de Segurança no Registro). Mais recentemente, o **Escritório de CTO** da ICANN liderou o projeto DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios), que gera relatórios mensais sobre abusos. Essa ferramenta tem sido apoiada veementemente pelo GAC e por várias Equipes de Revisão Específica como uma forma para criar transparência e identificar as causas dos problemas, que podem, assim, ser solucionados por meio da conformidade ou, quando necessário, uma nova política.

## Assuntos

As iniciativas anteriores ainda não resultaram em uma redução efetiva de abusos do DNS. Pelo contrário, está mais claro que ainda há muito a ser feito. Apesar da atenção da Comunidade da ICANN e as práticas recomendadas existentes do setor para mitigar o Abuso do DNS, algumas iniciativas de participação da Comunidade lideradas pelo GAC, bem como a análise estatística sobre abuso do DNS em gTLDs da Revisão de CCT (9 de agosto de 2017), que destacaram tendências persistentes de abuso, práticas comerciais que resultam em abuso e evidências de que há um "*escopo para o desenvolvimento e o aprimoramento das atuais proteções e medidas de mitigação*", além do potencial para desenvolver políticas no futuro[4].

Além disso, em função da entrada em vigor do GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) da União Europeia e de outros recursos para colocar em conformidade o sistema de WHOIS, uma ferramenta investigativa essencial contra crimes e

[3] Consulte as recomendações de devida diligência das agências legais fiscalizadoras (outubro de 2019) e a 12 recomendações das agências legais fiscalizadoras (1º de março de 2012)

[4] Consulte o comentário do GAC (19 de setembro de 2017) sobre o Relatório Final da análise estatística sobre abuso do DNS em gTLDs.

abusos, começaram a surgir preocupações quanto à capacidade de realmente mitigar o Abuso do DNS entre as agências legais fiscalizadoras e os círculos de segurança cibernética, segurança do consumidor e proteção de propriedade intelectual[5].

Nesse contexto, os Comitês Consultivos da ICANN, particularmente o GAC, o SSAC e o ALAC, e diversos terceiros afetados entraram em contato com o departamento de Conformidade Contratual e Proteções do Consumidor da ICANN para pedir que a Organização ICANN e a Comunidade da ICANN tomasse providências[6].

Essas providências exigiriam que a comunidade da ICANN encontrasse algum tipo de consenso sobre várias questões em aberto. As discussões sobre a mitigação de abuso e um possível trabalho de política na Comunidade da ICANN geralmente giram em torno dos seguintes tópicos:

- **Definição de Abuso do DNS:**
  O que constitui abuso considerando o âmbito da ICANN e dos contratos dela com Registros e Registradores?
- **Detecção e emissão de relatórios de abuso do DNS (perspectiva de transparência e conscientização):**
  Como podemos garantir que o Abuso do DNS seja detectado e informado às partes interessadas relevantes, inclusive consumidores e usuários da Internet?
- **Prevenção e mitigação de Abuso do DNS (perspectiva da eficiência):**
  Quais ferramentas e procedimentos a Organização ICANN, os participantes do setor e as partes interessadas podem usar para reduzir a ocorrência de abusos e responder adequadamente quando eles ocorrerem? Quem é responsável por quais partes do quebra-cabeça, e como diferentes partes podem cooperar entre si?

O GAC, em um esforço para melhorar a segurança e a estabilidade para os usuários da Internet em geral, talvez queira participar mais ativamente na discussão sobre esses tópicos para que possamos avançar em direção a soluções mais eficientes para a prevenção e a mitigação de abusos.

[5] Consulte a Seção III.2 e IV.2 no Comunicado do GAC de Barcelona (25 de outubro de 2018) que indica algumas pesquisas sobre o impacto nas agências legais fiscalizadoras na seção 5.3.1 do Relatório Preliminar da Equipe de Revisão de RDS (31 de agosto de 2018) e em uma publicação dos Grupos de Trabalho sobre Anti-phishing e Antiabuso de Mensagens, Malware e Dispositivos Móveis (18 de outubro de 2018)

[6] Consulte a discussão sobre Proteções do consumidor e Abuso do DNS realizada durante a Cúpula da GDD (7 e 8 de maio de 2019)

## Proposta da liderança para ação do GAC

Durante o encontro ICANN65, em Marrakesh, o GAC talvez queira:

1. **Solicitar um processo para esclarecer o que constitui Abuso do DNS** em relação à missão da ICANN, e estabelecer sua própria posição sobre o assunto. Isso seria importante para incentivar as discussões sendo realizadas na Comunidade da ICANN sobre a existência dessa definição, as recomendações da Equipe de Revisão de CCT sobre Abuso do DNS, a consideração delas pela Diretoria da ICANN, bem como as iniciativas já implementadas pela equipe de Proteções do Consumidor da ICANN.

2. **Considerar a necessidade e a oportunidade para o desenvolvimento de políticas**, considerando uma discussão recente sobre essa possibilidade durante a Cúpula da GDD[7], e levando em conta as posições anteriores do GAC sobre essa questão[8].

3. **Analisar as ações tomadas com base nas recomendações da Revisão de CCT** sobre Abuso do DNS (Recomendações 14 a 19), inclusive a consideração delas pela Diretoria da ICANN e o trabalho que elas direcionaram à Organização ICANN, bem como outras considerações de processos e grupos constituintes relevantes da ICANN.

4. **Considerar a possibilidade de mostrar práticas recomendadas do setor no espaço de nomes de ccTLDs**, como a que o .DK apresentou durante o ICANN64[9], e a aplicação delas no setor de gTLDs.

---

[7] Consulte a discussão sobre Proteções do consumidor e Abuso do DNS realizada durante a Cúpula da GDD (7 e 8 de maio de 2019)

[8] Em particular, no seu comentário (19 de setembro de 2017) no Relatório Final da análise estatística sobre abuso do DNS em gTLDs, o GAC observou que

- *"O Estudo sobre Abuso do DNS menciona brevemente a descoberta que certos URLs são usados com mais frequência para distribuir materiais de abuso infantil [...] Seria interessante se o relatório pudesse explicar, elaborar e/ou quantificar essa afirmação de maneira mais clara para que as partes interessadas entendam até que ponto o estudo analisou essa questão, bem como para ajudar nas considerações para uma possível política no futuro."*
- *"As correlações observadas entre políticas de registro mais rigorosas e números menores de abuso sugerem possíveis áreas para o desenvolvimento de políticas no futuro."*
- *"o uso de análises estatísticas devem fornecer informações às políticas futuras sobre abuso do DNS e é necessário realizar outras análises para considerar como essas informações podem ajudar no trabalho da ICANN e das suas equipes de conformidade contratual e segurança, de modo que elas possam responder aos abusos do DNS e prevenir com maior eficiência ocorrências futuras e recorrentes."*

[9] Consulte Lições aprendidas com a sessão: como o domínio .DK reduziu o número de domínios abusivos (13 de março de 2019) e a subsequente discussão realizada pelo PSWG (17 de abril de 2019)

## Acontecimentos relevantes

**Definição de abuso do DNS: Consenso sobre a infraestrutura de abuso?**

Conforme destacado mais recentemente durante a Cúpula da GDD (7 a 9 de maio de 2019), **não há um acordo de toda a Comunidade sobre o que constitui "Abuso do DNS"**, em parte devido às preocupações de algumas partes contratadas com os impactos nos direitos dos usuários e nas funções básicas das partes contratadas, bem como de que a ICANN ultrapasse seu escopo[10].

No entanto, de acordo com a Equipe de Revisão de CCT, existe um **consenso sobre o que constitui "Abuso de segurança do DNS" ou "Abuso de segurança do DNS na infraestrutura do DNS"**, pois entende-se que isso inclui *"formas mais técnicas de atividades maliciosas"*, como malware, phishing e botnets, além de spam *"quando usado como um método de entrega de outras formas de abuso"* [11].

Recentemente, **o departamento de Conformidade Contratual da ICANN referiu-se a "Abuso da infraestrutura do DNS"** em suas comunicações sobre auditorias de Registros e Registradores com relação à implementação de disposições contratuais previstas no Contrato de Registro de Novos gTLDs (Especificação 11 3b) — que se refere a "*ameaças à segurança, como pharming, phishing, malware e botnets*"[12] — e no Contrato de Credenciamento de Registradores (Seção 3.18) — que se refere a "*contatos de abuso*" e "*relatórios de abuso*" sem apresentar uma definição para o termo "abuso" especificamente, mas incluindo a expressão "atividade ilegal" no escopo.

**Do ponto de vista do GAC**, a definição de "ameaças à segurança" incluída no Contrato de Registro de Novos gTLDs é de fato a transcrição exata da **definição apresentada no Conselho de Proteções do GAC sobre "verificações de segurança"**, aplicável a todos os novos gTLDs no Comunicado de Pequim (11 de abril de 2013).

Após a resolução da Diretoria (1º de março de 2019) orientando a Organização ICANN a "*facilita[r] o trabalho da comunidade para elaborar uma definição de 'abuso' a fim de ajudar nas próximas ações para essa recomendação*"[13] e a desenvolver atividades com a equipe de Proteções do Consumidor da Organização ICANN, **espera-se que mais discussões sejam realizadas sobre a definição de abuso até o encontro ICANN66**, em Montreal (2 a 7 de novembro de 2019).

---

[10] De fato, a definição de Mitigação de Abuso pode ter várias consequências no que diz respeito ao escopo das atividades supervisionadas pelos contratos e pelas políticas da ICANN. Embora os governos e outras partes interessadas tenham receio quanto ao impacto do abuso do DNS no interesse público, inclusive na segurança do público e na violação de direitos de propriedade intelectual, os Registros e os Registradores estão preocupados com as restrições nas atividades comerciais deles, na capacidade de competir, no aumento dos custos operacionais e na responsabilidade por consequências que poderão afetar os registrantes quando ações forem tomadas nos domínios abusivos. As partes interessadas não comerciais, por outro lado, estão preocupadas com a violação da liberdade de expressão e os direitos de privacidade de registrantes e usuários da Internet, e compartilham com as partes contratadas receios de que a ICANN ultrapasse a missão dela.

[11] Consulte a pág. 88 do Relatório Final da Revisão de CCT (8 de setembro de 2018)

[12] O Conselho, Especificação 11 (3)(b) do Contrato de Registro de Novos gTLDs (8 de junho de 2017) apresenta uma definição para "ameaças à segurança", que inclui "*pharming, phishing, malware, botnets e outros tipos de ameaças à segurança*".

[13] Consulte a pág. 5 do scorecard sobre a ação da Diretoria com relação às recomendações finais da equipe de CCT

**Definição de Abuso do DNS: Diálogo com a equipe de Proteções do Consumidor**

Desde a ampliação da função de Conformidade Contratual da ICANN para incluir Proteções do Consumidor em 2017[14], o GAC participou de várias atividades relacionadas:

- Uma apresentação do diretor do departamento de Proteções do Consumidor da ICANN (27 de junho de 2017), que falou sobre o estabelecimento de uma discussão informal com toda a comunidade para aumentar o conhecimento e entendimento dos membros, além de identificar algumas maneiras para a Organização ICANN fortalecer o desempenho das equipes de Conformidade Contratual e Proteções do Consumidor.

- Um webinário de discussão sobre Conformidade Contratual e Proteções do Consumidor (25 de setembro de 2017), que contou com a participação de quase 100 membros da comunidade, inclusive a discussão sobre um Resumo de Proteções sob o escopo da ICANN (11 de setembro de 2017) e seguida pelo envio de perguntas para contribuições da Comunidade em um blog subsequente (11 de outubro de 2017):
    - Qual deve ser a funções da ICANN na abordagem ao abuso do DNS?
    - Existem lacunas entre abuso do DNS e a autoridade da ICANN para tratar desse abuso?
    - Que dados ou ferramentas adicionais seriam importantes para avaliar o abuso do DNS?
    - Existem áreas onde medidas voluntárias poderiam ajudar?
    - Como a ICANN deve colaborar com outras partes interessadas para solucionar os abusos?
    - Existe uma ameaça de intervenção governamental se a comunidade da ICANN não conseguir solucionar o problema de abusos do DNS de maneira satisfatória?

- Uma reunião com representantes da Comunidade em Washington DC (11 de janeiro de 2019) foi organizada para debater essas questões ainda mais detalhadamente para facilitar a possível participação de toda a comunidade nos próximos encontros da ICANN.

Mais recentemente, durante a Cúpula da GDD (9 de maio de 2019), o departamento de Conformidade Contratual e Proteções do Consumidor liderou uma sessão para dar continuidade ao diálogo:

- **Algumas partes contratadas consideram suas práticas voluntárias de antiabuso adequadas e se opõem que elas se tornem obrigações**, em parte devido à limitação do escopo da ICANN, bem como à dificuldade que representam os relatórios de abuso que não apresentam sugestões viáveis de ações (geralmente enviados por partes que não conhecem o escopo limitado de mitigações disponíveis aos Registros [15] e Registradores).

---

[14] com a contratação do diretor do departamento de Proteções do Consumidor da ICANN (23 de maio de 2017), encarregado de "*aumentar o conhecimento sobre as atuais proteções da ICANN, facilitar a discussão entre as partes interessadas sobre outras formas que a ICANN pode usar para melhorar os mecanismos de proteção*"

[15] Consulte, por exemplo, as *Categorias de Ações de Registros em resposta a ameaças à segurança* no documento voluntário estrutura para operadores de registros responderem a ameaças à segurança

- Outros representantes sugeriram que a **ICANN tem o dever de definir regras e incentivos apropriados** para dissuadir as partes maliciosas, mas sem prejudicar as partes responsáveis (**princípio "poluidor-pagador"**) e que as **partes responsáveis pelo abuso devem ser indicadas** nos relatórios relevantes da ICANN.
- **A Organização ICANN apresentou a ideia de um Processo de Desenvolvimento de Políticas da GNSO** para alinhar os contratos com as expectativas dos Comitês Consultivos e de terceiros, bem como para evitar o impacto de futuras legislações heterogêneas que possam ser colocadas em vigor para substituir as políticas da ICANN.
- Essa sugestão recebeu uma **forte objeção e pedidos de maneiras alternativas para lidar com o problema**, inclusive a reconciliação das definições existentes nas partes relevantes da comunidade ou para entrar em negociações sobre o Contrato de Registro, da mesma forma que foi feito para o RAA (Registrar Accreditation Agreement, Contrato de Credenciamento de Registradores) de 2013.
- As **partes contratadas** solicitaram que a **Organização ICANN promova esforços para informar a Comunidade da ICANN** em nome delas durante o ICANN66, em Montreal, inclusive com uma apresentação de práticas recomendadas e de dados que mostram a prevalência de reclamações para as quais não há ações viáveis.

**Conhecimento e transparência: conversa com a Comunidade liderada pelo GAC**

O GAC e o PSWG (Public Safety Working Group, Grupo de Trabalho sobre Segurança Pública) têm realizado várias conversas entre comunidades nos encontros da ICANN nos últimos anos com o objetivo de **aumentar o conhecimento e explorar soluções com os especialistas relevantes**, a saber:

- Durante o ICANN57, em Hyderabad, (5 de novembro de 2016), o PSWG do GAC realizou uma sessão de tópico de maior interesse sobre a Mitigação de Abuso em gTLDs, que foi estruturada como uma troca de opiniões entre os membros da Comunidade da ICANN e destacou:
  - a ausência de um entendimento comum sobre o que é Abuso do DNS;
  - a diversidade de modelos de negócios, práticas e habilidades que influenciam as abordagens para mitigar abusos; e
  - a necessidade de haver mais cooperação entre os participantes do setor, que seria apoiada por dados compartilhados sobre ameaças à segurança.

- Durante o ICANN58, em Copenhague, (13 de março de 2017), o PSWG do GAC moderou uma sessão entre comunidades (Para a mitigação eficiente de abuso no DNS: prevenção, mitigação e resposta) que tratou das recentes tendências em Abuso do DNS, particularmente phishing, bem como em comportamentos, como "salto de domínio" entre registradores e TLDs, que podem exigir respostas mais coordenadas e sofisticadas no setor. A sessão também serviu para destacar:

    - a iniciativa DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) emergente,
    - a colaboração contínua entre as equipes de SSRT (Security and Stability Review Team, Equipe de Revisão de Segurança e Estabilidade) e Conformidade Contratual da ICANN, e
    - a oportunidade de utilizar os procedimentos para leilões de novos gTLDs para financiar as necessidades da mitigação de abusos.

- Durante o ICANN60, em Abu Dhabi, (30 de outubro de 2017), o PSWG organizou uma sessão entre comunidades sobre emissão de relatórios de abuso do DNS para a elaboração de políticas com base em fatos e mitigação eficiente para discutir o estabelecimento de mecanismo de emissão de relatórios sobre Abusos do DNS que fossem confiáveis, públicos e permitissem ações viáveis, a fim de evitar e mitigar abusos, além de facilitar a elaboração de políticas baseadas em evidências. A sessão confirmou a necessidade de haver a publicação de dados confiáveis e detalhados sobre Abuso do DNS, conforme incluídos na ferramenta DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios) . O PSWG considerou também elaborar possíveis princípios para o GAC[16].

**Conhecimento e transparência: estudos sobre Abuso do DNS**

Várias proteções relacionados a Abuso do DNS foram colocadas no Programa de Novos gTLDs por meio de novos requisitos[17] adotados pela Organização ICANN de acordo com o memorando sobre como mitigar condutas maliciosas (3 de outubro de 2009) e o Conselho de Proteção do GAC sobre as verificações de segurança.

Com base na avaliação da Organização ICANN sobre a eficiência das proteções do Programa de Novos gTLDs (18 de julho de 2016), que contou com a contribuição do GAC (20 de maio de 2016), a Equipe de Revisão de CCT buscou uma análise comparativa mais abrangente dos índices de abuso em gTLDs novos e legados, incluindo uma análise estatística inferida de hipóteses, como as correlações entre os índices de abuso e os preços para a venda de nomes de domínio.

As conclusões dessa análise estatística sobre abuso do DNS em gTLDs (9 de agosto de 2017) foram enviadas para Comentários Públicos. As contribuições da Comunidade foram relatadas (13 de outubro de 2017) como construtivas, elogiando o rigor científico da análise e solicitando que mais estudos como esse fossem realizados.

Nos seus comentários (19 de setembro de 2017), o GAC destacou, entre outras conclusões, que:

- O estudo deixou claro que há problemas sérios de abuso no DNS:
    - Em certos novos gTLDs, mais de 50% dos registrantes são abusivos

[16] Consulte o Anexo 1: Princípios para a Mitigação de Abusos no Documento do GAC do ICANN60 sobre Abuso do DNS e o relatório da sessão no Comunicado do GAC de Abu Dhabi (pág. 3)

[17] Investigar os operadores de registro, exigir um plano demonstrado para a implementação de DNSSEC, proibir o uso de caracteres curinga, remover registros glue órfãos quando uma entrada no servidor de nomes for removida da zona, exigir a manutenção dos registros de WHOIS thick, a centralização do acesso de arquivos de zona, exigir procedimentos e contatos de abuso no nível do registro documentados.

    - Cinco novos gTLDs foram responsáveis por 58,7% de todos os domínios de phishing em novos gTLDs colocados em uma lista negra
- Os abusos estão correlacionados às políticas dos Operadores de Registro:
    - Os operadores de registro dos novos gTLDs com o maior número de abusos são concorrentes diretos de preços;
    - As partes maliciosas preferem registrar domínios em novos gTLDs comuns (abertos para registro público), e não em novos gTLDs de comunidades (com restrições para quem pode registrar os nomes de domínio)
- Existe o potencial para o futuro desenvolvimento de políticas para:
    - Rodadas subsequentes de novos gTLDs, relacionadas a evidências de que o risco varia nas categorias de TLDs, além do rigor da política de registro
    - O aprimoramento das atuais medidas de mitigação e proteções contra abusos, conforme indicado pela análise estatística
- A ICANN deve continuar usando, e expandir esse uso, de análises estatísticas e dados para medir e compartilhar informações com a comunidade sobre o níveis de abuso do DNS.

**Conhecimento e transparência: DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios)**

O projeto de Geração de Relatórios de Atividade de Abuso de Domínios da Organização ICANN começou como um projeto de pesquisa simultâneo à conversa do GAC e do PSWG com a Comunidade e a Diretoria da ICANN sobre a eficiência da mitigação de abusos do DNS, entre o ICANN57 (novembro de 2016) e o ICANN60 (novembro de 2017)[18].

A finalidade declarada do DAAR é "*relatar as atividades de ameaças à segurança para a comunidade da ICANN, que poderá usar os dados para tomar decisões sobre políticas com informações relevantes*". Isso é feito desde janeiro de 2018 com a publicação de relatórios mensais, com base na compilação de dados de registro de TLDs com informações de um conjunto maior de feeds de dados de ameaças à segurança e reputação de alta confiança[19].

Dessa forma, o DAAR está contribuindo para o requisito identificado pelo GAC da publicação de *"dados detalhados e confiáveis sobre Abuso do DNS"* mencionado no Comunicado do GAC de Abu Dhabi (1º de novembro de 2017). No entanto, conforme destacado em uma carta recente do M3AAWG[20] para a Organização ICANN (5 de abril de 2019), ao não incluir as informações de ameaças à segurança de cada registrador para cada TLD, o DAAR ainda não atende às expectativas dos membros do PSWG do GAC e dos parceiros de segurança cibernética de fornecer informações para ações viáveis.

[18] Consulte as sessões entre comunidades lideradas pelo PSWG do GAC durante o ICANN57 (novembro de 2016), o ICANN58 (março de 2017) e o ICANN60 (outubro de 2017), bem como as perguntas enviadas à Diretoria da ICANN sobre a eficiência das proteções de abusos do DNS no Comunicado de Hyderabad (8 de novembro de 2016), as perguntas de acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017) e um conjunto de respostas preliminares (30 de maio de 2017) da Organização ICANN.

[19] Para saber mais, consulte https://www.icann.org/octo-ssr/daar-faqs

[20] Grupo de Trabalho de Mensagens, Malware e Antiabuso em Dispositivos Móveis

**Eficiência: atuais proteções contra abusos do DNS em contratos de Registros e Registradores**

Com base nas recomendações de devida diligência das agências legais fiscalizadoras (outubro de 2009), o GAC buscou a **inclusão das Proteções para a Mitigação de Abusos do DNS nos contratos da ICANN** com Registros e Registradores:

- O Contrato de Credenciamento de Registradores de 2013 (17 de setembro de 2013) foi aprovado pela Diretoria da ICANN (27 de junho de 2013) após a inclusão das disposições que abordavam as 12 recomendações das agências legais fiscalizadoras (1º de março de 2012)
- O Contrato de Registro de Novos gTLDs foi aprovado pela Diretoria da ICANN (2 de julho de 2013) após a inclusão das disposições alinhadas com o Conselho de Proteções do GAC no Comunicado de Pequim (11 de abril de 2013), consistente com a proposta de implementação de proteções do GAC aplicáveis a todos os novos gTLDs da Diretoria da ICANN (19 de junho de 2013)

Após os primeiros anos de operação dos novos gTLDs, durante o ICANN57 (novembro de 2016) **o GAC identificou uma série de disposições e proteções relacionadas para a qual não conseguiu avaliar a eficiência**. Em decorrência disso, no Comunicado de Hyderabad (8 de novembro de 2016) o GAC solicitou esclarecimentos à Diretoria da ICANN sobre a implementação. Isso resultou em um diálogo entre o GAC e a Organização ICANN, perguntas de acompanhamento no Comunicado do GAC de Copenhague (15 de março de 2017) e um conjunto de respostas preliminares (30 de maio de 2017) que foram discutidos em uma teleconferência entre o GAC e o CEO da ICANN (15 de junho de 2017). Várias perguntas continuaram em aberto e novas perguntas foram identificadas, conforme consta em um documento de trabalho posterior (17 de julho de 2017).

Entre os tópicos pendentes de interesse ao GAC, um Conselho, Especificação 11 (3)(b) do Contrato de Registro de Novos gTLDs foi publicado em 8 de junho de 2017 em resposta a perguntas de alguns operadores de registro que buscavam orientação sobre como garantir a conformidade com a Seção 3b da Especificação 11 do Contrato de Registro de Novos gTLDs. **O Conselho apresenta uma abordagem voluntária que pode ser adotada pelos operadores de registro** para realizar análises técnicas a fim de avaliar as ameaças à segurança e gerar relatórios estatísticos, conforme exigido pela Especificação 11 3(b).

Como parte das **auditorias regulares realizadas pelo departamento Contratual da ICANN**, uma auditoria direcionada de 20 gTLDs sobre o "*processo, procedimentos e gerenciamento da infraestrutura do DNS"* deles, entre março e setembro de 2018, revelou que "*havia relatórios de segurança e análises incompletos para 13 TLDs (Top Level Domains, Domínios de Primeiro Nível), bem como a ausência de procedimentos padronizados ou documentos para o gerenciamento de abusos e nenhuma ação tomada quanto às ameaças identificadas*"[21].

[21] Conforme relatado na postagem de blog de 8 de novembro de 2018, Conformidade Contratual: como lidar com abusos na infraestrutura do DNS: https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse

Pouco tempo depois, em novembro de 2018, uma auditoria sobre abusos na infraestrutura do DNS de quase todos os gTLDs foi iniciada para "*garantir que as partes contratadas cumpram suas obrigações contratuais com relação a ameaças à segurança e abusos na infraestrutura do DNS"*. Conforme relatado durante a Cúpula da GDD (9 de maio de 2019), a Organização ICANN ainda deverá lançar o relatório final dessa auditoria (originalmente planejado para maio de 2019) e atualmente planeja iniciar uma auditoria semelhante dos Registradores a partir de julho de 2019.

As **partes contratadas têm acompanhado os problemas com essas auditorias** como excedendo o escopo das suas obrigações contratuais[22]. Entende-se que os Grupos de Partes Interessadas de Registradores e Registros **têm trabalhado com o departamento de Conformidade Contratual da ICANN** para garantir que o relatório final da auditoria da infraestrutura do DNS de registros deixe bem claro qual é o escopo da ICANN (devido à preocupação de que a ausência de clareza faça com que a comunidade solicite o início de um Processo de Desenvolvimento de Políticas) e que os receios dos Registradores sejam levados em conta antes de iniciar a auditoria deles.

**Eficiência: estrutura não vinculativa para Registros responderem a ameaças à segurança**

Como parte do Programa de Novos gTLDs, a Diretoria da ICANN decidiu (25 de junho de 2013) incluir as chamadas "verificações de segurança" (Conselho de Proteções do GAC do Comunicado de Pequim) na Especificação 11 do Contrato de Registro de Novos gTLDs. No entanto, como foi determinado que essas disposições não têm os detalhes da implementação, a Implementação decidiu solicitar a participação da comunidade para elaborar uma estrutura para "*Operadores de Registro responderem a riscos de segurança identificados que representem risco real de dano (…)"*. Em julho de 2015, a ICANN montou uma Equipe Redatora composta de voluntários de Registros, Registradores e do GAC (inclusive com membros do PSWG) que elaborou a estrutura para operadores de registros responderem a ameaças à segurança publicada em 20 de outubro de 2017, depois de passar por um período de comentários públicos.

Esta estrutura é um instrumento voluntário não vinculativo projetado para articular orientações que possam ser usadas pelos registros para responder a ameaças à segurança identificadas, inclusive relatórios de agências legais fiscalizadoras. Ela introduz uma janela de no máximo 24 horas para responder a solicitações de alta prioridade (ameaça iminente à vida humana, infraestrutura essencial ou exploração infantil) de uma origem legítima e confiável, como uma autoridade de agência legal fiscalizadora governamental ou agência de segurança pública de uma jurisdição apropriada.

[22] Consulte a correspondência do RySG (Registries Stakeholder Group, Grupo de Partes Interessadas de Registros) (2 de novembro de 2019) com a seguinte resposta da Organização ICANN (8 de novembro), e nos comentários publicados na página de comunicados (15 de novembro): os registros identificaram problemas com as perguntas da auditoria considerando uma ação de execução ameaçadora que excede o escopo das obrigações contratuais deles [particularmente na Especificação 11 3b] e indicaram relutância para "*compartilhar com a Organização ICANN e a comunidade informações relevantes sobre nossos esforços aplicados para combates abusos do DNS […] como parte de um esforço de Conformidade da ICANN que vai além do que é permitido no Contrato de Registro*"

Conforme disposto na Recomendação 19, a Equipe de Revisão de CCT transferiu a tarefa de realizar uma avaliação da eficiência da Estrutura para uma revisão posterior[23].

**Eficiência: medidas proativas e prevenção contra abusos sistêmicos**

Com base na análise do cenário de Abusos do DNS[24], inclusive a consideração do Relatório da ICANN sobre as proteções do Programa de Novos gTLDs (15 de março de 2016) e a análise estatística sobre abuso do DNS independente (9 de agosto de 2017), a Equipe de Revisão de CCT recomendou, com relação a Abusos no DNS:

- A inclusão de **disposições nos Contratos de Registros para incentivar a adoção de medidas antiabuso proativas** (Recomendação 14)
- A inclusão de disposições contratuais com o objetivo de **prevenir contra o uso sistêmico de registradores ou registros específicos** para Abuso de Segurança do DNS, inclusive com limites de abusos que, se ultrapassados, acionarão consultas de conformidade automáticas, e considerar uma possível DADRP (DNS Abuse Dispute Resolution Policy, Política de Resolução de Disputas de Abusos do DNS), se a comunidade determinar que a Organização ICANN não é indicada ou não é capaz de exigir essas disposições (Recomendação 15)

A Diretoria da ICANN decidiu (1º de março de 2019) colocar essas recomendações com o status "Pendentes", já que orientavam a Organização ICANN a "*facilita[r] o trabalho da comunidade para elaborar uma definição de 'abuso' a fim de ajudar nas próximas ações para essa recomendação*"[25].

## Posições atuais

- Comunicado do GAC de Nairóbi (10 de março de 2010) seção VI. Recomendações de devida diligência das agências legais fiscalizadoras
- Comunicado do GAC de Dakar (27 de outubro de 2011) seção III. Recomendações de LEAs (Law Enforcement Agencies, Agências Legais Fiscalizadoras)
- Comunicado do GAC de Pequim (11 de abril de 2013), em particular as proteções de "verificações de segurança" aplicáveis a todos os novos gTLDs (pág. 7)
- Comunicado do GAC de Hyderabad (8 de novembro de 2016) inclusive o Conselho sobre Mitigação de Abusos solicitando respostas para o Anexo 1 — Perguntas à Diretoria da ICANN sobre a mitigação de abuso do DNS por parte da ICANN e partes contratadas (pág. 14 a 17)

---

[23] Recomendação 19 da Revisão de CCT: *A próxima CCT deverá revisar a "Estrutura para Operadores de Registro responderem a ameaças à segurança" e avaliar se a estrutura é um mecanismo suficientemente claro e eficiente para mitigar abusos, oferecendo medidas específicas e sistêmicas em resposta a ameaças de segurança.*

[24] Consulte a Seção 9 sobre Proteções (pág. 88) do Relatório Final da Revisão de CCT (8 de setembro de 2018)

[25] Consulte a pág. 5 do scorecard sobre ação da Diretoria com relação às recomendações finais da equipe de CCT

- Comunicado do GAC de Copenhague (15 de março de 2017) inclusive o Conselho sobre Mitigação de Abusos solicitando respostas para o scorecard de acompanhamento do GAC relacionado ao Anexo 1 do Comunicado do GAC de Hyderabad (pág. 11 a 32)
- Comunicado do GAC de Barcelona (25 de outubro de 2018) em particular as seções III.2 do Grupo de Trabalho de Segurança Pública do GAC (pág. 3) e IV.2 Legislação sobre Proteção de Dados e WHOIS (pág. 5)
- Comentário do GAC sobre o Relatório Inicial da SADAG (21 de maio de 2016)
- Comentário do GAC sobre a análise estatística de abuso do DNS em gTLDs (19 de setembro de 2017)
- Comentário do GAC sobre as recomendações e o Relatório Final da Revisão de CCT (11 de dezembro de 2018)

## Documentos de referência importantes

- recomendações de devida diligência das agências legais fiscalizadoras (outubro de 2019)
- Recomendações de LEAs sobre aditamentos aos Contratos de Registros (1º de março de 2012)
- Conselho de Proteções do GAC sobre "verificações de segurança" aplicável a todos os novos gTLDs (pág. 7) no Comunicado de Pequim (11 de abril de 2013)
- Perguntas do GAC sobre a mitigação de abusos e respostas preliminares da ICANN (30 de maio de 2017) de acordo com o Conselho no Comunicado do GAC de Hyderabad (8 de novembro de 2016) e seguimento no Comunicado do GAC de Copenhague (15 de março 2017)
- análise estatística sobre abuso do DNS em gTLDs (9 de agosto de 2017)
- Comentário do GAC sobre a análise estatística de abuso do DNS em gTLDs (19 de setembro de 2017)
- Comentário do GAC (16 de janeiro de 2018) sobre as novas seções do Relatório Preliminar da Equipe de Revisão de CCT (27 de novembro de 2017)
- Recomendações e Relatório Final da Revisão de CCT (8 de setembro de 2018), em particular a Seção 9 sobre Proteções (pág. 88)
- Comentário do GAC sobre as recomendações e o Relatório Final da Revisão de CCT (11 de dezembro de 2018)
- Scorecard de ação da Diretoria com relação às recomendações finais da equipe de CCT da Diretoria da ICANN (1º de março de 2019)

## Informações relacionadas

- ICANN65 — Sessão 11.1 do GAC sobre as Revisões da ICANN (inclusive os documentos relevantes sobre o status da implementação das recomendações da Revisão de CCT)
- ICANN65 — Sessão 8.1 do GAC sobre Política de Proteção de Dados e WHOIS
- ICANN65 — Sessão 4.1 do GAC sobre os Procedimentos Subsequentes de Novos gTLDs

## Administração do documento

| | |
|---|---|
| **Encontro** | ICANN65 de Marrakesh, 24 a 27 de junho de 2019 |
| **Título** | Mitigação de abusos do DNS |
| **Distribuição** | Membros do GAC e público (após o encontro) |
| **Data de distribuição** | Versão 1: 6 de junho de 2019 |