ICANN | GAC
Governmental Advisory Committee

ICANN 73 VIRTUAL COMMUNITY FORUM

Mitigação de Abusos do DNS

Sessão 10

Índice

Objetivo da sessão	p.1	Proposta da liderança para ações do GAC	p.1	Status atual e acontecimentos recentes	p.2	Principais documentos de referência	p.8

Objetivos da sessão

Esta sessão tem como objetivo dar continuidade à consideração pelo GAC das iniciativas da organização e da comunidade da ICANN para evitar e mitigar abusos do DNS. Isso inclui a implementação das recomendações feitas pelas equipes de revisão de CCT e SSR2, discussões que seguiram a conclusão do PDP WG da GNSO sobre Procedimentos Subsequentes de Novos gTLDs, as propostas recentes do SSAC para estabelecer um facilitador comum para resposta a abusos e um estudo recente publicado pela Comissão Europeia. A sessão também será uma oportunidade para continuar a discussão sobre possíveis propostas concretas do GAC.

Proposta da liderança para ações do GAC

1. **Considerar as conclusões e as recomendações do Estudo sobre Abusos do DNS publicado pela Comissão Europeia**[1] e enviado ao Grupo de Trabalho de Segurança Pública do GAC antes do ICANN73.[2]

2. **Revisar o andamento das atividades da Organização ICANN** com relação a abusos do DNS, de acordo com seus programas de Conformidade Contratual e de Mitigação de Ameaças à Segurança do DNS, conforme relatado mais recentemente no resumo do CEO da ICANN apresentado ao GAC antes do ICANN73.[3]

[1] Consulte o Estudo sobre Abusos do DNS da Comissão Europeia e seu Anexo com informações técnicas (31 de janeiro de 2022)

[2] Consulte https://gac.icann.org/sessions/pre-icann73-pswg-conference-call (17 de fevereiro de 2022) [login necessário]

[3] Consulte https://gac.icann.org/sessions/icann-org-ceo-pre-icann73-oral-briefing-for-the-gac (16 de fevereiro de 2022) [login necessário]

3. **Avaliar o andamento de discussões e de trabalhos de implementação na comunidade da ICANN com relação** às recomendações relevantes das equipes de revisão de CCT e SSR2 e da equipe de trabalho do SSAC sobre abusos do DNS (SAC115), bem como iniciativas voluntárias de partes contratadas, tendo em vista os Conselhos do GAC relevantes nos Comunicados de Montreal do ICANN66 e do ICANN72.

Status atual e acontecimentos recentes

Discussões da comunidade e etapas concretas realizadas até o momento

- Durante os encontros recentes da ICANN, **líderes do Grupo de Trabalho de Segurança Pública do GAC apresentaram um resumo ao GAC** sobre a questão de abusos do DNS[4], de maneira consistente com o Plano de Trabalho do PSWG para 2020-2021 e seu objetivo estratégico nº 1, de desenvolver recursos para a mitigação de abusos do DNS e crimes cibernéticos.
    - O GAC analisou **as medidas disponíveis para registros e registradores evitarem abusos do DNS**, especificamente a função das políticas de registro (incluindo a verificação de identidade) e estratégias de preços como determinantes essenciais dos níveis de abuso em um determinado TLD.
    - O GAC também examinou **iniciativas em andamento ou em potencial para lidar com abusos do DNS de maneira mais eficiente na Diretoria da ICANN e na Organização ICANN em geral**[5], incluindo revisões de contratos da ICANN com registros e registradores, a fiscalização dos requisitos existentes, a implementação das recomendações relevantes da revisão de CCT e de SSR2, as recomendações de políticas para provedores de Serviços de Privacidade/Proxy, o aprimoramento da precisão dos dados de registro e a publicação de dados mais detalhados sobre atividades de abusos em domínios.
    - No Comunicado do ICANN72 (1º de novembro de 2021), o GAC destacou "***a necessidade de aprimorar os requisitos contratuais para lidar com o problema de abusos do DNS com mais eficiência***. *Quanto a essa questão, a função da ICANN, conforme consta no Estatuto, inclui considerar adequadamente as preocupações de políticas públicas de governos e autoridades públicas e agir para o benefício do público. O Estatuto também autoriza a ICANN a negociar acordos, inclusive Compromissos de Interesse Público, a serviço de sua Missão. Dessa forma, a posição da ICANN é particularmente favorável para negociar aprimoramentos aos contratos existentes de modo a evitar abusos do DNS de maneira eficaz, conforme indicado pelo GAC e por outras partes interessadas atuando em defesa do interesse público*".

[4] Veja o material da sessão plenária do GAC relacionada durante o ICANN66, o ICANN68, o ICANN69, o ICANN70, o ICANN71 e o ICANN72

[5] Veja a ata do ICANN66, o Comunicado do GAC do ICANN68 e ata, o Comunicado do ICANN69 e ata, o Comunicado do ICANN70 e ata e o Comunicado do ICANN71 e ata.

- **Líderes do GAC e do Conselho da GNSO debateram sobre perguntas específicas do GAC** enviadas à GNSO antes de cada encontro da ICANN desde o ICANN70[6]
    - **O GAC solicitou atualizações da GNSO sobre o trabalho da comunidade que pretende realizar**, tendo em vista as conclusões do PDP de Rodadas Subsequentes de Novos gTLDs (que não fez recomendações sobre a mitigação de abusos do DNS apenas para futuros novos gTLDs), as recomendações da revisão de SSR2 e as recomendações do SSAC no SAC115.
    - **Os líderes do Conselho da GNSO reconheceram a importância desse assunto para a comunidade da ICANN** e a discussão já antiga sobre isso, mas observaram que, **para continuar trabalhando nisso, é necessário a elaboração de um escopo apropriado**, bem como o desenvolvimento de **um entendimento comum**, particularmente no que diz respeito à definição de abuso do DNS e sua compatibilidade com a missão da ICANN, **sem a indicação de um cronograma**[7].
    - Em 31 de janeiro de 2022, o Conselho da GNSO anunciou a formação de uma **Equipe Pequena da GNSO para considerar "*que trabalhos de políticas, se fosse o caso, o Conselho da GNSO deveria pensar em realizar*** *para apoiar as atividades que já estavam em andamento nas diferentes partes da comunidade para lidar com abusos do DNS"* e "*conversar com outros participantes da comunidade que se pronunciaram sobre o assunto (como o Comitê Consultivo para Assuntos Governamentais [...]) para entender melhor as expectativas deles para a GNSO, bem como se/como eles imaginam que mais atividades relacionadas a políticas contribuiriam (ou não) para as iniciativas que já estão em andamento"*.

- **Medidas e iniciativas para mitigar abusos do DNS por registros e registradores**
    - Em 27 de março de 2020, a organização ICANN executou o aditamento proposto no Contrato do Registro de .COM, que **amplia as disposições contratuais para facilitar a detecção e a geração de relatórios de abusos do DNS para dois terços do espaço de nomes de gTLDs[8]**. Além disso, uma carta de intenção vinculante entre a organização ICANN e a Verisign define uma estrutura de cooperação para desenvolver práticas recomendadas e possíveis novas obrigações contratuais, além de medidas para ajudar a medir e reduzir as ameaças à segurança do DNS.

[6] Veja as Mensagens e Perguntas para o Conselho da GNSO antes do ICANN70

[7] Consulte as Atas do ICANN70 (pág. 16), as Atas do ICANN71 (pág. 13) e as Atas do ICANN72 (pág. 9)

[8] Essas disposições incluem a Especificação 11 3b, que até o momento se aplicava apenas a novos gTLDs.

- **No contexto da crise gerada pela COVID-19, as partes contratadas e as partes interessadas de segurança pública** relataram[9] em sua colaboração encaminhar relatórios, sua revisão e referências à jurisdição relevante por meio da adoção de um formulário padronizado e do estabelecimento de um ponto único de contato para as autoridades relevantes. Essas iniciativas têm como base as relações de trabalho estabelecidas entre as agências legais fiscalizadoras e os registradores, além da publicação de um Guia para denúncias de abuso de registradores pelo **Grupo de Partes Interessadas de Registradores** durante o ICANN67. Esse guia foi atualizado (janeiro de 2022) e endossado pelo **Grupo de Partes Interessadas de Registros**.
- O **PIR (Public Interest Registry, Registro de Interesse Público)**, operador de registro de .ORG e vários novos gTLDs, lançou (17 de fevereiro de 2021) o **DNS Abuse Institute** (Instituto para Abusos do DNS). Essa iniciativa foi apresentada ao PSWG do GAC (3 de março de 2021). No Comunicado do ICANN70, o GAC parabenizou o lançamento do DNS Abuse Institute e *"incentiva[ou] que a comunidade trabalhe de modo colaborativo para lidar com Abusos do DNS de maneira abrangente"*. Desde então, o DNS Abuse Institute lançou um roteiro (14 de junho de 2021) e publicou um artigo (24 de agosto de 2021) que trata da mitigação de prejuízos em diversas camadas da infraestrutura da Internet. Mais recentemente, ele informou estar desenvolvendo uma ferramenta centralizada para denúncias de abusos (18 de novembro de 2021) e divulgou uma prática recomendada para a identificação de registros maliciosos (2 de dezembro de 2021).

- **Resposta multifacetada da Organização ICANN[10] (que agora faz parte do Programa de Mitigação de Ameaças à Segurança do DNS) e fiscalização contratual**
  - A Organização ICANN apresentou (22 de julho de 2021) seu Programa de Mitigação de Ameaças à Segurança do DNS, que tem como objetivo fornecer visibilidade e clareza sobre os diversos projetos e iniciativas dedicados a ameaças à segurança do DNS e permite a formação e a execução de uma estratégia centralizada.
  - **O OCTO (Office of the CTO, Gabinete do Diretor de Tecnologia) da ICANN e sua equipe de SSR (Security, Stability and Resiliency; Segurança, Estabilidade e Resiliência)** conduzem pesquisas e mantêm a expertise da ICANN em segurança do DNS para o benefício da comunidade. Ele participa em grupos de inteligência contra ameaças cibernéticas e resposta a incidentes e também desenvolve sistemas e ferramentas para ajudar na identificação, análise e denúncia de abusos do DNS[11].

---

[9] Veja as apresentações das partes contratadas antes e durante o encontro ICANN68 e o resumo do PSWG para o GAC durante o ICANN68.

[10] O CEO da ICANN fez uma publicação no blog em 20 de abril de 2020 detalhando a resposta multifacetada da organização ICANN a abusos do DNS.

[11] Durante uma conferência do GAC sobre questões relacionadas a abusos do DNS (24 de fevereiro de 2021), a organização ICANN apresentou atualizações sobre as atividades do OCTO dedicadas a abusos do DNS, que incluíram uma discussão sobre a definição de ameaças à segurança do DNS e abusos do DNS, as obrigações das partes contratadas, a plataforma de geração de relatórios de atividades de abuso em domínios (DAAR), informações, coleta e relatórios de ameaças à segurança de nomes de domínio (DNSTICR), o status da iniciativa de promoção da segurança em domínios (DSFI), a nova iniciativa de compartilhamento de conhecimento e criação de normas para a segurança em nomes de domínio (KINDNS) e uma revisão dos trabalhos do OCTO na área de treinamento e capacitação em todo o mundo.

- Diante da crise de COVID-19, o OCTO desenvolveu a ferramenta de **Coleta de informações e denúncia de ameaças de segurança de nomes de domínio (DNSTICR)** para ajudar a identificar nomes de domínio usados para abusos relacionados à COVID-19 e compartilhar dados com as partes adequadas. O GAC foi atualizado sobre essa questão antes do ICANN68 (12 de junho de 2020) e os membros foram convidados a contribuir para a diversidade linguística da ferramenta.
- Por meio da **plataforma de geração de relatórios de atividades de abuso em domínios (DAAR)**, a ICANN gerou relatórios mensais desde janeiro de 2018 sobre os registros de nomes de domínio e os comportamentos de ameaças de segurança observadas no DNS[12]. Em outubro de 2021, a Organização ICANN e o Grupo de Partes Interessadas de Registros informaram sobre seu acordo em princípio[13] de aproveitar os dados de registro detidos por Registros para fornecer informações no nível de registradores no DAA, conforme reconhecido pelo GAC em uma carta recente à ICANN (21 de fevereiro de 2022).
- O OCTO apoiou o **Grupo de Estudos Técnicos da Iniciativa de Promoção da Segurança no DNS**, lançado em maio de 2020 como parte da implementação do Plano estratégico do AF21-25, para *"explorar ideias sobre o que a ICANN pode e deve fazer para aumentar o nível de colaboração e interação com as partes interessadas do ecossistema do DNS a fim de melhorar o perfil de segurança do DNS"*. O Relatório Final desse grupo (15 de outubro de 2021) foi divulgado após 18 meses de deliberações. A Organização ICANN indicou ao GAC (16 de fevereiro de 2022) que, no momento, está elaborando um plano de ação adequado.

- **No que diz respeito à fiscalização de conformidade contratual**, em uma publicação no blog (20 de abril de 2020), o CEO da ICANN relembrou: "*A equipe de conformidade da ICANN fiscaliza as obrigações contratuais definidas em políticas e contratos da ICANN, incluindo o Contrato de Registro (RA) e o Contrato de Credenciamento de Registradores (RAA). A equipe de conformidade da ICANN também trabalha com o OCTO para identificar ameaças de segurança no DNS [...] e associar essas ameaças às partes contratadas responsáveis. A equipe de conformidade da ICANN utiliza dados coletados em auditorias [...] para avaliar se os registros e registradores estão cumprindo suas obrigações em relação às ameaças de segurança do DNS. Além das auditorias, a equipe de conformidade da ICANN utiliza dados coletados pelo OCTO e outros para interagir de forma proativa com os registros e registradores responsáveis por um número grande de ameaças de segurança no DNS. Quando não é possível resolver o problema por meio de interações construtivas, a equipe de conformidade da ICANN toma medidas em relação às*

[12] Várias partes interessadas e grupos da ICANN comentaram sobre as limitações da DAAR, especificamente uma carta do M3AAWG para a organização ICANN (5 de abril de 2019) e o Relatório Preliminar da equipe de Revisão de SSR2 (24 de janeiro de 2020), que teve o apoio do GAC (veja abaixo). O Grupo de Partes Interessadas de Registros, que também manifestou preocupação, enviou recomendações em uma correspondência para o CTO da ICANN (9 de setembro de 2020).

[13] Veja a carta do RySG para a ICANN (22 de outubro de 2021) e o Blog da ICANN (28 de outubro de 2021)

partes que se recusam a cumprir com as obrigações relacionadas a ameaças de segurança no DNS".

- Após uma **auditoria de conformidade contratual** anterior de operador de registro centrada em abusos na infraestrutura do DNS, concluída em junho de 2019[14], a ICANN relatou (24 de agosto de 2021) sobre os resultados nessa auditoria relacionados a **conformidade de registradores com obrigações relacionadas a abusos do DNS**:
  - 126 registradores foram auditados (responsáveis pela gestão de mais de 90% de todos os domínios registrados em gTLDs)
  - 111 registradores não estavam plenamente em conformidade com os requisitos referentes ao recebimento e à administração de relatórios de abusos do DNS (Seções 3.18.1 – 3.18.3 do RAA)
  - 92 registradores tomaram ações para entrar em plena conformidade, e 19 estão implementando mudanças
- Durante o resumo do CEO da ICANN apresentado ao GAC antes do ICANN73 (16 de fevereiro de 2022), a equipe de Conformidade Contratual da ICANN analisou as obrigações relacionadas a abusos do DNS nos Contratos da ICANN e divulgou o resultado de uma amostra com 3.378 reclamações referentes à consideração dada por registradores a denúncias de abuso, que resultaram em 456 consultas sobre conformidade e 1 aviso de violação.

Recomendações da comunidade para futuras atividades

- **Recomendações da Revisão de SSR2**
  - A Equipe de Revisão de SSR2 apresentou um Relatório Preliminar (24 de janeiro de 2020) com um foco significativo em medidas para prevenir e mitigar abusos do DNS. O comentário do GAC (3 de abril de 2020) endossou muitas das recomendações, inclusive relacionadas a aprimoramentos da DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividades de Abuso em Domínios) e ao fortalecimento de mecanismos de conformidade.
  - O Relatório Final (25 de janeiro de 2021) foi considerado pelo GAC durante o ICANN70 em preparação para o envio de comentários do GAC (8 de abril de 2021), como parte do procedimento de Comentários Públicos.
  - A Diretoria da ICANN tomou algumas medidas (22 de julho de 2021) quanto às 63 recomendações finais da equipe de revisão (25 de janeiro de 2021). Uma postagem no blog da Organização ICANN tem um resumo das ações realizadas:
    - 13 recomendações foram aprovadas (aguardando planejamento para implementação),

[14] Veja no blog da ICANN Contractual Compliance: Addressing Domain Name System (DNS) Infrastructure Abuse [Conformidade contratual: combatendo abusos na infraestrutura do DNS (Sistema de Nomes de Domínio)] (8 de novembro de 2018) e Contractual Compliance Report on Registry Operator Audit for Addressing DNS Security Threats (Relatório de conformidade contratual sobe a auditoria de operadores de registro para combater ameaças à segurança do DNS) (17 de setembro de 2019).

        - 16 recomendações foram rejeitadas (incluindo 6 que não puderam ser aprovadas por completo),
        - 34 recomendações estão aguardando mais informações e análises.
    - No Comunicado do ICANN72 (1º de novembro de 2021), o GAC aconselhou a Diretoria da ICANN a:
        - *Considerar como prioridade as ações de acompanhamento necessárias para ajudar na implementação rápida do scorecard da Diretoria [...] e*
        - *Fornecer mais informações sobre a interpretação divergente da Diretoria e da Equipe de Revisão do SSR2 sobre o nível de implementação de certas recomendações.*
    - A Diretoria da ICANN disponibilizou mais informações em sua resposta (16 de janeiro de 2022)

- **A Equipe de Trabalho sobre abusos do DNS do SSAC (Security and Stability Advisory Committee, Comitê Consultivo de Segurança e Estabilidade)** lançou seu Relatório publicado como o SAC115 (19 de março de 2021), que propõe uma Abordagem Interoperável para Lidar com Abusos no DNS.
    - Em seu relatório, o **SSAC propõe uma estrutura geral de processos e práticas recomendadas** para otimizar a geração de relatórios de abusos no DNS e na Internet em geral, debatendo em particular: ponto principal de responsabilidade para a resolução de abuso, padrão de evidências, caminhos de escalonamento, cronogramas razoáveis para ação e disponibilidade e qualidade das informações de contato.
    - **A principal proposta**, que o SSAC recomenda e que deverá ser analisada e aprimorada pela Comunidade da ICANN em colaboração com toda a comunidade da infraestrutura do DNS, **é a criação de um "facilitador comum para resposta a abusos"**, como uma organização não governamental, sem fins lucrativos e totalmente independente que atuaria como facilitadora para todo o ecossistema do DNS, incluindo as partes contratadas da ICANN, provedores de hospedagem, ISPs (Internet Service Providers, Provedores de Serviços de Internet) e CDNs (Content Delivery Networks, Redes de Fornecimento de Conteúdo) de modo a otimizar a geração de relatórios sobre abusos e minimizar a ocorrência de vitimização.
    - O DNS Abuse Institute informou estar desenvolvendo uma ferramenta centralizada para denúncias de abusos (18 de novembro de 2021)

Principais documentos de referência

- Estudo sobre Abusos do DNS da Comissão Europeia e seu Anexo com informações técnicas (31 de janeiro de 2022)
- Relatório Final da Revisão da SSR2 (25 de janeiro de 2021) e Scorecard de ação da Diretoria (22 de julho de 2021)
- Comunicado e relatório da ICANN (24 de agosto de 2021) da auditoria sobre a conformidade de registradores com as obrigações relacionadas a abusos do DNS
- Relatório do SSAC SAC115 (19 de março de 2021), uma proposta de Abordagem Interoperável para Lidar com Abusos no DNS

Mais informações

Documento de referência de políticas do GAC sobre Mitigação de Abusos do DNS:
https://gac.icann.org/briefing-materials/public/gac-policy-background-dns-abuse-mitigation.pdf

Administração do documento

Título	Sessão de resumo do GAC do ICANN73 – Mitigação de Abusos do DNS
Distribuição	Membros do GAC (antes do encontro) e público (depois do encontro)
Data de distribuição	Versão 1: 24 de fevereiro de 2022