
Mitigação de abusos do DNS

Sessão 3

Índice

Histórico	2
Questões	3
Proposta da liderança para ações do GAC	6
Acontecimentos relevantes	10
Visão geral dos acontecimentos recentes	10
Foco: definição de Abuso do DNS	13
Foco: proteções contra abusos do DNS em Contratos de Registros e Registradores	16
Foco: estrutura não vinculativa para Registros responderem a ameaças à segurança	17
Foco: consideração das recomendações da Revisão de CCT sobre abusos do DNS	19
Foco: discussão sobre o desenvolvimento de políticas da GNSO relacionadas à mitigação de abusos do DNS	21
Foco: DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividade de Abuso de Domínios)	22
Posições atuais	23
Principais documentos de referência	27

Objetivos da sessão

Esta sessão tem como objetivo dar continuidade à consideração pelo GAC das iniciativas da ICANN e da comunidade da ICANN para prevenir e mitigar abusos do DNS, inclusive em resposta às recomendações das equipes de revisão de CCT e SSR2 e discussões que seguiram o Relatório Final do PDP WG da GNSO sobre Procedimentos Subsequentes de Novos gTLDs. Esta sessão também incluirá o seguimento da discussão sobre possíveis propostas concretas do GAC sobre essa questão.

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.). Essas atividades podem ameaçar 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. No entanto, é importante observar que até mesmo a definição exata de “Abuso do DNS” é um assunto que está em debate.

Embora as partes interessadas da Comunidade da ICANN em geral concordem que os abusos do DNS sejam um problema que precisa ser resolvido, existem opiniões diferentes no que diz respeito às responsabilidades das partes relevantes. Por exemplo, registros e registradores estão preocupados em assumir mais obrigações contratuais (o que pode afetar seus modelos de negócios) e argumentam que as ferramentas que usam para mitigar abusos são limitadas e talvez não sejam apropriadas (alguns abusos precisam ser tratados pelos provedores de hospedagem e algumas ações por parte de registros/registratoros talvez resultem em danos colaterais e exposição de responsabilidade).

Algumas atividades de destaque da Comunidade da ICANN para tratar de abusos do DNS até o momento tiveram resultados com diversos níveis de eficiência:

- **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 produziu resultados de políticas e também não realizou uma discussão subsequente sobre [práticas recomendadas não vinculativas](#) para registros e registradores (inclusive workshops durante o [ICANN41](#) e o [ICANN42](#)).
- **Como parte do Programa de Novos gTLDs**, a Organização ICANN adotou uma série de novos requisitos¹ de acordo com seu memorando sobre [Mitigação de Condutas Maliciosas](#) (3 de outubro de 2009). [Relatório da ICANN sobre as Proteções do Programa de Novos gTLDs](#) (18 de julho de 2016) avaliou sua eficiência em preparação para a [Revisão de CCT \(Competition, Consumer Trust and Consumer Choice; Concorrência, Confiança e Escolha do Consumidor\)](#), definida pelo Estatuto, que apresentou suas recomendações em 8 de setembro de 2018.

¹ 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.

- 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 Contrato de Credenciamento de Registradores de 2013**², 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 registros³.
- **Mais recentemente, a Organização ICANN**, por meio do **Gabinete do CTO**, elaborou a [DAAR](#) (Domain Abuse Activity Reporting, Geração de Relatórios de Atividades de Abuso em Domínios) da ICANN, que possibilita a geração de relatórios mensais sobre abusos e o monitoramento de tendências, conforme [informado](#) mais recentemente ao GAC (24 de fevereiro de 2021). O monitoramento e a geração de relatórios de abusos do DNS têm sido apoiados enfaticamente pelo GAC e pelas equipes de revisão, que também recomendaram aprimoramentos. Espera-se que essas ferramentas proporcionem transparência e ajudem identificar as origens de problemas, que então poderão ser resolvidos por meio da conformidade ou, quando necessário, novas políticas corroboradas por informações.

Questões

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 das práticas recomendadas existentes do setor para mitigar abusos do DNS, algumas iniciativas de participação da comunidade lideradas pelo GAC, bem como as equipes de revisão, 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 futuro⁴.

Além disso, preocupações com a capacidade de mitigar de maneira eficiente os abusos do DNS foram ressaltadas nos círculos de agências legais fiscalizadoras, segurança cibernética, proteção do consumidor e proteção intelectual⁵ em decorrência da entrada em vigor do GDPR (General Data Protection Regulation, Regulamento Geral de Proteção de Dados) da União Europeia e os esforços para a alterar o sistema de WHOIS, uma ferramenta essencial na investigação de crimes e abusos, de modo a estar em conformidade com o GDPR. Mais recentemente, a COVID-19, que gerou uma

² Consulte as [Recomendações de Devida Diligência das Agências Legais Fiscalizadoras](#) (outubro de 2019) e as [12 Recomendações das Agências Legais Fiscalizadoras](#) (1º de março de 2012).

³ Essas disposições foram posteriormente complementadas por uma [Estrutura para Operadores de Registro responderem a ameaças à segurança não vinculativa](#) (20 de outubro de 2017) acordada entre a Organização ICANN, os registros e o PSWG do GAC.

⁴ See [GAC comment](#) (19 September 2017) on the Final Report of the [Statistical Analysis of DNS Abuse in gTLDs](#).

⁵ See Section III.2 and IV.2 in the [GAC Barcelona Communiqué](#) (25 October 2018) pointing to surveys of impact on law enforcement in section 5.3.1 of the [Draft Report](#) of the RDS Review Team (31 August 2018) and in a [publication](#) from the Anti-Phishing and Messaging Malware and Mobile Anti-Abuse Working Groups (18 October 2018)

emergência de saúde mundial, representou um exemplo dos desafios existentes à medida que aumentaram os registros de domínios relacionados à pandemia.

Os Comitês Consultivos da ICANN, particularmente o GAC, o SSAC e o ALAC, e diversos terceiros afetados pediram que a Organização ICANN e a Comunidade da ICANN tomassem providências⁶.

⁶ See [DNS Abuse and Consumer Safeguards discussion](#) during the [GDD Summit](#) (7-8 May 2019)

Essas providências exigiriam que a comunidade da ICANN encontrasse algum tipo de consenso sobre várias questões em aberto.

As discussões sobre a mitigação de abusos 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?
- **A detecção e a geração de relatórios de abusos do DNS:** Como podemos garantir que o abusos do DNS sejam detectados e informados às partes interessadas relevantes, inclusive consumidores e usuários da Internet?
- **A prevenção e a mitigação de abusos do DNS:** Que 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.

Proposta da liderança para ações do GAC

1. **Considerar o relatório da Equipe de Trabalho sobre Abusos do DNS** propondo uma [Abordagem Interoperável para Lidar com Abusos no DNS](#) (19 de março de 2021) com o objetivo de avaliar especificamente a criação sugerida 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.
2. **Considerar as deliberações da GNSO até o momento sobre abusos do DNS** tendo em vista as [discussões do Conselho da GNSO/GAC durante o ICANN70](#) e as sérias preocupações já manifestadas pelo GAC quanto à decisão do Grupo de Trabalho da GNSO do Processo de Desenvolvimento de Políticas sobre os Procedimentos Subsequentes de Novos gTLDs de não fazer nenhuma recomendação nessa área.
3. **Deliberar sobre as possíveis próximas etapas**, inclusive por meio de **propostas concretas para melhorar políticas e/ou as disposições contratuais e sua fiscalização**⁷ para administrar questões de políticas públicas relacionadas a abusos do DNS, conforme identificado em diversas contribuições do GAC e atividades da comunidade:
 - a. **As recomendações da Revisão de CCT** de acordo com seu [Relatório Final](#) (8 de setembro de 2018), considerando:
 - A [ação da Diretoria da ICANN](#) (1º de março de 2019) com relação a todas as 35 recomendações, a [adoção](#) subsequente (26 de janeiro de 2020) de um [plano de implementação](#) sugerido para as 6 recomendações que foram aceitas (6 de setembro de 2019) e a [resolução](#) mais recente da Diretoria da ICANN (22 de outubro de 2020) incluindo uma [ação](#) para 11 das 17 recomendações que inicialmente foram classificadas com status pendente, conforme informado por uma [avaliação detalhada](#) da Organização ICANN;
 - Contribuições do GAC em [comentários sobre o relatório preliminar](#) (19 de maio de 2017), [comentários](#) sobre a [análise estatística de abusos do DNS em gTLDs](#) (19 de setembro de 2017), [comentários sobre as recomendações preliminares adicionais](#) (15 de janeiro de 2018), [comentários sobre o Relatório Final da Revisão de CCT](#) (11 de dezembro de 2018) e [comentários sobre o plano de implementação](#) (21 de outubro de 2019);

⁷ Per [GAC ICANN69 Communiqué](#) Section IV.2: “the GAC believes there is now a solid expression of broad support for concrete steps to be taken to address the core components of effective DNS abuse mitigation”; and [ICANN69 GAC Minutes](#): Section 2.2 “Action Points: GAC PSWG to consider developing a concrete proposal regarding DNS Abuse Mitigation steps to prepare GAC for further discussions at ICANN70 (per GAC Wrap up Session discussion).”

- O Conselho do GAC no [Comunicado de Montreal](#) (6 de novembro de 2019) de *não dar prosseguimento a uma nova rodada de gTLDs até após a conclusão da implementação das recomendações da Revisão de Concorrência, Confiança e Escolha do Consumidor identificadas como “pré-requisitos” ou “alta prioridade”*.
 - [Perguntas de esclarecimento da Diretoria](#) (16 de dezembro de 2019) sobre o Conselho do GAC de Montreal, incluindo o tópico da Revisão de CCT e as Rodadas Subsequentes de Novos gTLDs e a definição de “conclusão da implementação”.
 - [Resposta do GAC às perguntas de esclarecimento da Diretoria](#) (22 de janeiro de 2020)
 - [Réplica da Diretoria à resposta do GAC para as perguntas de esclarecimento](#) (11 de fevereiro de 2020) referente à sua [decisão](#) (26 de janeiro de 2020) nem de aceitar ou rejeitar o conselho.
- b. Recomendações da equipe de Revisão de Segurança, Estabilidade e Resiliência (SSR2)** no seu [Relatório Final](#) (25 de janeiro de 2021), sobre as quais o GAC enviou [comentários](#) (8 de abril de 2021) e que deverão ser formalmente consideradas pela Diretoria da ICANN antes de 25 de julho de 2021.
- c. O Grupo de Trabalho da GNSO do Processo de Desenvolvimento de Políticas sobre os Procedimentos Subsequentes de Novos gTLDs** que determinou em seu [Relatório Final](#) (1º de fevereiro de 2021) que *“este Grupo de Trabalho de PDP não fará nenhuma recomendação com relação à mitigação de abusos em nomes de domínio além de declarar que qualquer trabalho futuro relacionado a esse assunto deverá se aplicar a gTLDs novos e existentes (e possivelmente a ccTLDs)”*, apesar das recomendações relevantes sobre abusos do DNS encaminhadas ao grupo pela equipe de Revisão de CCT⁸. O GAC manifestou sérias preocupações com essa decisão nos [comentários do GAC](#) (29 de setembro de 2020) sobre a versão preliminar do Relatório Final desse PDP WG, e sua expectativa de que o Conselho da GNSO tomasse alguma providência quanto a isso.
- d. Implementação e fiscalização de obrigações contratuais importantes** nos contratos de registros e registradores, em particular:
- **A Especificação 11 do Contrato de Registro de Novos gTLDs** e o Conselho de Proteção do GAC relacionado, incluído no [Comunicado de Pequim](#) (11 de abril 2013), considerando as conclusões da [Auditoria de operadores de registro para lidar com ameaças à segurança do DNS](#) (17 de setembro de 2019) e uma discussão no documento de [Perguntas e respostas do GAC/ICANN](#) (30 de maio de 2017), nos [comentários do GAC](#) sobre o Relatório Preliminar de CCT (19 de maio de 2017) e nos [comentários do GAC](#) sobre o Relatório Preliminar de SSR2 (3 de abril de 2020).
 - **A Especificação do Programa de Precisão de WHOIS** do [Contrato de Credenciamento de Registradores de 2013](#), que inclui disposições para a verificação, validação e precisão dos dados de registro de domínios, conforme

⁸ See [Sub Pro PDP WG Final Report](#) Recommendation 9.15 (p. 42) and related [ICANN Board action](#) on the CCT recommendations.

tratado no [comentário do GAC](#) sobre o Relatório Final da Revisão de RDS-WHOIS2 (23 de dezembro de 2019), e o **Contato do Registrador sobre Abuso e Dever de Investigar Relatos de Abuso** (Seção 3.18), que atualmente é objeto de uma [auditoria de conformidade contratual](#) iniciada para 153 registradores selecionados (15 de janeiro de 2021). Esses dois tópicos também foram discutidos no documento de [Perguntas e respostas do GAC/ICANN](#) (30 de maio de 2017) após Conselho do GAC incluído no [Comunicado de Hyderabad](#) (8 de novembro de 2016).

e. Discussões da comunidade sobre abusos do DNS e a eficiência das disposições

contratuais relacionadas, tanto em termos de fiscalização quanto de aplicabilidade:

- **Sessões de encontros da ICANN:** [webinário pré-ICANN66](#) (15 de outubro de 2019), [Sessão do At-Large no ICANN66 sobre preocupações dos usuários finais](#) (3 de novembro de 2019), [Sessão entre comunidades no ICANN66 sobre abusos do DNS](#) (6 de novembro de 2019), a [Sessão do At-Large no ICANN67 sobre conformidade contratual](#) (9 de março de 2020), a [Sessão do ALAC no ICANN68 sobre compromissos de interesse público e o procedimento de resolução de disputas associado](#) (22 de junho de 2020), a [Reunião entre o Conselho da GNSO e a Diretoria no ICANN68](#) que debateu as possíveis próximas etapas para abusos do DNS (14 de junho de 2020) e a [Sessão Plenária no ICANN69 sobre questões relacionadas a abusos do DNS](#)[https://69.schedule.icann.org/meetings/w8wuCYSW5rvL4Yzf3%23/?limit=10&sortByFields\[0\]=isPinned&sortByFields\[1\]=lastActivityAt&sortByOrders\[0\]=-1&sortByOrders\[1\]=-1&uid=a6ijir8iemBHYWRru](https://69.schedule.icann.org/meetings/w8wuCYSW5rvL4Yzf3%23/?limit=10&sortByFields[0]=isPinned&sortByFields[1]=lastActivityAt&sortByOrders[0]=-1&sortByOrders[1]=-1&uid=a6ijir8iemBHYWRru) (20 de outubro de 2020)
- **Correspondência entre a Diretoria da ICANN e os Grupos Constituintes Corporativo e de Propriedade Intelectual** da GNSO, incluindo: a [declaração do BC em relação à discussão da comunidade sobre abusos do DNS](#) (28 de outubro de 2019), uma [carta do BC à Diretoria da ICANN](#) (9 de dezembro de 2019) e a [resposta](#) subsequente (12 de fevereiro de 2020); seguida por uma [carta do IPC à Diretoria da ICANN](#) (24 de abril de 2020).

f. Implementação de medidas antiabuso proativas pelos operadores de ccTLDs que possam embasar as práticas de registro de gTLDs, como as que foram apresentadas pelos ccTLDs .EU e .DK⁹.

g. As recomendações da Revisão do RDS-WHOIS2, conforme detalhadas em seu [Relatório Final](#) (8 de outubro de 2019), que são relevantes para o uso legítimo do WHOIS como uma ferramenta importante para a investigação de crimes e abusos, considerando os [comentários do GAC](#) (23 de dezembro de 2019) e a [ação da Diretoria da ICANN](#) até o momento (25 de fevereiro de 2020).

4. Considerar e continuar o monitoramento do progresso de atividades importantes relacionadas à mitigação de abusos do DNS na Comunidade da ICANN para informar e promover padrões elevados nas práticas e nas obrigações contratuais:

⁹ See in particular a [EURid presentation](#) (28 January 2016) and [.DK presentation](#) during ICANN64 (12 March 2018)

- a. **Implementação de medidas voluntárias por Registros e Registradores de gTLDs**, de acordo com a [Estrutura para Lidar com Abusos](#) liderada pelo setor e a discussão em andamento na Rede de Políticas de Internet e Jurisdição¹⁰.
- b. **Melhorias na Geração de Relatórios de Atividades de Abuso em Domínios (DAAR) da ICANN**, conforme discutido pelos registros com o GAC e o SSAC e o Gabinete do CTO da ICANN¹¹.
- c. Em 27 de março de 2020, a Organização ICANN [executou](#) o [aditamento proposto no Contrato do Registro .COM](#), que **amplia as disposições contratuais para facilitar a detecção e a geração de relatórios de abusos do DNS** (incluindo a [Especificação 11 3b](#)) **para dois terços do espaço de nomes de gTLDs** (até o momento, elas se aplicavam apenas a novos gTLDs). 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.

¹⁰ The Internet and Jurisdiction Policy Network recently [announced](#) (22 February 2021) the launch of a toolkit on DNS Level Action to Address Abuses, which it is planning to present during a conference on Thursday 18 March.

¹¹ See most recently the [RySG DAAR Working Group Report](#) (9 September 2020), a [response](#) by ICANN's CTO (30 September 2020) and the [OCTO update to the GAC](#) (24 February 2021)

Acontecimentos relevantes

Visão geral dos acontecimentos recentes

- **Durante encontros recentes da ICANN**, os líderes do PSWG do GAC fizeram apresentações detalhadas ao GAC sobre a questão de abusos do DNS (consulte o material da [Sessão do GAC no ICANN66](#), as [Sessões do ICANN68](#) e o [Resumo do GAC do ICANN68 sobre abusos do DNS, Atualização do PSWG no ICANN69](#) para o GAC e a [Sessão do ICANN70](#)).
 - O GAC analisou as medidas disponíveis para que os registros e registradores evitem 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 e em potencial para lidar com abusos do DNS de maneira mais eficiente no âmbito da Diretoria da ICANN e da Organização ICANN (consulte a [Ata do ICANN66](#), o [Comunicado do GAC do ICANN68](#) e a [Ata](#), o [Comunicado do ICANN69](#) e a [Ata](#) e o [Comunicado do ICANN70](#) e a [Ata](#)).
 - O [Plano de trabalho do PSWG para 2020/2021](#) inclui todas essas áreas dentro do objetivo estratégico 1, que é desenvolver recursos de redução de abusos do DNS e crimes cibernéticos.
- **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, particularmente as 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), com parte do [procedimento de Comentários Públicos](#).
 - A Diretoria da ICANN agora deverá considerar formalmente o Relatório Final da Revisão de SSR2 antes de 25 de julho de 2021, de maneira consistente com o cronograma de seis meses definido no Estatuto da ICANN.
- **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.
 - Durante o encontro ICANN66, o SSAC informou ao PSWG que estava formando uma Equipe de Trabalho sobre abusos do DNS, com **a participação de um copresidente do PSWG do GAC**.
 - 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 a 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.

- **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 .COM](#), que **amplia as disposições contratuais para facilitar a detecção e a geração de relatórios de abusos do DNS** (incluindo a [Especificação 11 3b](#)) **para dois terços do espaço de nomes de gTLDs** (até o momento, elas se aplicavam apenas a novos gTLDs). 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.
- **No contexto da crise da COVID-19, as partes contratadas apresentaram suas ações e lições aprendidas** [antes](#) e [durante o encontro ICANN68](#) enquanto as partes interessadas do PSWG relataram trabalhos sendo realizados em colaboração com os estados-membros da UE, Europol, ccTLDs e registradores para facilitar denúncias, análises e seu encaminhamento à jurisdição relevante por meio da adoção de um formulário padronizado para denunciar domínios/conteúdos relacionados à COVID-19 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.
- **O PIR (Public Interest Registry, Registro de Interesse Público)**, o operador do registro .ORG e vários novos gTLDs [lançaram](#) (17 de fevereiro de 2021) o **DNS Abuse Institute (Instituto para Abusos do DNS)**, cujo objetivo declarado é *“reunir líderes do espaço antiabuso para: financiar pesquisas, publicar práticas recomendadas, compartilhar dados e fornecer ferramentas para identificar e denunciar abusos do DNS”*. Essa iniciativa foi [apresentada ao PSWG do GAC](#) (3 de março de 2021) antes de um [webinário](#) que foi realizado pelo Instituto sobre o estado de abusos do DNS, em 16 de março de 2021. No [Comunicado do ICANN70](#), o GAC parabenizou o lançamento do Instituto para Abusos do

DNS e “*incentiva[ou] que a comunidade trabalhe de modo colaborativo para lidar com Abusos do DNS de maneira abrangente*”.

- **Resposta multifacetada da organização da ICANN e execução de contratos**

- 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](#).
- **O gabinete do diretor de tecnologia da ICANN (OCTO) 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. O gabinete participa de vários fóruns de inteligência sobre ameaças cibernéticas e resposta a incidentes, incluindo o [Fórum de resposta a incidentes e equipes de segurança](#) (FIRST), o [Grupo de Trabalho Antiabuso de Mensagens, Malware e Dispositivos Móveis](#) (M3AAWG), o [Grupo de Trabalho Anti-phishing](#) (APWG), a [Aliança Nacional Americana de Treinamento e Análises Forenses Cibernéticas](#) (NCFTA) e as recentes Coalizão de Ameaças Cibernéticas (CTC) e Liga de Inteligência (CTI), ambas relacionadas à COVID-19. O gabinete também desenvolve sistemas e ferramentas para ajudar na identificação, análise e denúncia de abusos do DNS:
 - 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 [recebeu informações](#) sobre essa questão antes do ICANN68 (12 de junho de 2020), assim como a Comunidade da ICANN, [durante o encontro ICANN68](#).
 - 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 observados no DNS. A ICANN também monitora tendências por meio dos [Indicadores de integridade das tecnologias de identificadores](#) (ITHI). 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 havia manifestado preocupações em relação à DAAR e estava trabalhando com a ICANN na evolução da ferramenta, recentemente fez recomendações em uma [carta](#) para o CTO da ICANN (9 de setembro de 2020).
- O OCTO da ICANN também apoia o [recém-criado](#) (6 de maio de 2020) **Grupo de Estudos Técnicos da Iniciativa de Promoção da Segurança no DNS**, 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*”. As recomendações são esperadas para maio de 2021.

- 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.
- **Fiscalização de conformidade contratual:** em uma [publicação no blog](#) (20 de abril de 2020), o CEO da ICANN lembrou: *“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 partes que se recusam a cumprir com as obrigações relacionadas a ameaças de segurança no DNS”*. A publicação no blog também dava uma ideia sobre os volumes de denúncias, os recursos alocados ao processamento delas e estatísticas de resolução.

Foco: definição de Abuso do DNS

Conforme destacado 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 interessadas com os impactos nos direitos dos usuários e nas funções básicas das partes contratadas, bem como de que a ICANN ultrapasse seu escopo.¹²

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,

¹² Indeed, the definition of Abuse Mitigation may carry consequences in terms of the scope of activity overseen by ICANN policies and contracts. While governments and other stakeholders are concerned with the impact of DNS abuse on the public interest, including the safety of the public and the infringement of intellectual property rights, registries and registrars are concerned with restrictions on their commercial activities, ability to compete, increased operating costs and liability for consequences registrants may incur when action is taken on abusive domains. Non-commercial stakeholders on their part are concerned with the infringement of freedom of speech and privacy rights of registrants and Internet users, and share with contracted parties concerns about ICANN overstepping its mission.

phishing e botnets, além de spam *“quando usado como um método de entrega de outras formas de abuso”*¹³.

O Departamento de Conformidade Contratual da ICANN referiu-se a **“Abuso da infraestrutura do DNS” e “Ameaças à segurança”** 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”*¹⁴ — e no [Contrato de Credenciamento de Registradores](#) (Seção 3.18), que se refere a *“contatos de abuso”* e *“relatórios de abuso”* sem fornecer uma definição do 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).

Durante um [webinário que antecedeu o ICANN66](#) em 15 de outubro de 2019, **o PSWG e as Partes Contratadas discutiram os assuntos atuais e as práticas do setor**. Em preparação para esse webinário, o Grupo de Partes Interessadas de Registros enviou uma [Carta Aberta](#) (19 de agosto de 2019) apresentando as opiniões de registros sobre a definição de Abusos do DNS, as opções limitadas disponíveis para os registros usarem contra ameaças à segurança e suas preocupações com os [Relatórios de Atividade de Abuso de Domínios](#) da ICANN.

Em resposta, o GAC enviou uma [Declaração sobre Abusos do DNS](#) (18 de setembro), acompanhado pelo [Grupo Constituinte Corporativo](#) (28 de outubro). Em sua declaração, o GAC reconheceu a definição da Equipe de Revisão de CCT de abuso do DNS como *“atividades intencionalmente enganosas, mal-intencionadas ou não solicitadas que usam ativamente o DNS e/ou os procedimentos de registro nomes de domínio”* que, em termos técnicos podem assumir a forma de ameaças de segurança, como *“malware, phishing e botnets, e também spam, quando usado como método de distribuição dessas formas de abuso”*. O GAC reconheceu que o [Contrato de Registro de Novos gTLDs](#) reflete essa ideia na [Especificação 11](#), especialmente nas seções 3a¹⁵ e 3b¹⁶.

¹³ See p.88 of the [CCT Review Final Report](#) (8 September 2018) as highlighted more recently in the [GAC Statement on DNS Abuse](#) (18 September 2019)

¹⁴ The [Advisory, New gTLD Registry Agreement Specification 11 \(3\)\(b\)](#) (8 June 2017) provides a definition of ‘Security Threats’ as including *“pharming, phishing, malware, botnets, and other types of security threats.”*

¹⁵ Specification 11 3a provides that *“Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.”*

¹⁶ Specification 11 3b provides that *“Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.”*

Depois da publicação da [Declaração do GAC sobre abusos do DNS](#) (18 de setembro de 2019), um grupo de **grandes registros e registradores de gTLDs propôs uma estrutura voluntária para reduzir os abusos** (17 de outubro de 2019). Especificamente, essa estrutura inclui na cobertura de possíveis medidas pelos adotantes certas formas de “abuso de conteúdos de sites”, consideradas “tão graves que a parte contratada deve tomar medidas diante de uma notificação específica e confiável”. Depois da publicação e discussão durante o ICANN66, a [lista de signatários](#) dessa estrutura aumentou, incluindo outros grandes registradores e registros, além de pequenos provedores desse tipo de serviço.

Em 18 de junho de 2020, os presidentes dos **Grupos de Partes Interessadas de Registros e Registradores** (coletivamente chamados de Casa das Partes Contratadas da GNSO ou CPH) informaram aos líderes da Comunidade que **adotaram uma definição de abuso do DNS**, refletindo exatamente aquela da estrutura criada pelo setor para reduzir os abusos:

O abuso do DNS é composto por cinco categorias mais amplas de atividades nocivas na medida em que se relacionam ao DNS: malware, botnets, phishing, pharming e spam como mecanismo de distribuição de outras formas de abuso do DNS [fazendo referência ao documento de [abordagens operacionais, normas, critérios e mecanismos](#) da Rede de Políticas de Internet e Jurisdição para a definição de cada uma dessas atividades].

Essa definição **parece confirmar o que a Equipe de Revisão de CCT chamou de consenso existente em relação ao “Abuso de segurança do DNS ou Abuso de segurança do DNS na infraestrutura do DNS”** ([Relatório Final de CCT](#) pág. 8.) e **concorda com a definição ilustrativa do GAC de “ameaças de segurança”** nas ‘verificações de segurança’ do Conselho de Proteção do GAC válidas para todos os novos gTLDs no [Comunicado de Pequim](#) (11 de abril de 2013), incorporadas ao Contrato de Registro de gTLDs na [Especificação 11](#) 3.b.

Foco: 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 de disposições alinhadas ao Conselho de Proteções do GAC incluído no [Comunicado de Pequim](#) (11 de abril de 2013), de maneira consistente com a [Proposta da Diretoria da ICANN de Implementação de Proteções do GAC Aplicáveis a Todos os Novos gTLDs](#) (19 de junho de 2013)

Após os primeiros anos de operação dos novos gTLDs, durante o ICANN57 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, Contrato de Registro de Novos gTLDs, Especificação 11 \(3\)\(b\)](#) 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](#)<https://newgtlds.icann.org/sites/default/files/agreements/agreement-approved-31jul17-en.html%23specification11>. **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”*¹⁷. Pouco tempo depois, em novembro de 2018, uma [Auditoria sobre Abusos na Infraestrutura do DNS](#) de quase **todos os**

¹⁷ As reported in the blog post of 8 November 2018, Contractual Compliance: Addressing DNS Infrastructure Abuse: <https://www.icann.org/news/blog/contractual-compliance-addressing-domain-name-system-dns-infrastructure-abuse>

registros de 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”*. Em seu [relatório](#) dessa auditoria (17 de setembro de 2019), a ICANN concluiu que:

- a grande maioria dos operadores de registro está comprometida em resolver as ameaças à segurança do DNS.
- A maior parte das ameaças à segurança do DNS está concentrada em um número relativamente pequeno de operadores de registro.
- Alguns Operadores de Registro interpretam o texto contratual da Especificação 11 3(b) de maneira a dificultar o julgamento sobre se as iniciativas deles para mitigar as ameaças à segurança do DNS estão em conformidade e são eficazes.

Em janeiro de 2021, a equipe de Conformidade Contratual da ICANN [iniciou](#) uma auditoria para avaliar a **conformidade de registradores com suas obrigações relacionadas a ameaças à segurança do DNS**. Após colaborar com o Grupo de Partes Interessadas de Registradores no desenvolvimento de uma Solicitação de Informações (incluindo a documentação relacionada a como os registradores podem lidar com domínios potencialmente abusivos), a equipe de Conformidade Contratual da ICANN incluiu na auditoria 127 registradores que tinham pelos menos 5 nomes de domínio presentes em relatórios de ameaças de segurança fornecidos por registros em uma auditoria anterior, ou no relatório de abusos de novembro de 2020 montado pelo Gabinete do CTO da ICANN. Durante uma [atualização da equipe de conformidade que antecedeu o ICANN70](#), a Organização ICANN indicou que deverá publicar um relatório sobre essa auditoria no início de junho de 2021.

Foco: 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 ICANN [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”*.

De acordo com sua recomendação 19, a [Equipe de Revisão de CCT](#) deferiu a tarefa de realizar uma avaliação da eficiência da Estrutura para uma revisão subsequente¹⁸, uma vez que a Estrutura não existia há tempo suficiente para avaliar sua eficiência.

¹⁸ CCT Review recommendation 19: *The next CCT should review the "Framework for Registry Operator to Respond to Security Threats" and assess whether the framework is a sufficiently clear and effective mechanism to mitigate abuse by providing for systemic and specified actions in response to security threats*

Foco: consideração das recomendações da Revisão de CCT sobre abusos do DNS

Com base em sua [análise do cenário de Abusos do DNS](#),¹⁹ incluindo a consideração do [Relatório da ICANN sobre as Proteções do Programa de Novos gTLDs](#) (15 de março de 2016) e a [Análise Estatística Independente sobre Abusos do DNS](#) (9 de agosto de 2017), a Equipe de Revisão de CCT [recomendou](#), com relação a Abusos do 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”*²⁰.

Tendo em vista o [Conselho](#) no [Comunicado do GAC de Montreal](#) (6 de novembro de 2019) de que a Diretoria da ICANN *“não faça uma nova rodada de gTLDs antes de concluir a implementação das recomendações [...] identificadas como ‘pré-requisitos’ ou de ‘alta prioridade’”*, e da [resposta da Diretoria](#) a esse conselho (26 de janeiro de 2020), o PSWG continua monitorando a consideração das principais [recomendações da Equipe de Revisão de CCT](#) (6 de setembro de 2018) voltadas para a adoção de cláusulas contratuais para incentivar medidas proativas antiabuso (Rec. 14) e para evitar o uso sistêmico de registradores ou registros para abuso do DNS (Rec. 15); o aprimoramento das pesquisas sobre abuso do DNS (Rec. 16); o aprimoramento da precisão do WHOIS (Rec. 18); e a eficácia do processamento de denúncias de conformidade contratual (Rec. 20).

O PSWG do GAC também está considerando a resolução da Diretoria de continuar com o [plano de implementação](#) da ICANN (23 de agosto de 2019) para recomendações de CCT aceitas no [Scorecard de ações da Diretoria da ICANN](#) (1º de março de 2019). O GAC [comentou](#) (21 de outubro de 2019) sobre esse plano e destacou alguns pontos problemáticos com relação às importantes recomendações de combater abusos do DNS, incluindo a publicação da cadeia de partes responsáveis pelos registros de nomes de domínio de gTLDs (Rec. 17), informações mais detalhadas sobre denúncias de conformidade contratual (Rec. 21), medidas de segurança proporcionais à oferta de serviços que envolvem a coleta de informações confidenciais de saúde e financeiras (Rec. 22).

Depois da adoção pelas partes contratadas de uma definição de abuso do DNS, o **GAC pediu esclarecimentos à Diretoria da ICANN durante o ICANN68** (veja o [material das reuniões do GAC](#)

¹⁹ See Section 9 on Safeguards (p.88) in the [CCT Review Final Report](#) (8 September 2018)

²⁰ See p.5 of scorecard of [Board Action on the Final CCT Recommendations](#)

[com a Diretoria](#) em 24 de junho de 2020), em relação à implementação da Rec. 14 da CCT-RT (a ICANN deveria negociar cláusulas contratuais para fornecer incentivos financeiros às partes contratadas para a adoção de medidas proativas antiabuso), perguntando o status e o planejamento para a condução de iniciativas da comunidade para desenvolver uma definição de “abuso” e embasar outras ações da Diretoria em relação a essa recomendação. O GAC registrou em sua [Ata do ICANN68](#) que “a Diretoria continuará promovendo o diálogo da comunidade como já vem fazendo, conduzindo discussões regionais e entre comunidades, fazendo pesquisas e desenvolvendo ferramentas para ajudar a embasar os debates da comunidade, além de enviar palestrantes quando solicitado”.

Durante o encontro ICANN68, o PSWG observou com as partes interessadas do ALAC que o progresso na implementação da recomendação da CCT-RT aceita e a consideração das recomendações pendentes não estão claros. Também ficou clara a insatisfação com um recente [comunicado](#) (29 de abril de 2020) do **Grupo de Trabalho do Processo de Desenvolvimento de Políticas da GNSO para Procedimentos Subsequentes de Novos gTLDs**, dizendo que “não planeja fazer recomendações em relação à redução do abuso de nomes de domínio, apenas dizer que tais iniciativas devem ser aplicadas tanto aos gTLDs existentes quanto aos novos (e possivelmente aos ccTLDs)”. Essa afirmação é independente das recomendações relevantes endereçadas ao grupo pela Equipe de Revisão de CCT, também apoiada pela Ação da Diretoria da ICANN sobre essas recomendações, bem como o [Conselho do Comunicado do GAC de Montreal](#) (6 de novembro de 2019) e outros pareceres do GAC, conforme registrado no [Comunicado do GAC do ICANN67](#) (16 de março de 2020).

Em seu [Relatório Final](#) (1º de fevereiro de 2021), o Grupo de Trabalho do Processo de Desenvolvimento de Políticas da GNSO para Procedimentos Subsequentes de Novos gTLDs confirmou sua decisão²¹. O GAC manifestou sérias preocupações quanto a isso nos [comentários do GAC](#) (29 de setembro de 2020) sobre a versão preliminar do Relatório Final desse PDP WG, e sua expectativa de que o Conselho da GNSO tomasse alguma providência.

²¹ See [Sub Pro PDP WG Final Report](#) Recommendation 9.15 (p. 42)

Foco: discussão sobre o desenvolvimento de políticas da GNSO relacionadas à mitigação de abusos do DNS

Após a decisão inicial do Grupo de Trabalho do PDP de Procedimentos Subsequentes de Novos gTLDs de não fazer recomendações em relação à área de abusos do DNS para futuros contratos de novos gTLDs, o **Conselho da GNSO discutiu** em uma [reunião](#) realizada em 21 de março de 2020 a **possibilidade de iniciar um Grupo de Trabalho Entre Comunidades (CCWG)** sobre questões relacionadas a abusos do DNS e possivelmente um subsequente PDP da GNSO, caso fossem necessários novos requisitos contratuais.

O Conselho não abordou uma proposta informal feita pela [liderança do GAC](#) (12 de maio de 2020) para considerar uma discussão de afinidades entre especialistas relevantes, inclusive operadores de ccTLDs, a fim de estabelecer um escopo para qualquer iniciativa futura de política.

Até 20 de maio de 2021, essa questão ainda está identificada como “não planejada” no [Radar de decisões e ações do Conselho da GNSO](#), sendo que o Conselho da GNSO “*determinará as próximas etapas, se for o caso, sobre abusos do DNS*”.

Desde o ICANN70 e a [conferência com a liderança do GAC/GNSO que antecedeu o ICANN70](#) (8 de março de 2021) e a [reunião do GAC com a GNSO no ICANN70](#) (24 de março de 2021), o Conselho da GNSO discutiu as informações que recebeu sobre a questão de abusos do DNS durante sua reunião mensal recente:

- Em [22 de abril de 2021](#), o **grupo dedicado a abusos do DNS da Casa de Partes Contratadas da GNSO** revisou diversas iniciativas realizadas pelas Partes Contratadas nos últimos anos e sobre as quais o GAC já foi informado pelo seu PSWG. Com relação ao trabalho já em andamento e os futuros, várias iniciativas foram mencionadas:
 - Colaboração com o PSWG do GAC para lidar com malware e botnets em escala
 - Consideração por registradores de programas de incentivo
 - Iniciativas de divulgação para outros grupos constituintes da ICANN, incluindo uma sessão de perguntas e respostas, uma pesquisa na Comunidade e outros recursos informativos
- Em [20 de maio de 2021](#), o Conselho da GNSO recebeu um [resumo](#) dos líderes do SSAC sobre o Relatório SAC115 lançado recentemente que propõe uma [Abordagem Interoperável para Lidar com Abusos no DNS](#) (19 de março de 2021). Durante essa reunião, o Conselho da GNSO não realizou uma discussão para tratar do SAC115 ou das próximas etapas em geral para lidar com abusos do DNS.

Foco: 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).²²

A [finalidade](#) 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 incluindo informações de um [conjunto enorme de feeds de dados de ameaças à segurança e reputação de alta confiança](#).²³

Dessa forma, a 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 M3AAWG²⁴ 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.

Recentemente, os registros relataram em uma [Carta Aberta](#) (19 de agosto de 2019) uma interação com Escritório do CTO da ICANN *“para analisar o DAAR com o objetivo de recomendar aprimoramentos ao Escritório do CTO a fim de garantir que o DAAR atenda melhor sua finalidade intencionada e fornecer à comunidade da ICANN um recurso valioso”*. Embora os registros reconheçam que *“alguns membros da comunidade possam depender dos dados fornecidos pela Geração de Relatórios de Atividade de Abuso de Domínios da ICANN (DAAR) para corroborar alegações de Abusos do DNS sistêmicos ou amplos”*, eles acreditam que *“a ferramenta tem limitações significativas, não é capaz de assegurar evidências de relatórios precisas e confiáveis de ameaças à segurança e ainda não atende aos seus objetivos”*.

O Grupo de Partes Interessadas de Registros detalhou o trabalho que realizou em seu [Relatório do Grupo de Trabalho de DAAR](#) (9 de setembro de 2020), ao qual o CTO da ICANN enviou a seguinte [resposta](#) (30 de setembro de 2020): *“a maioria das recomendações na carta enfatiza o aprimoramento da comunicação sobre os dados exportados do sistema DAAR, uma vez que essa comunicação é considerada pelo Grupo de Trabalho como potencialmente incerta, tanto no que diz respeito à atual documentação de metodologia do DAAR quanto ao que consta nos relatórios mensais do DAAR. Embora a maior parte das recomendações se concentre em mudanças específicas no relatório, algumas delas (como a recomendação 3, que pede que seja calculada a*

²² See cross-community sessions led by the GAC PSWG during [ICANN57](#) (Nov. 2016), [ICANN58](#) (March 2017) and [ICANN60](#) (October 2017), as well as questions to the ICANN Board regarding the effectiveness of DNS Abuse Safeguards in [Hyderabad Communiqué](#) (8 November 2016), follow-up questions in the [GAC Copenhagen Communiqué](#) (15 March 2017) and a set of [draft responses](#) (30 May 2017) by ICANN org.

²³ For more information, see <https://www.icann.org/octo-ssr/daar-faqs>

²⁴ Messaging, Malware and Mobile Anti-Abuse Working Group

‘persistência’ da atividade abusiva relatada) podem exigir investigações e análises em longo prazo.”

Durante a [atualização do OCTO ao GAC](#) (24 de fevereiro de 2021), o CTO da ICANN discutiu os planos futuros para o desenvolvimento do DAAR: adicionar mais ccTLDs ao escopo do DAAR, continuar trabalhando com o Grupos de Trabalho de DAAR do RySG e explorar soluções para superar desafios relacionados ao acesso aos dados de WHOIS para elaborar métricas para os registradores, como consultas diárias ao WHOIS apenas para domínios na lista de bloqueio, amostragem aleatória de domínios ou aprovação obrigatória para usar dados de BRDA (Bulk Registration Data Access, Acesso a Dados de Registro em Lote).

Posições atuais

As posições atuais do GAC são listadas abaixo, em ordem cronológica inversa:

- [Comentários do GAC](#) (8 de abril de 2021) sobre o Relatório Final da Equipe de Revisão de SSR2 para serem considerados pela Diretoria da ICANN
- [Comunicado do GAC do ICANN70](#) (25 de março de 2021) observando que *“Abusos do DNS devem ser administrados em colaboração com a comunidade da ICANN e a Organização ICANN antes do lançamento de uma segunda rodada de novos gTLDs. O GAC apoia o desenvolvimento de disposições contratuais propostas aplicáveis a todos os gTLDs com o objetivo de melhorar as respostas a Abusos do DNS. O GAC também enfatizou a importância de definir medidas para garantir que os Registros, Registradores e provedores de Serviços de Privacidade/Proxy estejam em conformidade com as disposições contratuais firmadas com a ICANN, inclusive as auditorias. O GAC parabeniza o lançamento recente do DNS Abuse Institute (Instituto para Abusos do DNS) e incentiva que a comunidade trabalhe de modo colaborativo para lidar com Abusos do DNS de maneira abrangente.”*
- [Comunicado do GAC do ICANN69](#) (23 de outubro de 2020) ressaltando a opinião do GAC de que *“existe agora um apoio amplo para que sejam tomadas medidas concretas para lidar com os componentes principais da mitigação eficaz de abusos do DNS”,* tendo em vista a visibilidade do assunto e o diálogo construtivo na Comunidade da ICANN (veja a Seção IV.2 pág. 6).
- [Comunicado do GAC do ICANN68](#) (27 de junho de 2020) destacando que *“novos esforços para lidar com abusos do DNS não devem substituir, mas sim complementar, as iniciativas existentes para melhorar a precisão dos dados de registro, como o Sistema de Relatórios de Precisão, e para implementar políticas sobre serviços de privacidade e proxy, que no momento estão paradas”* (veja a Seção IV.3 pág. 7).
- [Comentário do GAC](#) (3 de abril de 2020) sobre a Versão Preliminar do Relatório da Equipe de Revisão do SSR2
- [Comentário do GAC](#) sobre as recomendações finais da Revisão do RDS-WHOIS2 (23 de dezembro de 2019).
- [Declaração do GAC sobre o DNS](#) (18 de setembro de 2019)

- [Comentários do GAC](#) sobre o Relatório Final da Equipe de Revisão de CCT (11 de dezembro de 2018)
- [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)
- [Comentário do GAC](#) sobre a Análise Estatística de Abusos do DNS em gTLDs (19 de setembro de 2017)
- [Comentário do GAC](#) sobre o Relatório de Proteções do Programa de Novos gTLDs contra Abusos do DNS (21 de maio de 2016)
- [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)
- [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 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)
- [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 Dakar](#) (27 de outubro de 2011) seção III. Recomendações de LEAs (Law Enforcement Agencies, Agências Legais Fiscalizadoras)
- [Comunicado do GAC de Nairóbi](#) (10 de março de 2010) seção VI. Recomendações de devida diligência das agências legais fiscalizadoras
- [Recomendações de LEAs sobre Aditamentos aos Contratos de Registros](#) (1º de março de 2012)
- [Recomendações de Devida Diligência das Agências Legais Fiscalizadoras](#) (outubro de 2009)

Perguntas para serem consideradas pelos representantes do GAC

Em preparação para esta e outras sessões do GAC no ICANN71 e em encontros futuros, foi considerado que os representantes do GAC seriam beneficiados com uma discussão mais detalhada sobre os diversos tópicos da ICANN em seus próprios governos ou organizações. Listadas abaixo, como uma experiência para o ICANN71, a equipe da Organização ICANN elaborou de maneira colaborativa algumas perguntas para serem consideradas pelos representantes do GAC como parte da preparação e do compartilhamento de informações para a sessão, de modo a ajudar nas discussões, compartilhar práticas recomendadas e possivelmente identificar diversas abordagens ou estratégias que os diferentes governos assumem para essas questões. As perguntas abaixo podem ser usadas pelos leitores para se preparar ou como uma forma de ampliar o diálogo

em encontros futuros. Informe à equipe de apoio do GAC se você considera esses tipos de perguntas interessantes na preparação para encontros.

Com relação à fiscalização de conformidade das disposições de abuso incluídas nos Contratos de Credenciamento de Registros e Registradores:

- O seu governo tem uma definição para abuso do DNS? Se sim, qual é essa definição?
- As autoridades públicas no seu país já encontraram nomes de domínio que parecem ser usados para perpetrar abusos do DNS e os denunciaram para o registro ou registrador relevante? Se sim, dos nomes de domínio de gTLDs denunciados ao registro ou ao registrador, quantos foram encaminhados para a equipe de Conformidade da ICANN devido a falhas de Partes Contratadas de lidar adequadamente com a denúncia de maneira razoável e em tempo hábil?
- Quantos desse nomes que parecem ser usados para perpetrar abusos do DNS estão registrados em gTLDs, em comparação aos registrados em ccTLDs?
- As autoridades públicas do seu país já revisaram as diretrizes publicadas pelo Grupo de Partes Interessadas de Registradores, que fornece informações que talvez sejam úteis ao registrar reclamações de abuso com os registradores?
- As autoridades públicas do seu país conhecem as disposições incluídas no RA (Registry Agreement, Contrato de Registrados) e no RAA (Registrar Accreditation Agreement, Contrato de Credenciamento de Registradores) que são executáveis e fiscalizadas pela ICANN? (Particularmente, a Especificação 11 3a e 3b do RA, e a 3.18 do RAA)
- Que autoridade fiscalizadora e mecanismos as autoridades públicas do seu país acreditam que a ICANN tem que sejam relacionados a domínios abusivos?

Com relação ao trabalho da Organização ICANN para detectar e relatar ameaças à segurança:

- O DAAR (Domain Abuse Activity Reporting, Geração de Relatórios de Atividades de Abuso em Domínios) da ICANN tem como objetivo dar à Comunidade da ICANN dados baseados em fatos, confiáveis, persistentes e imparciais usando uma metodologia aberta e verificada pela comunidade que pode ser usada para ajudar a informar as discussões sobre políticas. Que melhorias o seu governo ou as autoridades públicas relevantes sugerem que sejam feitas no DAAR?
- Que melhorias o seu governo ou as autoridades públicas relevantes sugerem que sejam feitas na ferramenta de Coleta de informações e denúncia de ameaças de segurança de nomes de domínio (DNSTICR) da ICANN, que tem como objetivo identificar atividades de malware e phishing relacionadas à COVID-19?
- O seu governo está ciente das descobertas feitas por essa iniciativa até o momento, particularmente de que algumas dezenas de evidências de problemas que precisavam ser relatados a Partes Contratadas foram encontrados?

Com relação ao trabalho da ICANN de apoiar a mitigação de ameaças à segurança do DNS:

- O seu governo acredita que é apropriado para a ICANN se concentrar em apoiar a mitigação de ameaças à segurança do DNS em gTLDs, conforme definido pelo GAC (phishing, malware, botnets de comando e controle e pharming, além de spam quando usado como um vetor para disseminar outros tipos de ameaças à segurança), tendo em vista a proibição no Estatuto da ICANN da regulação de conteúdo e a ausência de jurisdição sobre ccTLDs?
- O seu governo tem alguma sugestão para contribuir na deliberação em andamento da comunidade da ICANN para definir o problema e determinar a melhor forma de avançar com relação à mitigação de abusos do DNS, seja na criação de práticas recomendadas voluntárias, ou seja em uma política de consenso, ou seja ainda em uma combinação dessas opções?
- Que dados objetivos e baseados em fatos o seu governo acredita que a ICANN possa fornecer para facilitar essas discussões da comunidade?

Principais documentos de referência

- Documento do GAC sobre Abusos do DNS
 - [Sessão do GAC no ICANN70 sobre abusos do DNS](#) (23 de março de 2020)
 - [Documento do GAC sobre abusos do DNS no ICANN68](#) (18 de junho de 2020)
 - [Perguntas do GAC sobre a Mitigação de Abusos e Respostas Preliminares da ICANN](#) (30 de maio de 2017) conforme o Conselho no [Comunicado do GAC de Hyderabad](#) (8 de novembro de 2016) e Acompanhamento no [Comunicado do GAC de Copenhague](#) (15 de março de 2017)
- Definição de Abuso do DNS (incluindo a perspectiva de partes interessadas do setor)
 - [Definição de partes contratadas para Abuso do DNS](#) (outubro de 2020)
 - [Estrutura para Lidar com Abusos](#) (17 de outubro de 2019)
 - [Declaração do GAC sobre o DNS](#) (18 de setembro de 2019)
- [Relatório Final](#) da Revisão de SSR2 (25 de janeiro de 2021)
- Segunda revisão do RDS-WHOIS
 - [Scorecard de ações da Diretoria da ICANN](#) (25 de fevereiro de 2020) sobre as recomendações finais da Revisão do RDS-WHOIS2
 - [Recomendações finais da Revisão do RDS-WHOIS2](#) (3 de setembro de 2019)
- Revisão de Concorrência, Confiança e Escolha do Consumidor
 - [Scorecard de ações da Diretoria da ICANN](#) (22 de outubro de 2020) sobre 11 das 17 recomendações da CCT pendentes e a [avaliação detalhada](#) associada fornecida pela Organização ICANN
 - [Scorecard de Ação da Diretoria da ICANN](#) sobre as Recomendações Finais da Revisão de CCT (1º de março de 2019)
 - [Recomendações e Relatório Final da Revisão de CCT](#) (8 de setembro de 2018), em particular a Seção 9 sobre Proteções (pág. 88)
 - [Análise Estatística de Abusos do DNS em gTLDs](#) (9 de agosto de 2017)

Administração do documento

Encontro	Fórum Virtual de Políticas ICANN71, de 14 a 17 de junho de 2021
Título	Resumo do GAC do ICANN71 – Sessão 3 – Mitigação de Abusos do DNS
Distribuição	Membros do GAC (antes do encontro) e público (depois do encontro)
Data de distribuição	Versão 1: 1º de junho de 2021