ICANN84 | Assembleia Geral Anual – Discussão do GAC sobre atenuação do abuso de DNS
Terça-feira, 28 de outubro de 2025 – 13h15 às 14h30 IST

JULIA CHARVOLEN

Bem-vindos a Sessão do GAC do GAC para o Uso Indevido do DNS. Segunda-feira, 28 de outubro, 13h00 UTC. Esta sessão está sendo gravada e se rege pelos Padrões de Comportamentos Esperados do ICANN e Código de Conduta da ICANN e a Política Antiassédio da ICANN.

Durante a sessão, as perguntas e os comentários serão lidos em voz alta, se forem formatados como correspondem no chat do Zoom. Nesta sessão, há interpretação nos seis idiomas das Nações Unidas e o português. Se quiserem falar durante a sessão, levantem a mão na sala do Zoom. Digam o seu nome para os registros e o idioma, que vai utilizar, caso não seja inglês. Por favor, falem a uma velocidade razoável para permitir uma interpretação correta.

E agora, passo a palavra ao Presidente do GAC.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

Obrigado, Julia. Sejam todos bem-vindos. Espero que todos tenham aproveitado o almoço nesta linda cidade de Dublin. Eu tenho agora o prazer de apresentar nossos oradores convidados. Está Edmon Chung, de DotAsia e Jo-Fan Yu. Espero ter pronunciado

bem o sobrenome, de TWNIC. E quem não está vendo, o Sr. McDermott.. Eu penso que vai chegar daqui a pouco. Muito obrigado. Sejam bem-vindos, já falei. Se vão preparando, não tem pressa. E os temas preparados pelo GAC, como é o uso indevido do DNS, o abuso do DNS. Vemos que Susan Chalmers, dos Estados Unidos e Mr. Tomo Miyamoto do Japão. Então, mais uma vez, e Martina Barbero, da Comissão Europeia. Primeiro, Tomo, vai assumir a palavra e vai guiar um pouco, dando uma introdução e lembrar quais são os objetivos e de que forma estão vinculados com o projeto, a agenda anual do GAC. Então, por favor, Tomo. Estão em uso da palavra.

TOMONORI MIYAMOTO Obrigado, Sr. Presidente. Sejam bem-vindos à Sessão de Mitigação do Abuso do DNS. Sou Tomonori Miyamoto, do Japão.

E esta é a agenda para hoje. Em primeiro lugar, vamos fazer uma introdução do meu cargo. Depois vamos escutar uma apresentação do País Anfitrião, que tem a ver com o que será, o que falará o Declan McDermott, Chefe dos Assuntos Legais do IE. Também vamos escutar e ver quais os avanços, quanto ao tema do uso indevido, o abuso do DNS e as políticas, também que vão ser apresentadas por Jorge Cancio e outras apresentações de outros membros.

Vou começar com os antecedentes. Os senhores e as senhoras sabem que o abuso do DNS é muito importante para o GAC. Muitos dos colegas que estão aqui estão familiarizados com os programas

implementados em cada um dos seus países. Isso também é um assunto importante para as partes interessadas, porque já vimos na ICANN. Porque há muitas sessões, que estão vinculadas com a questão do uso indevido, o abuso do DNS. Com base no contrato com a ICANN, o RA e RAA, modificados ano passado, em 2024, que são os registros e registradores de gTLDs, que devem apresentar relatórios sobre o uso indevido ou o abuso do DNS.

O que precisamos marcar é que o abuso do DNS, dentro da definição da ICANN, está limitado a *malware, botnets, phishing, pharming e spying*. Bem como os mecanismos de entrega. Muitos países têm diferentes assuntos, quanto a esse abuso. Pode existir fraude também. Estão envolvidas as autoridades de aplicação da lei. No Japão, por exemplo, esta questão do *malware* também é um grande problema. E também, como temos.... o que falamos para a Próxima Rodada, temos que levar em conta este assunto. E também qual é a definição da ICANN sobre o abuso do DNS.

O prazo, no qual queremos implementar uma nova política, que é antes da delegação dos novos gTLDs. No segundo lugar, também temos que gerar capacidades para mitigação do abuso do DNS e compartilhar as melhores práticas, que podem ajudar outros nas iniciativas voluntárias, que estejam desenvolvendo em cada um dos seus comitês. Então, há diferentes tipos de programas de uso indivíduo do DNS. Seguinte slide.

Alguns de vocês talvez lembrem deste gráfico. Porque aqui vemos qual é o panorama das comunidades, onde está o alcance do

contrato da ICANN, que é bastante limitado, como já falei. Há uma definição também. E essa definição tem a ver com a relação entre a ICANN e a parte contratada. Agora, aqui temos vinculação contratuais. Isso é bastante importante. A questão é implementar medidas adequadas de forma oportuna antes da delegação dos novos gTLDs.

Claro que precisamos considerar também, o que temos dentro de uma comunidade mais ampla, onde estão os registros, registradores e os operadores desses gTLDs, e a cooperação com os outros parceiros. Seguinte slide. Seguinte. Obrigado.

Aqui também vemos o passado, como chegamos até a discussão atual do PDP. Isso está dentro do mandato da ICANN e da sua incumbência para implementar as políticas. Tivemos que ver quais eram os alcances dos PDPs e alguns elementos importantes. Em novembro de 2024, acho que muitos de nós lembramos o que era o relatório informal. Sim, o estudo informal, onde foram sugeridos alguns fatores que são os que estimulam o uso indevido ou o abuso, como pode ser a API de conexão livre e alguns fatores negativos, que era a verificação adicional e a informação de contato.

Em maio deste ano, NetBeacon emitiu um documento, o que nós chamamos de Livro Branco, onde foram apresentados os PDPs e se falou de cinco elementos para controlar o abuso de DNS. Nós, aqui no GAC, debatemos esses pontos. E agora estamos falando dos PDPs sobre mitigação do abuso de DNS, que começou na reunião

passada da ICANN83. O que eles receberam como pedido é fazer as modificações necessárias, para começar esse processo de políticas com alcance um pouco mais limitado.

Agora vamos apresentar o país anfitrião e damos as boas-vindas a Declan McDermott, que está cargo da administração de ccTLDs no .IE.

DECLAN MCDERMOTT Sejam todos e todas bem-vindos. Eu sou Chefe do Relatório de ccTLDs do .IE e eu sou da parte de política. Eu não sou técnico, então não vai ser uma apresentação técnica, a minha. Se tiverem perguntas técnicas sobre como mitigar o abuso, eu peço que mitiguem as suas expectativas, quanto ao que eu posso dizer. Mas, se tem alguma pergunta para mim, podem realizar nos corredores. E se eu não tenho a resposta, eu procurarei. Muito bem.

O .IE. Então, é gerenciado o registro do .IE. Desde 2000, maneja todo o domínio que tem a ver com IE. Então, fizemos já 25 anos, há um mês. E eu quero destacar que temos um baixo volume e baixa capacidade e taxas de usos indevidos ou de abusos. Há registrações de nomes de domínio, que são, como 300.000. A maioria são pessoas humanas, são físicas. NetBeacon, eu acho que publicou uma imagem de como eram os números de uso indevido ou abuso do .IE. E tem informação completa até agosto que encontraram um caso detectado de *phishing*, se não estou errado.

Então, digamos que a taxa de abuso é bastante baixa ou baixo, o volume também. E aí, a Federação de Investigação da Internet

marcou, que chegamos a 0,05 de abuso. E nos últimos 365 dias, eu acho que passou para 100 instâncias detectadas. Então, o que eu quero dizer com isso é que, se bem o registro é pequeno, comparado com outros. E também tem uma baixa taxa de uso indevido ou abuso. E eu acho que é o que acontece geralmente entre os ccTLDs.

O .IE também tem um requisito específico, que chamamos *Connection to Ireland*, ou Conexão a Irlanda. Desde a sua criação de nome de domínio IE, foi utilizado por pessoas ou as organizações dentro da *Connection to Ireland*. Isso tem quatro categorias em especial, que são pessoas que têm a sua base ou moram na Irlanda, podem ser cidadãos da Irlanda que moram no exterior também, ou podem ser organizações com base na Irlanda, como pode ser a **[inaudível – 00:10:29]**, a CRO, ou fora da Irlanda; que oferecem serviços ou vendem coisas à Irlanda. Então, essas são as quatro categorias que estão vinculadas com a Irlanda.

Se bem eu entendo e não sei aqui se alguém tem outra informação, eu acho que nenhum outro registro tem uma exigência como *Connection to Ireland*, ou Conexão a Irlanda. E quando falamos do abuso, queremos manifestar que o .IE tem uma imagem mais ampla do que a ICANN considera o abuso do DNS. Nós tentamos dividir em três categorias. Um tem que ser o uso indivíduo técnico, o abuso técnico, *botnet, malware* e mais. E é o que a maioria das pessoas conhecem, como abuso do DNS. Mas nós também falamos de abuso de conteúdo, que são conteúdo ilegal, como podem ser

fraudes, ou também o que tem a ver com os menores. E também o uso indivíduo de registração, que são essas registrações de má fé.

A mensagem principal que quero dar é que essas definições são importantes, do meu ponto de vista pessoal. O que é muito mais importante é que temos diferentes medidas, que podem proporcionar uma resposta adequada, dependendo da situação.

Não é adequado para que o registro comece definindo se é um crime ou se é uma questão ilegal, má fé. Mas, no entanto, se há um juiz, um regulador ou um árbitro que diga isso é ilegal ou má fé, então devem existir medidas implementadas, como para responder essas decisões, assim que tudo isso for necessário.

Então, eu gosto dessa sigla que é ATOM, Medidas Técnicas e Organizacionais Adequadas. Esta é uma lista, que não inclui todas as medidas que temos. Mas o que quero mencionar aqui é que nós consideramos que é necessário ter essas medidas organizacionais e técnicas, porque eu não acho que exista uma única coisa, que possa evitar tudo. Então, podem existir suspensões de nome de domínio, medidas de governo, com regulações. Pensamos que todos são instrumentos. E é como um martelo, é muito necessário quando é necessário, mas se eu quero utilizar um martelo apenas para fazer um ninho, com certeza que não vai ser de utilidade.

Então precisamos de diferentes instrumentos e ferramentas e um enfoque mais amplo também. Então, sei que alguns de vocês vêm do aspecto da cibersegurança, então precisamos controles preventivos. E eu quero utilizar outro quadro, outra realidade,

digamos, que vem da saúde, outro aspecto que vem da saúde pública.

E aqui vemos que no mundo da saúde pública, em termos gerais, falamos da prevenção, não mitigação. Mas prevenção para utilizar intervenções adequadas para deter uma coisa ruim, para que isso não aconteça na saúde da comunidade ou no ecossistema ou numa população. Essencialmente, como já falei, é um papel fundamental, que fala da prevenção. É uma intervenção que é necessária e proporcional para deter um efeito adverso, para que esse efeito não aconteça. Há diferentes camadas. Isso vem da saúde pública. Mas eu acho que também aplica a diferentes áreas de políticas.

Como eu posso ver, que tem a ver com as avaliações ambientais. E eu entendo que geralmente eu tendo a utilizar, quando estamos falando de diferentes medidas para mitigação ou controle. Essas são diferentes camadas. Primeiro, a prevenção primária, porque é encontrar um problema e parar antes de que se torne um risco. Ou seja, deter esse tema ou trabalhar para evitar o que acontece depois, para que não aumente o risco, o perigo.

Então temos também o nível organizacional, que é contar com as políticas, boas práticas de governança. Nível governamental, isso pode ser ver se os entornos regulatórios ou as questões da lei podem ajudar a cumprir o objetivo. Se o objetivo é aumentar a segurança, a cibersegurança, as leis ou regulamentações estão obrigando os registradores a fazer ou não fazer coisas, para que

tudo se torne mais seguro? Se queremos melhorar a segurança de dados, existem diferentes políticas ou regulações que estejam implementadas para que as organizações façam coisas, que protejam os dados pessoais?

Em última instância, com a prevenção primária, vemos isso de uma forma mais ampla para ajudar a cumprir os resultados. Se é um instrumento adequado, por exemplo.

A prevenção secundária está mais perto do problema. Porque deter uma ameaça que é iminente, como as primeiras etapas de uma doença. Há alguns sintomas que detectamos, detectamos o problema. E temos uma resposta rápida, para que isso não piore. Então, nesse contexto, se um site é comprometido e tem risco de *phishing*, há sistemas para detectar isso, há processos implementados também. Se tivemos um ataque de DDoS, por exemplo, podemos ter como um AnyCast, algum controle para deter esse ataque iminente.

Agora, a prevenção terciária, que já existe no hospital, por exemplo, há um *ransomware* no hospital, aconteceu alguma coisa ilegal e é a redução do dano. Quais são os controles implementados, então para corrigir ou evitar que esse dano continue avançando no âmbito avançando. No DNS, por exemplo, pode ser uma baixa suspensão.

E a última prevenção, quaternária que é sobre evitar as intervenções inadequadas. Se a prevenção secundária é evitar falsos negativos; no caso da quaternária, trata-se de evitar falsos

positivos. Não precisamos intervir ou só... não intervir de forma desproporcional. Isso que haja um desbalanço com os direitos fundamentais. Por isso, precisamos desse tipo de medidas implementadas, para ver como são as revisões de políticas, as avaliações, o impacto regulatório, entre outras coisas.

Então, com o .IE, colocamos o foco nas diferentes medidas. Começamos com políticas e práticas mais amplas, depois com medidas técnicas mais detalhadas. Mas eu queria transmitir para vocês que de forma individual podem ter diferentes funções, mas todas com o mesmo objetivo, que o .IE seja seguro e confiável.

Então, como exemplo, vou mostrar um protocolo implementado por nós com um relacionamento muito bom com os órgãos governamentais. Os colegas desses órgãos e o protocolo da autoridade regulatória é um exemplo excelente. Esse aqui é um protocolo, em que se tivermos um órgão da lei, regulador, que destacou que pode haver um problema. Por exemplo, alguém que diz que é arquiteto e não é um arquiteto, e é infração da lei. Então o órgão regulador de arquitetos diz “Bom, esse senhor aqui não é arquiteto. Portanto devemos tomar alguma medida”. Então faremos uma verificação de antecedentes, analisaremos a solicitação. E se tivermos as fundamentações jurídicas, informação suficiente para tomar uma decisão sobre o que pede, determinamos se é necessário e determinado.

A lei estabelece que essa informação deve ser oferecida. Então, se vemos que a solicitação é proporcional, vemos que o registratário

recebe uma notificação. Se não for urgente, o registratário tem uma série de dias para resolver a questão, recebe a informação de contato do órgão regulador. E, se tiver em consulta, podem fazê-la diretamente. Porque queremos evitar ter essa posição de juízes. Então, nós queremos ser esse canal através do qual, o órgão regulador, quando há algum problema, pode entrar em contato com a pessoa que tem o problema. Então poderá ser resolvida a questão de forma mais direta.

Então esse período diz que se tivemos uma resposta insatisfatória e, dependendo da situação, adotamos uma medida corretiva, com uma suspensão desse nome de domínio. Mas, quase sempre, o que acontece é que o registrador diz “Eu não sabia”. Então fazemos a modificação rapidamente e está tudo bem.

Então, para o caso de uma questão urgente, grave, um pesadelo. Nesse caso, os órgãos regulatórios sabem que, se algo deve ser suspenso, logo devem recorrer ao provedor de hospedagem. E podemos ter alguém, talvez, que possa ter acesso ainda ao endereço IP, sem eliminar o conteúdo. Portanto, os órgãos reguladores e policiais sabem que devem recorrer aos provedores de hospedagem.

Eu não sei de alguma coisa como essa. Mas se houver a necessidade de suspensão de um site, o que podemos fazer é dificultar o acesso. Espero que isso não aconteça, nunca aconteceu.

Aqui, uma última estrutura, que gostaria de mostrar a vocês, inspirada na saúde pública. E acho que este interesse é a escala da intervenção, que mostra diferentes maneiras em que um órgão, um governo, pode intervir. E dependerá do nível de invasão, quanto mais invasão, mais justificativa, mais proporcionalidade.

Começamos com o verde, a base, nenhuma intervenção é requerida. É uma opção por defeito, com a qual devemos comparar. Então, o governo deve mostrar porque uma coisa deve ser feita. Depois temos uma intervenção que exige o fornecimento de informação. Nós protegemos dos abusos do DNS, o *phishing*, facilitamos alguma inversão, escolhemos bloquear o DNS. Depois mudar por defeito, de forma automática. Não publicamos a informação no WHOIS, salvo se alguém pedir afirmativamente, que seja publicada. Depois entramos em um âmbito mais teórico e complexo, como os incentivos econômicos.

Se alguém quiser que as organizações tenham melhor cibersegurança, aqui teremos fundos para conseguir isso. E, por outra parte, temos desincentivos que é o contrário. Aumentamos as auditorias, para aqueles que não têm algum tipo de credenciamento. Depois temos a escolha restrita, como ABC. Isso para os registros, pelo qual devem informar informações dos registrantes.

E, por último, eliminar a possibilidade de escolher algo, que deve ser informado, não é escolha. Há um mandado judicial, que exige uma coisa. E, por exemplo, na Irlanda temos uma ordem que pode

solicitar ou ser emitida por um juiz de bloqueamento. E, se estivermos em uma situação de vida ou morte, e se não houver infração dos direitos fundamentais de um usuário de internet e o juiz estiver convencido de que isso corresponde, então ele poderá emitir essa ordem de bloqueamento por 21 dias, como máximo. Depois pode haver uma prorrogação.

E, portanto, a opção mais invasiva de eliminar as opções utilizadas nas situações mais extremas. Essas ferramentas, de forma combinada, podem ser úteis. Mas se não corresponderem, podem ter efeitos adversos.

Então, as principais mensagens aqui, para lembrar é que a mitigação é efetiva e para isso não alcança ter uma única ferramenta. Mas precisamos de diferentes medidas, técnicas organizacionais, intervenções apropriadas necessárias e proporcionais, a colaboração significativa entre reguladores, registradores e o registro-chave nessas situações. E é importante evitar intervenções exageradas. Muito obrigado.

TOMONORI MIYAMOTO Muito obrigado, Declan, pela apresentação. E, por questões de tempo, vamos aceitar só uma pergunta ou duas perguntas ou comentários. Só vejo aqui uma mão levantada, o Dr. Shamsuzzoha, representante de Bangladesh.

DR. SHAMSUZZOHA

Obrigado por essa excelente apresentação. É muito interessante observar como é feita a operação do ccTLDs, aqui na Irlanda. Duas perguntas. Primeiro, tem a ver com esse protocolo regulatório. Eu entendo que é mais de natureza reativa e que depende mais do que mais, por exemplo, o que vem dos órgãos regulatórios. E, segundo, quanta as medidas de mitigação para processar informação, qual é o processo seguido? Essa é a minha primeira pergunta.

E a segunda, se nós levarmos em conta a proporcionalidade do sistema, se algo é proporcional ou não, então, qual é o mecanismo que, .IE, está utilizando? Há algum sistema obrigatório, ou só estão baseados na boa-fé, ou são simplesmente processos autoiniciados, automáticos?

DECLAN MCDERMOTT

Temos diferentes mecanismos. Mecanismo de Revisão de Políticas; um Comitê de Políticas Multissetoriais Externo; diferentes registradores, governos, representantes e organizações locais, que trabalham também pela comunidade da Internet da Irlanda. Esse é um mecanismo para revisar as modificações de políticas ou qualquer medida importante. E deve passar por esse comitê, para assegurar-se de que não esteja deixando alguém em desvantagem e que esteja alinhado com os valores do .IE.

Mas também está a opção para o caso de uma mudança significativa de políticas e que possam submeter-se a uma consulta pública, como fizemos ano passado, quando tivemos algumas modificações importantes nas políticas. Mas quanto à sua primeira

política, em última instância, vai depender do contexto específico. Eu respondo ao meu registro, .IE. Não faz sentido para nós ter uma moderação de conteúdos que seja proativa, nem sequer poderíamos fazê-lo e acho, segundo a legislação nacional.

Mas eu acho que isso vai depender do contexto regulatório, em que esse registro existir e dependerá da busca de um bom balanço e quanto risco queremos aceitar. Porque, se olharmos para os dados estatísticos e quanto abuso há em .IE, vemos que a exposição ao risco é muito baixa.

TOMONORI MIYAMOTO Muito obrigado pelas perguntas. Vamos agora às novidades sobre o PDP. E a Martina Barbero vai falar o mais rapidamente possível sobre esse assunto.

MARTINA BARBERO Estamos atrasados. O Tomo já mencionou que, em Praga, o GAC emitiu um texto no *Communiqué,* em que recomendava à Diretoria e à GNSO, que tomasse todas as medidas preparatórias necessárias antes do próximo PDP. E isso foi seguido por um relatório de questões preliminares sobre o PDP, sobre a mitigação de abusos de DNS. Foi feito em setembro e depois foi apresentada uma resposta.

E eu vou mostrar aqui, o que nós levamos em conta como importante dessa resposta do GAC. Mas, principalmente, o que vemos é que a sugestão é de priorizar três lacunas em matérias de

política. São as APIs irrestritas, às verificações de domínios associados e os algoritmos gerados pelos domínios. Primeiro, as APIs e os controles de domínios vinculados são adequados para o fim perseguido pela política. Enquanto o último, os DGAs, não necessariamente são os que poderiam ser abordados através da política.

Depois, o GAC ofereceu apoio para os dois temas mencionados, esses dois primeiros, sobre as APIs e os controles de nomes de domínio associados.

E o GAC quer priorizar mecanismos que permitam baixar com a maior rapidez possível. Também mencionamos que o relatório de assuntos contém outras brechas ou diferenças que devemos levar em conta. Porque os dois PDPs que talvez sejam começados serão com avanços significativos com o uso indevido ou abuso do DNS. Sabemos que esse é um assunto muito amplo. E esses dois PDPs não podem ser suficientes para tratar tudo que tem a ver com o abuso do DNS.

Também vemos outras questões identificadas no relatório de assuntos. O GAC mencionou que há problemas que são de especial importância e também são enumerados esses problemas no relatório. Também o GAC disse que queria participar do PDP. Mas que precisava mais informação sobre os métodos de trabalho e a possibilidade de alternar os participantes. Porque isso é o que fez o GAC em outro processo de PDP e que funcionou muito bem. Seguinte slide.

Ontem, houve uma Sessão Dirigida com a GNSO, com a comunidade, sobre os PDPs previstos. Eu quero destacar algumas das coisas discutidas ontem. Com respeito à estrutura dos PDPs, parece existir certas ideias alinhadas, quanto a ter dois PDPs e não apenas um. Mas muitos detalhes quanto a carta orgânica, o funcionamento, não foram tratados ontem especificamente no debate. Também existe o apoio da comunidade de pensar duas vezes antes de abordar os DGAs, como um tema que não tem a ver com um PDP. Ou seja, esperariam que existisse um PDP a respeito desses algoritmos.

E também com respeito às APIs e nomes vinculados, existiram algumas dúvidas, quanto às APIs irrestritas. Em termos gerais, falávamos antes de registrações massivas e não de APIs. Mas agora parece que as APIs são uma das formas de registrar os domínios de forma massiva. Mas dessa forma não resolveríamos o tema que queremos resolver. E

quanto aos nomes de domínio associados. Esse parece ser um tema relativamente simples de abordar. Mas é importante manter o equilíbrio e esclarecer que controles são feitos, segundo que características, se tem a ver com a identidade do registratário, a forma de pagamento, manter a transparência em contraposição com permitir que os registradores em especial, utilizem um enfoque que não outorga àqueles que querem criar algum uso indevido os elementos suficientes. E no seguinte slide.

Sugere que se esses PDPs avançassem, como talvez aconteça nessa instância, com as cartas redefinidas, o GAC poderia participar neles. E conforme experiências prévias, é uma coisa que funciona muito bem. Ah, desculpe, eu tenho que falar mais devagar. Mas eu tenho que falar rápido também. Porque temos pouco tempo, mas nem tão rápido. Uma coisa que funcionou nos PDPs anteriores foi ter um grupo reduzido. Porque no Processo de Desenvolvimento de Política vão existir um ou dois representantes do GAC. Mas outro substituto, caso se substituir a carta ou se modificar a carta estatutária. Mas nem todo o GAC pode participar. E o abuso de denúncias é um tema importante para todos.

E ter a garantia de que todos os que querem participar participem. Ter grupos menores. Por isso falamos de grupos reduzidos, subgrupos, que prepare todo o trabalho sobre o PDP e quem estiver interessado possa participar e fazer as trocas de opinião com o representante de opinião do GAC. Isso funcionou muito bem para os dados de registração e poderia ser um modelo a utilizar para esses PDPs. Passemos ao seguinte slide.

Este é o meu último slide e espero que possamos falar, porque há três perguntas que queremos fazer para vocês. Primeiro, se segundo as deliberações mantidas nesta sala do GAC e também com a comunidade no dia de ontem, se há alguma mensagem adicional que deveríamos comunicar à Diretoria com respeito a esses PDPs? Quanto à estrutura ou com qualquer outro elemento, podem nos avisar, que poderiam lhes interessar. Se estariam dispostos a participar da iniciativa do PDP ou desses grupos

reduzidos? Porque queremos saber quem estaria interessado em assumir esse trabalho.

A segunda pergunta tem a ver com o trabalho adicional, que deve ser feito sobre o abuso do DNS fora os PDPs. Há uma lista de possíveis temas que ainda devemos tratar e se há alguma mensagem para transmitir à comunidade a respeito? Fora o que já foi mencionado no comentário público do GAC, essa seria a oportunidade para que vocês falem.

E a última pergunta, geral, se há alguma outra consideração ou assunto que devemos tratar em termos do abuso do DNS sobre a base desse relatório de assuntos preliminares? E é esta oportunidade para que vocês se apresentem nesses temas e queiram ver refletidas nessas deliberações. Nico, passo a palavra para moderar a segunda parte.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Mais uma vez obrigado por esta apresentação com tantos detalhes. Martina, Comissão Europeia, realmente este é um bom momento, para que os nossos distintos membros do GAC participem. Quanto a qualquer uma das três perguntas ou qualquer outro assunto, obviamente, a Alemanha está pedindo a palavra. Por favor, Alemanha.

RUDY NOLDE: Rudy Nolde, da Alemanha. Em primeiro lugar, obrigado, líderes, por apresentar essa excelente apresentação e também por

preparar essa apresentação e também pelo trabalho realizado nos últimos meses. Para a Alemanha, o abuso do DNS, obviamente que é uma prioridade na ICANN. Nós estaríamos também satisfeitos em qualquer preparação, em qualquer forma de participação no GAC, ainda na forma de grupo reduzido. E nós somos flexíveis nesse sentido.

Quanto à segunda pergunta, sobre as diferenças de política, eu acho que é um pouco mais geral. E esperaria talvez que o PDP ou os PDPs pudessem agir como um ponto de partida para um trabalho maior, analisar um tema e depois rapidamente avançar. Entendendo que a GNSO, assim que tratados esses dois assuntos e vemos que há outros temas, como para trabalhar. Não temos que dizer "Olhe, esperemos dois anos para ver o que é que está acontecendo" e de outra forma poder talvez ir assumindo um tema após outro. Esses são os comentários que eu quero fazer agora. Obrigado.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Alemanha. E eu vou supor que a Alemanha está se oferecendo como voluntário para a parte 1A da pergunta? Não, não, não, é uma brincadeira. Muito obrigado, obrigado Alemanha. Agora está na lista Estados Unidos. Não, desculpe, Índia primeiro e depois, os Estados Unidos. Por favor, a Índia tem a palavra.

SANTHOSH THOTTINGAL: Santhosh, representante da Índia. Obrigado, Sr. Presidente. Sim, nós estamos interessados também em trabalhar no PDP. E

também apoiamos este PDP com um alcance mais limitado. Porque tem que tratar temas de alta prioridade, que foram identificados no Relatório de Assuntos Preliminares, especialmente o que está a respeito das registrações massivas.

E esses assuntos obviamente têm a ver também com poder automatizar o que é a registração sistêmica. Então na ICANN 83 houve uma recomendação, por consenso, que tinha a ver com as ações que podiam ser tomadas sobre sistemas do PDP. Obrigado.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado, Índia. Agora tomamos nota. E agora passamos a palavra para a representante dos Estados Unidos.

SUSAN CHALMERS: Quanto à segunda pergunta, eu lembro uma discussão que tivemos hoje de manhã com o ALAC sobre a transparência e a apresentação de relatórios, onde foi mencionado que os requisitos para apresentar relatórios das partes contratadas na atualidade não estão nos contratos. Eu acho que há um requisito para ter e manter registro do abuso do DNS, recebido pelos registradores. Existe sim, mas não para fazer uma apresentação de relatórios, que seja pública sobre os relatórios de abuso, quando receberam e também quando responderam a esses abusos.

Eu menciono este ponto porque durante a discussão intercomunitária, que foi uma sessão muito boa - não devemos esquecer - falou-se sobre o cumprimento para a verificação dos

domínios associados, que poderia ser eficaz do ponto de vista do cumprimento. Então, há também um requisito de transparência, que pode ajudar ao cumprimento. É uma intervenção muito técnica, mas eu acho que também teria sentido para cumprir. E também já mencionamos no comentário feito no GAC, quando participamos logo de início de todo este assunto. Muito obrigado.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Obrigado. Agora está a Dinamarca.

FINN PETERSEN: Finn Petersen, da Dinamarca, para os registros. Muito obrigado pela apresentação. E a respeito da pergunta 1, eu acho que também mencionamos que as APIs podem ser, talvez, um pouco restritas ou restritivas. Em termos gerais, falávamos de deixar de lado a registração. Desculpe. Falamos de registrações massivas no GAC. Mas eu não sei se podemos dar o alcance ao PDP para tratar de investigar, para saber quais são os outros métodos que uma API possa estar dentro desse PDP de alcance limitado, como para não tratar de resolver o problema incorreto, de uma forma incorreta. Mas ter um PDP que o resultado possa ser implementado de forma eficaz.

Por outra parte, quando falamos da registração de nomes de domínio, ou nomes de domínios associados, eu vejo que as verificações que vão ser realizadas são difíceis de realizar, se começamos do zero, do começo. Então, se pensamos no que fazer,

talvez vamos pensar de que forma o cumprimento pode analisar, se estão cumprindo o PDP ou não. Eu acho que essas são outras perguntas que deveríamos analisar. De que forma? Por uma parte, não damos a transparência aos ruins, aos bandidos. Mas de que outra forma mantemos os instrumentos necessários, para que o cumprimento da ICANN possa analisar e ver como estão implementando esse PDP, agora no futuro.

Do lado técnico, nós, como Dinamarca, também gostaríamos de contribuir a este tema com qualquer nome que possam dar.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Muito bem, Dinamarca. Tomamos nota dos comentários. Este seria o ponto 1A, da pergunta 1A. Agora, está a Comissão Europeia, por favor.

GEMMA CAROLILLO: Muito obrigado, Nico. Eu acho que, em primeiro lugar, devemos assinalar ou mencionar que avançamos muito nos últimos anos. Então, ainda não continuamos falando do abuso do DNS. Porque agora falamos de forma coletiva, não só o GAC, mas como comunidade avançamos, eu acho. Por isso, eu quero manifestar a minha satisfação a respeito.

No que tange a pergunta número 2, porque a número 1, eu acho que não temos forma de fugir dela. A Comissão já faz parte e seus líderes também. Enfim, eu quero apoiar um pouco o que falou o Susan, dos Estados Unidos e também Finn mencionou isso. Não se

trata porque somos brilhantes, mas porque o GAC já está ou esteve no momento das emendas contratuais. E se falou da transparência, eu acho que é muito importante. Eu acho também que isso não foi devidamente tratado no momento das emendas e ficou como, uma das brechas ou diferenças dentro da política. Porque também foi motivo do Relatório de Questões.

E há outros dois assuntos mencionados no Relatório de Assuntos, como o uso de medidas proativas preventivas. Nico fez referência aos algoritmos de detecção. Então, bom, este seria outro trabalho, outra área de trabalho, que deveríamos enfrentar. E também, no Relatório de Assuntos, se fala da necessidade de falar sobre a exatidão dos dados de registração, especialmente o que tem a ver com a validação, com normas que talvez alguém pode me corrigir. Porque já foi feito pela presidência da GNSO. Eu acho que vão passar agora a GNSO, que está falando do uso indevido, abuso do DNS. Mas há muitas atividades, que têm a ver com este tema tão importante.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

Obrigada, Comissão Europeia. Sim, eu gosto desse algoritmo. Mas lembrem também que os maliciosos conhecem essas ferramentas. Eu não estou falando do ChatGPT ou na IA Generativa, LLMs. Mas sobre algoritmos muito sofisticados, como o *clustering* ou o *random forest*. Não vou entrar em detalhes a respeito deles.

Mas sim, mais algum comentário ou pergunta antes de continuarmos. Porque ainda devemos mencionar e falar sobre

algumas outras questões. Então, ninguém levantou a mão, nem aqui, nem online. Então passo a palavra a Susan Chalmers, que vai falar sobre a questão dos Programas de Notificadores Confiáveis.

SUSAN CHALMERS Obrigada, Presidente. Vou mudar um pouco aqui o foco, e como a colega mencionou antes, os Objetivos Estratégicos do GAC sobre a questão de abusos do DNS, os organizamos em duas categorias principais. Primeiro, o trabalho de defesa quanto ao abuso do DNS. E estamos avançando, quanto ao trabalho de políticas, e encorajando os PDPs, e também temos uma sessão de capacitação.

E os colegas de tópicos estão trabalhando, e vão continuar trabalhando para fornecer recursos aos representantes do GAC, para gerar capacitação sobre a questão dos abusos do DNS em geral. E no item 4.7, aqui, uma das ideias foi fornecer informação sobre esses Programas de Notificadores Confiáveis.

E aqui temos um bem conhecido. E vemos que esses programas podem ser utilizados para resolver atividades do DNS, fora da incumbência dos contratos à ICANN. Então, hoje, temos muita sorte de ter aqui dois representantes da DotAsia e da TWNIC, que estão aqui na outra ponta da mesa, que vão apresentar o seu trabalho sobre Redes de Notificadores Confiáveis.

EDMON CHUNG

Muito obrigado. Eu vou primeiro, e depois passo para o Jo-Fan. Muito obrigado pelo convite. Esse assunto eu conheço muito bem. Eu vou falar um pouco sobre a história disso. Mas acho que é algo importante, é um assunto importante.

Aqui vejo a minha versão do que o Tomo e a Susan apresentaram no seu slide. É isso que está acontecendo no ecossistema de abusos. E é uma parte muito importante, porque acontece em diferentes componentes da rede. E é por isso que focarmos só na incumbência da ICANN não é satisfatório, não é suficiente.

Aqui nesse slide temos uma visão diferente, que é parecida com o que apresentou o Declan antes, sobre ter uma visão mais ampla dos abusos. Aqui é como a DotAsia vê isso, vemos os abusos cibernéticos mais amplos. Depois temos um círculo menor, o abuso do DNS. E existe um círculo ainda menor, que são abusos apropriados para os registros de domínios de topo, para sua mitigação. E dentro da ICANN, e parte que vai além do mandato da ICANN, inclusive o CSAM e outros estão incluídos. E é importante observar isso. Não deve acabar com o PDP da ICANN.

Podem ser outras coisas também. Vemos aqui o nosso trabalho com o .KIDS, que começamos antes da última rodada, sabíamos claramente naquele momento que essa mesma política para o .SEX era bastante diferente do .KIDS. E aqui temos um aspecto importante, que é como é que os registros... Bom, vamos reformular. Os registros começaram com o mandato da ICANN,

como base para lidar com abusos. Mas isso vai além de tudo isso. E devemos abranger muito mais o .KIDS.

É um bom exemplo. E também queria destacar que hoje, quando lançamos o .KIDS, faz dois anos, as plataformas e tecnologias de abuso do DNS, implementadas nos últimos 15 anos, foram muito instrumentais para permitirmos fazer ainda mais coisas e resolver mais abusos. E depois eu vou entrar em detalhes sobre isso.

E aqui, por exemplo, essa é a nossa jornada, começou em 2011 em Singapura. Tivemos um Fórum de Abuso do DNS, um dos primeiros nos quais DotAsia participou. E temos avançado nos últimos 15 anos.

E aqui nesse slide eu queria falar sobre o Notificador Confiável. E queremos ir bem além do mandato e os requisitos da ICANN. E começamos com um tipo de abordagem registro a registro, e esses são os que foram formalizados, e outros registros de ccTLDs também, e também de gTLDs. Mas eu vou me focar nos ccTLDs.

E por que isso para registros? E é para manter um nível similar de sensibilidade para a suspensão de domínios... uma suspensão de domínios. E isso tem um efeito bem mais amplo e também similares sensibilidades também para os registros, para que possam ver isso e transmiti-lo através de uma suspensão expedita. Então, nos dois pilotos que criamos com .TW e .UK, tivemos um canal de comunicações e um e-mail dedicado com chaves compartilhadas.

Sabemos quem é que nos envia, sabemos que é confiável, e isso tem um formato de *due diligence* e agimos rapidamente. Então, é isso que estamos fazendo e esperamos que daqui e em outros âmbitos convidemos outros ccTLDs para trabalhar conosco. E nos últimos meses, no último ano de fato, criamos isso e cada vez mais, estão ativos e há domínios que recebem notificações.

E por que isso? Porque vocês talvez saibam, em situações reais, que às vezes há *phishes*, que são dedicadas para regiões particulares. Há um que é para Taipei e alguns sistemas de monitoramento não os detectam. E, portanto, devemos contatar os colegas em Taiwan, para que enviem uma notificação e possamos lidar com isso. E é por isso que estamos tão felizes por agir e trabalhar com outros ccTLDs. Porque isso ajuda muito. Há coisas que talvez perderíamos, os *phishes* ou os ataques para certas regiões geográficas.

Portanto, é muito bom trabalhar com outros ccTLDs. E estamos explorando outros aspectos também, bem além da incumbência da ICANN. Por exemplo, começamos com a definição de abuso do DNS. Mas realmente queremos continuar expandindo os Notificadores Confiáveis, essa rede para cobrir outros tipos de abusos também. E convidamos os ccTLDs a fazer isso e, através deles, conectar-nos com as equipes de resposta, serviços nacionais. E, através dos ccTLDs, podemos manter a sensibilidade em nível de registro e, ainda assim, poder lidar com os abusos, bem

além da incumbência da ICANN. Essa é a minha apresentação. Passo aqui para a Susan, talvez. Sim.

SUSAN CHALMERS

Olá. Obrigada. Só queria voltar um pouco para trás. Aqui, temos um representante de um registro que administra um gTLD e também o CEO de TWNIC, que administra um ccTLD. Eu queria destacar isso, o TWNIC. E isso é muito importante. Então, só queria perguntar uma coisa.

O que é que um notificador seja confiável? Você poderia explicar isso? Muito obrigada.

JO-FAN YU

Muito obrigada. Obrigada a todos e obrigada pelo convite. Estou muito contente por compartilhar isso sob a perspectiva do ccTLD e o marco de notificadores confiáveis.

Por quê? Porque esse Marco de Notificadores Confiáveis se os abusos são globais e, por outra parte, temos uma demanda cada vez maior de prestação de contas. Agora, as respostas tradicionais não são suficientemente rápidas e também temos restrições. E também o que é importante aqui sob a perspectiva das OIGs é que, como ccTLD, recebemos notificações irregulares sobre sites irregulares, isso dos governos. Isso foi em 2025 até final de setembro. E podemos ver os dados aqui. Só menos de 1% dos sites ilegais são de .TW, o que significa que as nossas restrições, mais de

99%, vão além da capacidade de adotar ações para realmente acompanhar a perspectiva do ccTLD.

E qual é o Marco, então, de Notificadores Confiáveis? Isso é para ações rápidas, baseadas na confiança e em regras pré-acordadas. E o objetivo é resolver abusos especialmente sérios de forma mais efetiva e eficiente. E também é importante ter uma série de princípios como confiança, transparência e processo devido.

Nesse marco, colaboramos com registos e registradores como DotAsia, .UK, .KR, .TOP e registradores como CSC. Além disso, quanto ao conteúdo, também nos focamos nos abusos dos DNS, especialmente o *phishing*. E, por exemplo, chegamos a acordos, negociamos com os parceiros, incluindo os princípios de transparência e processo devido e confiança, o que estamos fazendo agora.

Então, vemos aqui, nesse slide, que sem Notificadores Confiáveis, recebemos inteligência dos governos, também das forças de lei, comunidades de segurança, e nós, também, da TWNIC, os cidadãos. Investigamos uma denúncia e, para registradores e registrantes, eles fazem uma outra investigação. E, com base nos resultados, começam a agir., um bloqueamento por exemplo. E bloquear ou suspender um domínio.

Então, no âmbito dos Notificadores Confiáveis, depois de que a TWNIC chamou, seria investigado e, depois de notificar os registradores e registros, entra em jogo o acordo que está

estabelecido conosco. Então, podemos, utilizar esses recursos sem ter que gastar qualquer outro adicional para tomar ações.

Quais são os benefícios, então, do nosso ponto de vista? Em primeiro lugar, isso gera um espaço para criar um intercâmbio mais rápido e, também, para gerenciar os casos de abuso. Também reduz a carga de investigação dos registradores e registros. Em terceiro lugar, consideramos também muito importante, que podemos ser muito mais proativos. Porque ser eficiente pode significar várias coisas. Então, detectar um caso de *phishing* pode levar vários dias. Então, dessa forma, podemos tomar ações rapidamente antes de que aumentem de nível.

E esses são os dados de 2025. Todos, de forma resumida, aparecem aqui no slide até agora. Gerenciamos 51 domínios em 2025. Esperaríamos números mais altos. Porque, com os nossos sócios, começamos a trabalhar na segunda parte do ano. Então, esperamos ainda números mais altos para o ano próximo. 78% dos casos são de *phishing* confirmado. Então, se tomou alguma medida.

Também, o tempo de resposta, em tempo geral, é menor a dois dias. Entre um e dois dias, geralmente. Mas, também, consideramos que podemos acelerar o processo incorporando a automatização. Outra coisa boa até agora, é que não recebemos qualquer apelação, ou reclamação, talvez. Isso demonstra que o resultado é bom. Seguinte slide.

Então, quais seriam os desafios para nós? Como os registros e registradores têm diferentes critérios, nós dependemos disso nos nossos acordos bilaterais. Pode acontecer que o problema aumente, por isso temos essa referência. Então, como próxima etapa, vamos continuar expandindo as parcerias com esses Notificadores Confiáveis. E, talvez, podemos desenvolver e demonstrar um modelo não-regulatório bem-sucedido para ter a cooperação da indústria e nos alinhar também com as boas práticas da ICANN e do GAC, quanto ao abuso do DNS.

E essa seria uma referência, que constitui uma etapa fundamental para poder compartilhar a responsabilidade da internet entre as comunidades. E também encorajo todos vocês a considerarem mais este tema, inclusive a trabalhar em conjunto conosco. Então, qualquer dúvida, ficamos à disposição. Muito obrigado.

SUSAN CHALMERS Obrigado, Jo-Fan e Edmon, por essas apresentações tão oportunas. Agora, queremos passar a palavra aos representantes do GAC, para ver se tem alguma pergunta. Vejo que a OMP pediu a palavra.

BRIAN BECKHAM Obrigado, Susan, Jo-Fan. Eu sou Brian Beckham, da OMP. Eu tenho uma dúvida, uma pergunta quanto ao primeiro ponto do último slide. O tema que tem a ver com os critérios possivelmente diferentes para os registros, registradores e a escala. Então, eu não sei se consideraram ter talvez uma referência padronizada, para

resolver essa situação, para que os Notificadores de Confiança possam utilizar tudo o que tem num contexto, como para todo o ecossistema de forma mais ampla.

JO-FAN YU

Obrigado pela pergunta. Sim, seria muito útil, se conseguíssemos ter uma plataforma para ter essas negociações, intercâmbio de informação. Mas essa dificuldade agora está no nível de conscientização na comunidade. Até onde sabemos, se bem cada vez há mais consciência, ainda o nível de conhecimento é bastante baixo. Então, como a comunidade poderia formular uma norma, um padrão, critérios para compartilhar e tomar ações? Eu acho que ainda isso é um problema.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

Obrigado. Quer responder a Edmon?

EDMON CHUNG

Apenas eu quero complementar. A resposta simples é sim, claro que sim. O DotAsia está trabalhando com TW. E há tanto uma consideração e reunião de dados e materiais, que contribuam com provas e evidências para acelerar qualquer processo de suspensão. E trabalhar com o CleanDNS e também com o NetBeacon e outras organizações, com todas elas trabalhamos para chegar a alguma sorte de norma ou padrão de fato na indústria. Mesmo que não necessariamente seja talvez, uma coisa tão rígida.

TOMONORI MIYAMOTO Quero fazer uma pergunta. Obrigado pela apresentação. Como cada membro ou cada governo poderia ajudá-los?

EDMON CHUNG Bom, podem estimular seus ccTLDs, que trabalhem em conjunto conosco. Como já falei, nós priorizamos os registros por questões de sensibilidade das notificações de baixa, que é uma coisa proporcionalmente adequada para os nomes de domínio nos registros de primeiro nível. Então, eu encorajo e convido a que falem com seus ccTLDs para eles se somarem a nossa rede.

JO-FAN YU Eu acho que os seus ccTLDs têm um papel muito importante. Eu acho que os representantes do GAC podem ajudar a gerar consciência e estar aqui, se somem ao trabalho.

NICOLÁS CABALLERO, PRESIDENTE DO GAC Obrigado, Japão, pela pergunta. Há algum outro comentário ou pergunta nos últimos cinco minutos, que temos antes de passar a palavra aos Estados Unidos, para fazer algumas considerações quanto ao Comunicado? Colômbia?

THIAGO DAL-TOE Muito obrigado pela apresentação. Minha pergunta tem a ver justamente com isso. Basicamente, nós, a nível nacional, não temos que configurar o nosso próprio Programa de Notificadores

Confiáveis. Ou seja, podemos nos somar a outros, que já funcionam. Então, nesse caso, como fazemos? Qual o processo para anexar, digamos, ou para que sejam aceitas as nossas solicitações? Obrigado.

EDMON CHUNG

Atualmente, fazemos de forma bilateral, porque cada ccTLD em especial pode ter exigências diferentes, talvez dos outros, mesmo levemente. Esqueci outra coisa. Também nas notificações mútuas, compartilhamos dados. A cada três meses, compartilhamos os dados de suspensão com TW, e ao contrário também, e vice-versa. Mas esse tipo de acordos poderia não incluir necessariamente este ponto.

Então, basicamente, se trata de um acordo bilateral entre nós e outros ccTLDs. Com respeito a, se é necessário, sistemas, bom o nosso canal básico é tão simples como um correio confiável com chaves de intercâmbio. Mas por trás da cena, nos nossos sistemas, vocês determinam, como ccTLD aqui, que sistemas querem como backend.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

E como compartilham os dados? É CSV, são valores separados por vírgula, como compartilham?

EDMON CHUNG: É CSV e é um código simples, que explica a suspensão, além da suspensão do nome do domínio suspenso.

NICOLÁS CABALLERO, PRESIDENTE DO GAC: Susan, o tempo é seu.

SUSAN CHALMERS: Talvez podemos passar a tratar o último ponto da agenda para esta sessão. Os membros do GAC, com certeza, que viram que disponibilizamos previamente alguns textos a considerar para sua incorporação no Comunicado, para talvez gerar um pouco de reflexão, antes de redigir o Comunicado de Dublin na sessão sobre o abuso do DNS. Os responsáveis por esses assuntos ainda não têm qualquer recomendação. Estamos conformes com a recomendação produzida, oferecida em Praga e com o avanço feito pela comunidade nesse sentido.

Então, recomendamos incluir o seguinte nos Assuntos de Importância. Eu não vou ler, mas podem ver aqui na tela. Então, se alguém quer sugerir algum elemento adicional para a sessão de Assuntos de Importância do GAC, seria maravilhoso. Estamos trabalhando com um rascunho atualmente, então deixamos aberto o microfone.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

Obrigado, Estados Unidos. Como Susan mencionou de forma certa, está aberto o microfone. Se querem fazer alguma contribuição, ideia, é claro que sempre recebemos com beneplácito, as boas ideias. Alguma coisa que queiram adicionar antes de encerrar? Não vejo pedido de palavra, em linha também não, nem mão levantada aqui na sala. O que significa que basicamente estamos de acordo.

Então, muito obrigado, não precisamos estender mais. Temos dois minutos da sessão, mas, enfim, não precisamos cumprir esses minutos. Vamos fazer o recesso para o café. De fato, temos 30 minutos. Por favor, voltem 3 da tarde em ponto. Obrigado.

**[FIM DA TRANSCRIÇÃO]**