ICANN84 | Assembleia Geral Anual – Encontro conjunto: GAC e SSAC
Terça-feira, 28 de outubro de 2025 – 15h às 16h IST

NICOLÁS CABALLERO, PRESIDENTE DO GAC	Novamente, bem-vindos todos. Vamos começar daqui a um minuto. Ocupem seus lugares, por favor.
GÜLTEN TEPE	Bem-vindos à reunião do GAC com o SSAC. Terça-feira, 28 de outubro, 15h00 UTC. Por favor, vão anotando que esta sessão está sendo gravada e se rege pelos Padrões de Comportamento Esperados da ICANN, o Código de Conduta dos Participantes da ICANN e a Política Antiassédio da comunidade da ICANN. Durante a sessão, vão ser lidas em voz alta as perguntas e comentários, se forem apresentadas num formato adequado, no chat do Zoom. A interpretação da sessão nos seis idiomas das Nações Unidas e português. Quem quiser falar durante a sessão, levante a mão na sala do Zoom, digam seu nome para os registros e o idioma no qual vão falar, se não for inglês. Por favor, falem a uma velocidade razoável para permitir uma interpretação correta. Agora passo a palavra ao presidente do GAC, Nicolás Caballero.

NICOLÁS CABALLERO, PRESIDENTE DO GAC

Muito obrigado Gülten. Sejam bem-vindos mais uma vez. Espero que todos tenham aproveitado o café irlandês. E agora vou apresentar um bom amigo, o Ram Mohan do SSAC. Também está Suzanne e Maarten e Tara. Sejam bem-vindos. Vamos ter uma reunião muito interessante, pelo menos do meu ponto de vista, dividida em quatro partes.

A primeira e a mais importante, obviamente, conforme a minha opinião, tem a ver com a importância de um software livre de código aberto na indústria do DNS, também há outros. Mas enfim, o que tem a ver com a colisão de cadeias de caracteres semelhantes, o uso indevido do DNS, que é quase inevitável agora, e também a chance de cooperação entre o SSAC e o GAC. E agora ou depois das apresentações, vamos ter tempo para perguntas e respostas.

Agora então passo a palavra a Ram Mohan, meu bom amigo.

RAM MOHAN

Para mim, é um prazer estar aqui, Nico, com todos vocês aqui em Dublin e também com vocês do GAC. Realmente foi uma honra para nós que agora, depois de várias reuniões, vocês tenham continuado esses convites e nos dedicar o tempo dentro da sua agenda tão complicada. Porque também valorizamos esse tempo, que passamos com vocês e nos preparamos de forma intensiva para isso. Porque queremos ter a certeza de que a informação, que passemos durante a interação e comunicação com vocês, estejam

no nível correto. Mas também que seja informação sobre a que possam fazer coisas, tomar ações. Essa é a base de que nos preparamos.

E agora o que queremos então é, me concentrar na primeira parte, que tem a ver com a importância de um software livre de código aberto na indústria do DNS, e apresentar esse tema, falar de alguns detalhes com vocês. E agora eu vou passar a palavra a Maarten Aertsen, que é um dos copresidentes do Grupo de Trabalho sobre esse tema. Maarten?

MAARTEN AERTSEN Obrigado Ram, obrigado Nico. Hoje eu vou falar então de software. O SSAC, em termos gerais, exige documentos bastante técnicos. Mas este não é o caso. Então, a comunidade da ICANN, em si, não é seu público. Mas isso está redigido para os reguladores e formuladores de políticas dentro do mundo. Então, eu acho que estou no lugar certo. Se não são vocês, eu suponho que tem colegas que se encarregam, sim, da cibersegurança.

Por isso é que vamos falar de software. Se condensarmos o relatório em uma única frase, percebemos que o DNS está construído em um software livre de código aberto. E isso não é apenas para defendê-lo, sinal de que esse código livre e aberto é uma declaração sobre como o DNS está realmente construído.

Então, FOSS significa Software Livre de Código Aberto. Livre significa liberdade de expressão, né? E também, como uma cerveja Guinness de graça, depois desta apresentação, *Free* significa

liberdade e também gratuidade. Também temos uma liberdade e uma gratuidade no uso, né? Porque pode ser estudado o código, compartilhar, porque pode ser distribuída as cópias do software. E modificações ou mudanças, porque também pode mudar conforme necessário e também compartilhar essas mudanças.

Então, essas quatro liberdades geram um ecossistema fundamentalmente diferente para o desenvolvimento do software. Mas também para a distribuição e a manutenção em comparação com aqueles, que são software de propriedade exclusiva. Há uma diferença filosófica entre o que é o software livre e o código aberto, porque aqui em FOSS temos os dois conceitos concentrados nessas quatro liberdades.

O modelo de FOSS tem diferentes perfis de risco, diferente de um software com propriedade ou de propriedade exclusiva. Em termos gerais, esse software livre de código aberto é mantido pelos voluntários, onde a motivação realmente tem um papel fundamental. Se uma pessoa está trabalhando em software como voluntário, também pode sofrer um esgotamento profissional, um cansaço profissional e abandonar um projeto.

Então, por isso, outro dos riscos do FOSS é que não existe qualquer garantia ou apoio garantido e os operadores precisam, então, assumir a responsabilidade para reter dentro das suas empresas, aqueles que tenham conhecimento específico para fazer desenvolvimento, solucionar problemas de software, no caso, ou também gerar contratos onde isso aconteça.

Não se trata, então, de voluntários, mas são as organizações profissionais, as que assumem esse desenvolvimento de software. Então, temos esses beneficiários gratuitos onde pode existir uma situação, onde o financiamento não fique vinculado ao uso, onde quem faz a manutenção tem base numa iniciativa, que paga aqueles que fazem a manutenção. Mas isso gera diferenças entre o de financiamento, que tem a ver com novas cargas regulatórias. Por exemplo, o modelo de financiamento pode se ver ameaçado.

Então, isso é real e é o que acontece no modelo FOSS. A regulamentação, que não considera essas concessões, pode piorar esses riscos ou melhorá-los.

Também há algumas fortalezas no modelo. Aqui veremos especificamente o DNS. No slide anterior falávamos de FOSS em geral. Quando vemos o DNS em especial, podemos ver que há maior transparência e uma segurança de colaboração. Porque as comunidades, tanto acadêmicas como operacionais, mantêm uma cultura ativa e importante, robusta, sobre o que é a revisão do software de DNS em FOSS. Isso acontece durante décadas. Podemos ver documentos de 90, onde há algumas falhas no FOSS e que se tratou de solucionar, que é o que acontece na realidade.

E os operadores, que nós perguntamos ou pesquisamos, que foram mais de 100, conseguiram realmente diagnosticar, verificar e solucionar os problemas de vulnerabilidade. Porque não dependem do fornecedor. Mas podem agir proativamente em caso de falhas.

No DNS em especial, há diferentes projetos de DNS, que são mantidos pelos voluntários e também por organizações de longa data e também estáveis. Isso significa manter a implementação do software durante mais de 20 anos. Esta longevidade gera então um registro sobre o que confiam os operadores.

Outra das fortalezas do FOSS no DNS é que existe uma flexibilidade operacional na diversidade. Porque podem nem existir diferentes situações de FOSS, implementações; para que os operadores façam correr diferentes ou executem diferentes softwares. E baixa os obstáculos para as organizações para ter a sua própria infraestrutura, o que evita o risco de concentração. Ou, como também vimos no assunto candente faz pouco tempo, os equilíbrios entre o que podem ser entidades estrangeiras e as suas dependências.

E agora vamos falar de segurança. O SSAC se concentra na segurança e é muito importante entender o que significa segurança em software. Porque a segurança não está determinada por um código aberto ou fechado. Também não se os desenvolvedores são voluntários ou recebem algum pagamento. E também não é definido pelo software, quando provém de uma empresa comercial ou sem fins lucrativos.

Mas o que determina a segurança tem a ver com a revisão do código, como estão disponíveis essas revisões e também manter a sustentabilidade dos recursos para manter esse software.

Então, temos no caso que considerar a qualidade dos processos de desenvolvimento dos projetos e não só a habilidade do código fontes.

Muitas vezes escutamos, mas FOSS é mais ou menos seguro que o software de propriedade exclusiva? A resposta é nenhuma coisa, nem outra. Porque a segurança está determinada pela qualidade do processo de desenvolvimento e não pelo modelo de outorga de licença.

Então, o desafio da política é que FOSS tem um perfil de risco diferente. Não podemos ou não pode ser feita uma cópia e cola no que acontece no mundo do software de propriedade exclusiva, para levar para a realidade do FOSS.

No começo, eu disse muito importantes, mas agora vou apresentar dados a respeito dessa informação. Vamos começar com o sistema de informação raiz. Perguntamos aos 12 fornecedores de sistema raiz para tentar identificar o software, que utilizavam. E vimos uma dominância do software livre de código aberto. Nove dos 12 operadores de servidor raiz utilizam o software livre de código aberto, exclusivamente. Inclusive, os operadores que utilizam o software de propriedade exclusiva para tanto, em termos gerais, também executam software, ou FOSS, ao mesmo tempo. Então, o que colocamos aqui é que não se trata de uma porcentagem baixa. Mas a grande maioria que utiliza FOSS dentro do DNS.

Agora veremos os operadores de TLDs, de domínios de alto nível. Estas entidades têm serviços autoritativos de DNS e o que

encontramos é que os operadores, que servem para os operadores que são 9 de 10 utilizam FOSS, como estrutura ou infraestrutura do DNS.

Talvez para essa audiência seja mais pertinente saber como funciona no âmbito de cada um dos países com domínios de alto nível. Podemos ver que 20 dos 25 operadores de ccTLDs utilizam FOSS. Em termos gerais, então, os operadores atendem 234 ccTLDs exclusivos, que utilizam FOSS. Isso é apenas no âmbito, que vimos esse resultado, que podem ser ainda maiores esses números.

Isso não é para operadores experimentais, mas aqueles que atendem centos de nomes de domínios. Por exemplo, o Reino Unido, ccTLD na China, apenas para mencionar alguns.

Então, veremos o sistema de registro que são as bases de dados que guardam os domínios dentro dos TLDs. Vemos dois modelos. O primeiro dos modelos completamente é FOSS. Existe, não a maioria, mas apresenta do que é possível. E é um ponto importante isso.

O modelo mais popular é onde estão os registros com propriedade exclusiva. Mas aqui podemos ver que esses sistemas de propriedade exclusiva não começam do zero. Mas são integrações que correm por cima das plataformas com software livre de código aberto. Ou seja, incorporam elementos de FOSS. Então, se bem falamos de propriedade exclusiva, o fundamento, a base, é FOSS.

Agora vamos falar, então, do ecossistema dos resolutores, que é mais difícil. Aqui vemos, sim, que há um grande uso, uma presença

fundamental do software livre de código aberto. 80% dos usuários de todo o mundo utilizam o resolutor local. E aqui, FOSS é quem domina. Inclusive, quando vemos as soluções comerciais, e sabemos que existem muitas, a maior parte das situações, do que vendem são FOSS. A mesma coisa aplica para os resolutores públicos. Muitos deles são FOSS.

E fizemos, por exemplo, em um estudo em Clouflare, onde tem um núcleo de propriedade exclusiva, mas que está rodeado por FOSS. Então, também temos que os hiperescaladores mais importantes utilizam FOSS para a resolução do DNS. E outros utilizam a biblioteca do FOSS, como resolutores. Passemos agora, ao seguinte slide.

O que podemos mencionar, então, do relatório é que, nas partes mais críticas da infraestrutura do DNS, FOSS é a norma, e o software de propriedade exclusiva a exceção. E não é exagero isso, que estou dizendo. Mas é o que nós encontramos na pesquisa rigorosa que fizemos. Também podemos falar de sistemas de nomes, que têm o software desenvolvido de forma colaboracionista e distribuído de forma gratuita. Seguinte slide, por favor.

Ora bem, a abordagem regulatória para a cadeia de fornecimento tradicional impõe algumas condições em termos de segurança e normas. E as impõe aos operadores da infraestrutura crítica. E, em geral, os considera responsáveis em caso haja falha e requisitos que se estabeleceu aos fornecedores através dos contratos. E com

FOSS, supostamente, pode não haver uma relação de fornecedor no sentido tradicional.

Não há um contrato de operação. Não há um fornecedor com o qual estabelecer uma regulação. É algo voluntário. Supõe-se que esse é o modelo de fornecedor e cliente, com transações financeiras. Isso no modelo tradicional, mas aqui não há.

Impondo um encargo de cumprimento sobre os operadores sem afetar a cadeia de fornecimento e pode levar a uma desestabilização das pequenas instituições. E podem utilizar a possibilidade de abandonar seu projeto, mudar de licença proprietária ou evitar algumas jurisdições. Então, o software do qual todos dependem está menos disponível e é menos seguro.

Então, fizemos alguns estudos de caso em algumas jurisdições, como nos Estados Unidos, Reino Unido, União Europeia. Desenvolveram políticas que levam em conta FOSS. E eu não vou entrar em detalhes. Mas se pode fazer, é possível fazer.

Ora bem, essas são as cinco diretrizes sobre as quais é possível agir e que nós desenvolvemos. SSAC é indiferente, se vocês querem regulamentar ou não. Temos posição... não temos posição. Mas se vocês querem aplicar regulações, considerem o papel crítico que tem FOSS. Reconheçam, que a estrutura global depende e que é necessário que se preserve.

E também consultem com a comunidade de código aberto, falem com as entidades encarregadas da manutenção, com os

desenvolvedores de políticas. E evitem as consequências não intencionais.

E utilizem casos contemporâneos para entender, quais são os efeitos nos modelos emergentes, encorajem a sustentabilidade do FOSS. E abordem os riscos sistêmicos, que existem no espaço de software em geral, não só em FOSS, de forma coletiva.

Encontrem soluções para todo o ecossistema em lugar de colocar a encargo nas entidades de manutenção individuais.

Eu acho que com isso chego ao final da apresentação e espero as suas perguntas.

MARCO HOGEWONING Obrigado, Maarten, por essa apresentação tão completa. E também Ram, agradeço e encorajo a que leiam o relatório mencionado antes.

Temos tempo para algumas perguntas. A primeira é feita por alguém que está aqui, ao meu lado.

NICOLÁS CABALLERO, PRESIDENTE DO GAC Vamos para a Comissão Europeia.

GEMMA CAROLILLO Obrigado, Sr. Vice-presidente, Presidente. Se o presidente quer falar antes, pode fazê-lo. Sou Gemma Carolillo, da Comissão

Europeia. Sou daqueles que estão recebendo essa informação com 3 dos 4 estudos de caso.

Isto é extremamente importante para nós. E nós, como entidade reguladora, aprendemos ao longo do processo a respeito de como incorporar as diferentes características do código aberto na regulamentação sobre questões digitais. Foi um processo doloroso. Mas também muito útil, e a aprendizagem coletiva, estamos obtendo bons resultados pelo momento.

A minha pergunta tem a ver com a segurança da cadeia de fornecimento. Porque isso continua sendo um problema, mesmo quando tentamos evitar, continua sendo um problema. Tem alguma posição com relação a iniciativas ou com respeito às listas de materiais para software? E como isso poderia abordar a questão da segurança na cadeia de *suministro* ou de suprimento, fornecimento?

MAARTEN AERTSEN Obrigado, Gemma. Está perguntando se a SSAC tem uma opinião sobre a lista de materiais de software. Infelizmente, falando em nome do SSAC, não analisamos essa medida em particular. Posso compartilhar minha opinião pessoal, mas é só pela minha conta.

Se houver um problema no espaço de software com a segurança, quando falamos de software proprietário de código aberto, acho que a lista de materiais de software pode nos ajudar quando alguém, uma organização adquire software que é proprietário. Mas principalmente está construído com base em FOSS. Aí é onde

entramos em situação, onde um componente é vulnerável, e é vulnerável para todos, inclusive para os produtos que estão no mercado. Se não sabemos o que está dentro, como fornecedor ou comprador, como pode começar a corrigir as coisas? Então, é um instrumento interessante nesse sentido.

Também está nas suas primeiras fases. E agradeço pelo comentário sobre aprendizado coletivo. Eu estou falando agora por mim. Mas acho que é fascinante ver o processo de desenvolvimento de políticas, como se deu na União Europeia. E estou muito contente de que tenhamos um estudo de caso, que possamos incluir no relatório.

MARCO HOGEWONING Obrigado, Comissão Europeia e Marco. Passo a palavra para Bangladesh. E vou fechar as intervenções com o presidente.

DR. SHAMSUZZOHA Obrigado pela apresentação tão completa, principalmente sendo de uma organização, que trabalha com diferentes organismos de normalização em Bangladesh. Acho que é muito interessante.

E em dois sentidos. De um lado, trabalhando com o ccTLD de Bangladesh, com as normas de segurança para garantir de ter o software certo. E, em segundo lugar, colaboramos com aqueles que se encarregam da infraestrutura crítica, vendo as soluções que podemos ter para a cibersegurança.

E considerando o sistema de compras no governo, estamos promovendo a compra de software de código aberto. Um dos argumentos colocados tem a ver com a capacidade inerente do FOSS, no que diz respeito às mudanças. Se a gente não tem capacidade para fazer as modificações, esse é um grande risco para toda a infraestrutura nacional e pode nos levar a um grande custo.

Queria saber como vem o tema da infraestrutura crítica sensível nesse sentido?

MAARTEN AERTSEN

Nesse sentido, eu acho que há menos diferença entre o software proprietário e o FOSS. E é menor a diferença, do que a gente esperaria. Se operarmos a infraestrutura crítica, o operador tem a responsabilidade de fazer que tudo funcione de maneira interrompida. É o que a maior parte decide, na realidade. Então, tem um conhecimento interno, que representa um custo, tem que contratar especialistas ou tem que encontrá-los em outra parte. Em muitos casos, se vocês virem, o software mais popular, essas organizações estão financiadas através de contratos para dar suporte.

Se apenas falamos de software proprietários, talvez pagaria um custo pela essência e, possivelmente, receberia um suporte. Acho que não há grande diferença nesse sentido, eu acho, considerando todas as fortalezas, que se viram na apresentação.

Podemos ter uma diferença, que não tenha que se amarrar a um só fornecedor, mas infraestrutura técnica especial, onde existem

esses requisitos. É necessário conhecimento especializado, experiência, cada operador pode escolher dependendo da sua largura de banda dada pelo governo e para tomar essas decisões.

MARCO HOGEWONING Obrigado aos dois. Vou passar a palavra para Nico, que é um grande defensor de FOSS.

NICOLÁS CABALLERO, PRESIDENTE DO GAC Vou ser muito breve. Obrigado, Maarten, por essa apresentação. Pode fazer um comentário sobre como o código aberto evita essas situações, nas quais estamos amarrados a uma determinada entidade, principalmente os países em desenvolvimento. Não só do ponto de vista do custo, mas do ponto de vista... Bom, eu vou dizer assim, os custos de cibersegurança.

MAARTEN AERTSEN Bom, estar amarrado a um fornecedor significa, que a gente decide investir num certo produto e depois não pode migrar. Porque o investimento feito é grande demais. E as mudanças ou os custos para modificar, mudar de fornecedor são muito altos.

Inclusive na cibersegurança, quando a gente fica amarrado a um determinado fornecedor, não está obrigado a manter a relação com a entidade de manutenção original. Às vezes há outras organizações que podem dar apoio à implementação, principalmente para a operação de *patches*.

Mas sempre vai depender do original, do fornecedor original. Não é como no caso do software proprietário, onde só há uma entidade com a qual tem que trabalhar. Então, talvez um país com orçamento menor poderia ver isso como um impulso à inovação para desenvolver esse conhecimento especializado, em lugar de ter que pagar a outras entidades fora do país. Mas suponham que isso é algo que devem escolher.

Mas é isso que posso dizer com relação a estar amarrado a um fornecedor. Essa é a minha opinião pessoal. Porque não fazemos referência a isso no relatório.

MARCO HOGEWONING Obrigado, Nico, pela pergunta. Obrigado, Maarten, pela sua resposta. Acho que, por questões de tempo, vamos passar para a seguinte parte, o seguinte tema. Então, quero dizer que convidamos o SSAC, para que também nos ajudasse a desenvolver isto e para benefício dos membros mais novos do GAC, que estão aqui na sala. Essa é uma questão relativamente nova, mas está adquirindo a cada vez mais importância na medida em que nos aproximamos da próxima rodada. Então, vou passar a palavra para Suzanne.

SUZANNE WOOLF Obrigado, Marco. Obrigado, Maarten. Sempre é um prazer falar depois de você. Como disse, Marco, eu tenho que trabalhar sobre a colisão de nomes. Porque eu estou encarregada do projeto de análise de colisão de nomes, que foi algo originalmente proposto

por SSAC. Mas depois foi desenvolvido por um grupo em toda a comunidade.

Como disse, Marco, primeiro tínhamos alguns desafios com a colisão de nomes, devido à rodada anterior. Mas tivemos que revisar rodada anterior, mas tivemos que revisá-lo. Porque eu vi algumas coisas, que mudaram a partir da tecnologia e as expectativas e o ecossistema, no qual devemos nos deslocar.

Então, o que é uma colisão de nomes? É difícil definir a colisão de nomes. São essas coisas, em que é difícil identificá-lo rapidamente. Podemos pensar numa analogia dos nomes de domínio, como endereço de uma casa. Se uma casa ou duas têm o mesmo endereço, é difícil entregar o correio, o produto de mercado e a questão de segurança. Vejam as consequências da segurança.

Então, no DNS, colisões de nome, é quando há um domínio utilizado no espaço global de nomes de DNS, se usam outros nomes. Por exemplo, uma empresa privada pode ser um fornecedor de VPN, onde são utilizados diferentes nomes que são válidos. Mas se é o mesmo nome, o que a gente procura pode ser interpretado de forma errada e gera confusão rapidamente. E os próximos slides.

Vou passar rapidamente, vou evitar detalhes para chegar a falar em nível geral, mas essa apresentação está disponível e depois poderemos entrar nos detalhes, quando vocês quiserem.

O que é que não é uma colisão de nomes? Alguns dos termos podem ser... É possível que vocês conheçam. Porque viram no Guia

do Solicitante. A colisão de nomes, não é o mesmo que uma similaridade em cadeias de caracteres ou cadeias de caracteres confusamente similares.

Ele é um problema técnico que gera questões de segurança e estabilidade. Porque se delega exatamente o mesmo TLD, que se utiliza em um contexto privado. Por exemplo, EXAMPLE.COM pode ser SAMPLE.COM, numa internet aberta. E os riscos são, então, que as consultas pelos nomes privados podem filtrar-se ao DNS público.

Então, aparecem conflitos técnicos e de segurança. A semelhança das cadeias de caracteres também é um desafio para o Projeto de Novos gTLDs, Guia do Solicitante ou Manual do Solicitante. Mas também tem a ver com a percepção do usuário. Então, isso tem a ver com a possibilidade de confusão através de diferentes TLDs públicos, que podem se ver iguais, conforme... Aqui temos o .exaMple com M minúscula e um .examplE com E maiúscula. Isso pode ser confuso para o olho humano. Então, aí temos possibilidades de falhas de confiança, *phishing*, fraudes, e isso impacta nos usuários.

Então, o que temos que lembrar é que sempre há temas de colisão que podem gerar, e a questão é que, quando o computador confronta essas semelhanças, podem existir, então, resultados perigosos e confusos. Por esse motivo, deixando os detalhes técnicos de lado, devemos entender que a colisão de nomes é importante para a segurança da Internet e que tem a ver com a

responsabilidade da ICANN, para o que é a estabilidade, segurança e resiliência da internet. Há consequências, quando as empresas utilizam nomes nos níveis internos, que podem filtrar a Internet global.

Também, se temos mais que TLDs, temos mais chances de ter esses problemas. Porque há mais nomes que podem estar sendo utilizados em contextos privados. Mas que também podem se delegar ao espaço de nomes públicos.

Medir a colisão de nomes é difícil. Porque há uma infraestrutura de rede de tecnologia, que vai evoluindo especialmente, quando falamos da Última Rodada de gTLDs. Existiram melhoras na privacidade do DNS, o que torna mais difícil o que está acontecendo. Porque tudo tem a ver com as melhoras da privacidade e também o sistema de nomes alternativos, que fizeram com que o panorama do DNS, seja mais complexo e mais difícil de medir. Então, não era brincadeira, quando se falava que... por favor, um slide para frente. Sim. Obrigada.

Em 2012, houve uma Nova Rodada de gTLDs, que acelerou o crescimento, que disse “Bom, o que vai acontecer, quando se adicionem novas cadeias de caracteres, que já talvez estivessem sendo utilizadas em outro contexto, que não seja o público”.

Em 2013, a SSAC tomou esse tema e emitiu uma recomendação destacando os problemas significativos de segurança e estabilidade, que podiam resultar da colisão de nomes.

A colisão de cadeias de caracteres mais importante detectada foi no caso de .HOME, .CORP e .MAIL, que foram utilizadas no contexto privado. E houve muitos dados, muitos riscos para identificá-las e tratar de delegá-las no sistema de nomes de domínio público.

Em 2017, a Diretoria da ICANN pediu à SSAC, que realizassem estudos amplos para permitir as possíveis, futuras delegações de gTLDs de uma forma previsível, segura e estável.

E apareceram dois projetos que surgiram nessa época. E também geraram algumas outras perguntas. E na etapa final, tivemos o Exame 2 da NCAP, publicado em 2024. Porque nós queríamos ter a certeza de que os achados encontrados podiam se unir e aparecerem recomendações para fazer parte da Próxima Rodada de Novos gTLDs.

Tínhamos uma equipe de toda a comunidade, não só membros do SSAC. Isso, obviamente, funcionou muito bem para nós, foi bom. Mas, claro, isso levou mais tempo anterior, com pesquisas mais recentes. O que temos que tirar do projeto NCAP é analisar a situação atual, que tinha a ver com lutar e mitigar a colisão de nomes e também pensar em tudo isso para a Próxima Rodada. Isso também tinha a ver não só com ver qual era a colisão de nomes, mas também quais eram as medidas possíveis a tomar para evitá-lo.

Temos que mencionar também, que a avaliação foi muito mais difícil por diferentes motivos. Estamos falando disso, não é. Mas o mais difícil é a quantidade de nomes nos dados, que são

procurados. Isso também tinha a ver com aqueles que se utilizam no âmbito privado. Isso pode ser bom para os usuários, mas não tem a ver com os esforços, que nós estamos levando.

Houve grandes desafios no caminho, mas conseguimos trabalhar com os elementos, que tínhamos e conseguimos também cumprir os objetivos.

O Número 1 era garantir que podia ser avaliada a colisão de nomes. E também agora temos um quadro, uma agenda, uma situação de nível de análise que pode ser escalada, quantos detalhes para ver o que está presente dentro de determinadas colisões de nomes.

E o Objetivo Número 2 é dar um processo à ICANN, para ver planos de mitigação e remediação, em caso de colisão de nomes. O que vimos é que, mais do que no passado, todas essas experiências serão muito diferentes umas das outras.

Então, não vamos ter que prestar exame. Mas esse é o diagrama, que está no relatório e que surgiu do Exame da NCAP. Levar em consideração as colisões de nomes e, na verdade, os desafios que enfrentamos no futuro.

Também tem que existir uma equipe técnica para realizar uma revisão e enviar os relatórios, os resultados à Diretoria. Pensamos que em muitos dos casos não tem que existir um risco contínuo.

Porque a mitigação e a prevenção são possíveis. Mas, como não são iguais os dois casos, hipótese, precisamos de muitos elementos para saber, que estão sendo tratados bem o assunto de colisão de

nomes. Há uma coisa que tem a ver com meios automatizados e também podemos enviar isso a uma equipe de especialistas, que é o que utiliza a ICANN em outros elementos, onde os problemas podem se complicar, ficar mais difíceis. Então, precisamos de uma avaliação específica para informar e conseguir formar o processo.

Os benefícios, então, desta agenda de análise de risco de colisão de nomes, que seria o ponto 2 no NCAP, publicado para toda a comunidade, é que a função tem a ver com uma função de risco, como para identificar e permitir a remissão desses problemas de mitigação, antes que provoquem o dano. Que o marco, o quadro, a agenda, tentamos que trabalhar para que seja uniforme e eficaz, um enfoque centralizado para garantir uma avaliação de risco profunda e mitigação em todas as aplicações dos novos gTLDs, devido à responsabilidade também para a zona-raiz. Trabalhamos com a ICANN para isso.

O quadro, digamos, está dentro já da ICANN para determinar os espaços dos nomes da internet. E também conseguimos enfrentar várias das preocupações de privacidade. Porque se bem o risco é inerente à avaliação de colisão de nomes, o risco da privacidade, que encontramos... é que o risco de privacidade não pode avaliar com precisão e exatidão todas as colisões de nomes. E é maior do que os riscos associados com a avaliação. Então nós pensamos que o risco de privacidade de não avaliar exatamente a colisão de nomes é maior, que o risco associado com a avaliação.

Então, esse risco de agir em comparação com o de não atuar ou agir, isso dá uma ferramenta excepcional ou extra para analisar esse tipo de casos. Então, na verdade, a detecção precoce do risco e a mitigação informada são fundamentais para a segurança e estabilidade do DNS. E isso, então, é uma ideia geral, né? E não sei se temos perguntas, tempo para perguntas.

MARCO HOGEWONING Obrigado, Suzanne. Agradecemos muito, então. E não sei se... Eu acho que o tema da colisão, para mim, ficou um pouco mais claro para ver que colisão de nome não é igual a cadeia de caracteres semelhantes. Então, veremos se continuamos falando com a SSAC durante o ano todo. Então, não vejo ninguém. Nico, não sei se quer dar algumas palavras.

NICOLÁS CABALLERO, PRESIDENTE DO GAC Se podemos voltar para a página 23, por favor? Porque aqui há quatro etapas. E a minha pergunta tem a ver com os prazos. Como média, digamos, qual o prazo? Estamos falando de dias, semanas, meses. Porque eu queria comparar isso com as 32 etapas. Não sei se lembram, ontem, na apresentação com a GNSO, falamos da eficiência e da velocidade e de muitas outras coisas. Então, como média, como tempo médio. Quanto tempo levaria tudo isso?

SUZANNE WOOLF Bom, essa é uma pergunta que também debatemos, e ainda não temos um consenso sobre o que recomendar. Porque, como já

falaram, há pressões em uma direção de que isso seja o mais rápido possível. Mas nós também não queremos deixar de lado riscos importantes. Então, estamos pensando em semanas, meses, anos, enfim. Isso é uma questão que ainda temos que deixar para a comunidade, para que o pessoal tome a decisão final a respeito.

MARCO HOGEWONING Obrigado. Bom, eu acho que podemos assumir outra pergunta, mas não estou vendo o pedido de palavras. Então, obrigado, Susan, pela explicação.

Podemos passar, então, ao seguinte tema, que estará a cargo dos encarregados do uso indevido do DNS. Agora temos um documento de assuntos gerais. Então, vocês, os colegas do SSAC, podem compartilhar talvez algumas recomendações técnicas.

RAM MOHAN Obrigado, Marco. Antes de responder a sua pergunta, eu quero informar o GAC com respeito ao slide anterior sobre um trabalho que acaba de começar e que se vincula com o espaço dos nomes. Começamos com um grupo de trabalho, que se concentra na integração responsável do DNS no sistema de nomes de nomes. O que acontece com os identificadores em outros sistemas, quando se quer interagir com outros identificadores que estão em outro sistema? Então, começamos esse trabalho para começar também a reunir algumas conclusões. O que é verdade que nos preocupa é

o ciclo de vida do nome de domínio, a confusão dos usuários, a fraude, esse tipo de coisas.

A segurança, a estabilidade, riscos que poderiam introduzir no sistema do DNS, quando temos sistemas com outros espaços de nomes, que utilizam palavras ou nomes que são semelhantes aos nomes de domínio, que nós temos, mesmo que não sejam totalmente iguais. Começamos com esse trabalho apenas. Então, vamos mantê-los informados a respeito.

Agora, quanto à pergunta feita, Marco, estamos muito satisfeitos de manifestar que há um documento sobre política, um trabalho, pelo menos, que começou para desenvolver políticas referidas ao uso indevido do DNS.

Em anos passados, o que fez o SSAC foi fazer comentários e dar recomendações, depois de formadas as recomendações de políticos. Agora, mudamos o modelo em colaboração com os colegas da GNSO. Nos convidaram a estarmos representados nesse PDP, ou no processo de PDP, para ser mais preciso.

E não estamos participando nos debates sobre se é uma Via 3, 2, 2, de trabalho, todas as vias combinadas. Isso corresponde às pessoas que trabalham no desenvolvimento de políticas. Mas nós tentamos nos incorporar neste trabalho para falar de assuntos específico, que têm a ver com o uso indevido, apresentando as nossas observações. Especialmente, porque dedicamos muito tempo para ver a evolução do uso indevido e para onde está caminhando.

Então, estamos muito focados nessas áreas, achamos que é um assunto muito importante nas conversas que realizamos com a Diretoria da ICCAN, especialmente quando pensamos nas prioridades para 2026. Apoiamos também algumas coisas que estava falando a Câmara de Partes Contratadas da GNSO, quanto ao local prioritário, o lugar prioritário que tem que ter o uso indevido do DNS. Mas se tudo isso não é feito de boa maneira, não só serão afetados os usuários. Mas também a reputação desse Modelo Multissetorial que é autorregulável, que nós queremos apresentar como um grande exemplo.

Por isso, queremos nos concentrar em maior medida no uso indevido do DNS. Então, estamos envolvidos para participar ou em participar mais na etapa de desenho, mais do que fizemos em anos anteriores.

MARCO HOGEWONING Obrigada, Ram. É maravilhoso escutá-lo. Agora, me pergunto se as pessoas, que se encarregam mais do tema de uso indevido do DNS querem fazer alguma pergunta adicional para os membros do SSAC? Ou qualquer outra pessoa, é claro, que possa ter alguma consulta sobre esse assunto. Comissão Europeia.

JANOS DRIENYOVSZK Obrigado por estarem aqui conosco. Obrigado pelas suas apresentações. Eu me pergunto, com os PDPs, é importante ter o alcance certo, se investe muito esforço. Então, eu me pergunto, quais são as suas opiniões com relação ao trabalho sobre as

registrações maciças? Porque eu entendo que, no final de contas, queremos ter algo que tenha impacto.

E falamos das APIs. Mas eu me pergunto se essa abordagem vai abranger a maioria das tecnologias ou das medidas, que facilitem as registrações em grandes volumes. Não é mesmo? Acho que... Quero saber se vocês consideram que essa é uma boa abordagem ou deveríamos definir o escopo de forma tal, que fique à prova do que acontece no futuro?

Não sei se há uma resposta, se há alguma coisa técnica que possa existir e permita essas registrações maciças.

RAM MOHAN Há diferentes nuances nesta questão. Há motivos legítimos pelos quais se podem fazer registrações maciças. Uma empresa que quer proteger seu novo produto e registra centenas de produtos. E também podem se fazer registrações em múltiplos TLDs. Dentro do TLED há algumas coisas específicas.

O acesso por API não é a única forma para gerenciar as registrações maciças. Vimos muitos casos, nos quais pessoas com intenções ruins registraram, utilizando um modelo não baseado em API, onde podem se ocultar, porque nem tudo de API, se observa.

Mas, tendo dito isso, acho que esse é um bom âmbito para pesquisar. As registrações maciças têm que ser definidas. E uma das preocupações, que compartilhamos com outros integrantes da comunidade é que, se estabelecido um limiar, tudo quanto ficar

por baixo de um determinado número, não vai se submeter a um escrutínio de tal nível. Achamos que isso pode ser alcançado, mas há trabalho para fazer.

Eu confio em que poderia haver uma política gerada para estabelecer o âmbito adequado para o tipo de conduta, que queremos prevenir. Em lugar de ter métodos específicos através dos quais são realizadas essas atividades ou é executada essa conduta. Acho que essa é a distinção que queremos fazer com o Processo de Desenvolvimento de Políticas.

MARCO HOGEWONING Obrigado, Ram. Vejo que não há pedido para fazer uso da palavra, então tenho a oportunidade de fazer um comentário. Agradecemos pelas contribuições. Agradecemos tudo o que falou sobre o PDP. Continuamos fortalecendo o vínculo entre o GAG e o SSAC. Então, agora, acho que devemos responder essa pergunta. Onde podemos encontrar oportunidades para colaborar e fazer parte desse PDP? Talvez não haja um único caminho.

E vamos passar para o próximo slide. A Índia quer fazer um comentário sobre o uso indevido do DNS ou sobre o que eu acabo de colocar?

ÍNDIA Tem a ver com o uso indevido do DNS. Eu queria conhecer a opinião do Ram com relação a qual poderia ser a redução dessa janela de 15 dias para o WHOIS, do ponto de vista do uso indevido do DNS.

Acho que esse é um dos passos práticos que podemos levar adiante. Reduzimos significativamente, ou avançamos muito para trabalhar na mitigação dos indevidos do DNS.

E atualmente se apresentou essa modificação através da validação, verificação, que podia ter sido um desafio faz dez anos, mas agora se faz várias vezes diariamente. Por exemplo, entramos em um hotel, fazemos autenticação em um aeroporto também. Como poderiam permitir que uma pessoa, alguém tenha um nome de domínio? Nem sequer está verificando, apenas é uma autenticação.

Então queria que comente, qual é a sua opinião a esse respeito. Porque não entendo por que a janela deveria ser essa.

MARCO HOGEWONING Entendo que tem a ver com essas duas semanas, que se estabeleceram para verificação, não é mesmo?

RAM MOHAN Muito obrigado. Demos a nossa opinião sobre as Solicitações Urgentes de informação antes. E para ser breve, se realmente for urgente, tem que significar alguma coisa. Na nossa opinião, ali é requerida um tipo de resposta muito breve. É o equivalente de chamar um serviço de emergência na vida real. Quando chamamos um serviço de emergência, não esperamos ter uma resposta daí a 15 dias ou em dois dias úteis. Então a nossa abordagem é que isso é importante.

Mas com relação à pergunta da validação e verificação do SSAC, a partir do SSAC, não sei se necessariamente temos um ponto de vista compartilhado em todo o SSAC. Mas sabemos, sim, que existem pesquisadores em questões de segurança e algumas pessoas dos organismos de aplicação da lei, que dizem que se veem impedidos pela falta de acesso a alguma informação dos registratários ou não têm uma forma fácil de acessar. Então estamos promovendo o desenvolvimento de sistemas de acesso, que possam divulgar informação, aquelas partes que têm um interesse legítimo em acessar essa informação.

Então é aí onde estamos localizados com relação às Solicitações Urgentes. Principalmente quando o GAC e a Diretoria trabalham sobre esse assunto, tem que ter presente que a definição de dicionário de urgente e não... Não, tem que ter em conta essa definição e não se ater àquilo, que é comercialmente razoável.

ÍNDIA Eu quero saber o potencial de mitigação do uso indevido do DNS sobre a registração do domínio, essa janela de 15 dias sobre validação e aprovação. É algo que eu não consigo entender hoje.

RAM MOHAN Sim. Obrigado por esclarecer. Então, acho... Mais uma vez, não sei se posso falar em representação do SSAC. Porque isso é algo, que temos que analisar, precisamos analisar profundamente. Temos que ver qual é o prejuízo nos usuários, mensurá-los, compará-los contra outros requisitos contratuais e outros processos de

desenvolvimento de políticas. Mas, sim, temos nessa área, que pensar principalmente no prejuízo.

MARCO HOGEWONING Obrigado, Índia. Obrigado, Ram, SSAC. Há alguma outra pergunta? Ficam dois minutos. Então, poderia começar a encerrar a sessão, porque sei que é o que se interpõe com o café. Mas como podemos continuar falando no futuro? Nico, disse que tem uma pergunta.

NICOLÁS CABALLERO, PRESIDENTE DO GAC E seria parte desse pacote, isso do Código Aberto, porque no último IGF, no governo da Noruega, bom, basicamente compartilhou diferentes soluções. E há mais de 45 países, que estão se beneficiando disso neste momento. Então, qual seria a forma, caso nós tenhamos algum distinto colega do GAC, se há algum interesse, para ver de que forma cooperar nesse sentido? Qual seria o procedimento?

RAM MOHAN Eu acho que podem entrar em contato comigo, como Presidente ou todo o excelente pessoal do SSAC. Porque nós vamos promover o diálogo e encontrar a melhor forma para poder dar o conteúdo e qualquer outro tipo de apoio a vocês e trabalhar também junto com vocês. Para aqueles que são interessados nessa área, esse é um dos poucos relatórios do SSAC, que está com essa ideia. Então, nós quisermos fazer esse trabalho para vocês. E é por isso que, se

	vocês querem trabalhar conosco, podemos validar e fazer esse tipo de trabalho para trabalhar com vocês. É bom.
MARCO HOGEWONING	Obrigado, em verdade. Muito obrigado, Ram, Susan, Maarten, Sarah. Muito obrigado por estarem conosco. E espero, como líder do tema, da questão, continuar com a colaboração do futuro. Não sei se há algum tipo de comentário final.
NICOLÁS CABALLERO, PRESIDENTE DO GAC	Não, somente temas administrativos. Temos uma pausa para o café e nos reunimos novamente em 16h30. Com isso, damos por encerrada a sessão.

[FIM DA TRANSCRIÇÃO]