ICANN84 | Reunión General Anual – Debate del GAC sobre la mitigación del uso indebido del DNS
Martes, 28 de octubre de 2025 – 13:15 a 14:30 IST

JULIA CHARVOLEN

Bienvenidos a la sesión del GAC sobre mitigación del uso indebido del DNS del martes 28 de octubre a las 13:15 UTC. Esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN, el código de conducta de la ICANN y la política antiacoso de la ICANN.

Durante la sesión, las preguntas y los comentarios se leerán en voz alta si se incluyen en el formato adecuado en la zona de chat de Zoom. En esta sesión hay interpretación en los seis idiomas de Naciones Unidas y portugués. Si quieren hablar durante la sesión, levanten la mano en la sala de Zoom y digan su nombre para los registros y el idioma en que van a hablar en caso de que no hablen en inglés. Por favor, hablen a una velocidad razonable para permitir una interpretación correcta. Ahora le doy la palabra al presidente del GAC.

NICOLÁS CABALLERO

Gracias, Julia. Bienvenidos a todos. Espero que todos hayan disfrutado del horario del almuerzo en esta hermosa ciudad de Dublín. Tengo el placer de presentarles a nuestros oradores invitados en el día de hoy. Tenemos a Edmon Chung, de DotAsia. Jo-Fan Yu. Espero haber pronunciado bien su apellido. De TWNIC.

A quien no veo es al señor McDermott. Supongo que va a llegar en breve. Muchísimas gracias. Bienvenidos. Tómense su tiempo. No hay ningún apuro. Los líderes del tema del GAC para este tema que es tan importante para nosotros, que es la mitigación del uso indebido del DNS van a ser Martina Barbero, de la Comisión Europea, Susan Chalmers, de Estados Unidos, y el señor Tomonori Miyamoto, de Japón. Una vez más, muchas gracias. Le voy a dar la palabra ahora a Tomo precisamente. Él nos va a dar una introducción y recordarnos cuáles son los objetivos y de qué forma estos están vinculados con el plan anual del GAC, etc. Tomo, le doy la palabra.

TOMONORI MIYAMOTO Muchísimas gracias, señor Presidente. Bienvenidos a la sesión de mitigación de uso indebido del DNS. Soy Tomonori Miyamoto, de Japón. Este es el temario para esta sesión. En primer lugar vamos a hacer una introducción, que va a estar a mi cargo. Después vamos a tener una presentación del país anfitrión, a cargo de Declan, gerente de asuntos legales de .IE. Después vamos a ver cuál es el avance que se está dando en cuanto al tema de uso indebido del DNS y el desarrollo de política, que lo va a tratar Jorge Cancio. Después también va a haber presentaciones a cargo de otros miembros.

Voy a dar parte de los antecedentes. Ustedes saben que el tema del uso indebido del DNS es muy importante para el GAC. Creo que muchos de los colegas que están aquí están familiarizados con los

programas implementados en cada uno de sus países. También es un tema para las partes interesadas, porque nosotros lo hemos visto en la ICANN. Hay muchas sesiones que están vinculadas con el tema del uso indebido del DNS.

Sobre la base del contrato con la ICANN, el RA y el RAA, que fueron modificados el año pasado, en 2024, que son los registros y los registradores de gTLD, deben presentar informes sobre el uso indebido del DNS. Lo que necesitamos señalar es que el uso indebido del DNS dentro de la definición de la ICANN está limitado a malware, botnets, phishing, pharming y spam, así como los mecanismos de entrega.

Muchos países tienen distintos problemas con el tema del uso indebido. Puede haber fraude y también están involucradas las autoridades de aplicación de la ley. En Japón, por ejemplo, el tema del malware también es un gran problema. Para la próxima ronda, tal como estuvimos hablando, tenemos que tener en cuenta este tema. También tener en cuenta cuál es la definición actual de la ICANN sobre el uso indebido del DNS.

El plazo en el que queremos implementar una nueva política es antes de la delegación de los nuevos gTLD. En segundo lugar, también tenemos que generar capacidad sobre la mitigación del uso indebido del DNS, compartir las mejores prácticas que puedan ayudar a otros en las iniciativas voluntarias que estén haciendo en cada uno de sus comités.

Hay distintos tipos de programas de uso indebido del DNS. Siguiente imagen. Algunos de ustedes quizá recuerden este gráfico porque aquí vemos cuál es el panorama de las comunidades pertinentes, donde tenemos el alcance del contrato de la ICANN, que es bastante limitado, como dije. Tenemos una definición y la definición tiene que ver con la relación entre la ICANN y las partes contratadas.

Aquí tenemos vinculaciones contractuales. Esto es bastante fuerte. El tema es implementar medidas que sean adecuadas en forma oportuna antes de la delegación de los nuevos gTLD. Por supuesto que necesitamos considerar también lo que tenemos dentro de una comunidad más amplia donde tenemos los registros, los registradores, los operadores de ccTLD y la cooperación con el resto de los aliados. Siguiente imagen, por favor. ¿Podemos pasar a la siguiente? Gracias.

Aquí también vemos el camino, cómo llegamos a la discusión actual del PDP. Esto está dentro del mandato de la ICANN, de la zona de incumbencia, para implementar la política. Tuvimos que ver cuáles eran los alcances de los PDP y algunos elementos importantes.

En noviembre de 2024, creo que muchos de nosotros nos acordamos del estudio INFERMAL, donde se sugirieron algunos factores, que son los que impulsan el uso indebido como pueden ser las API de conexión libre y algunos factores negativos que eran la verificación adicional de información de contacto.

En mayo de este año, NetBeacon emitió lo que llamamos el libro blanco, donde propuso PDP y habló de cinco elementos para el uso indebido del DNS. En el GAC los hemos debatido y ahora estamos hablando del PDP sobre mitigación del uso indebido del DNS, que se inició en la reunión pasada de la ICANN.

En este caso, lo que se le pidió es que la GNSO haga las preparaciones necesarias para iniciar entonces este proceso de desarrollo de políticas con un alcance un poco más limitado. Ahora vamos a la presentación del país anfitrión. Le damos la bienvenida al señor Declan McDermott, que está a cargo de la administración de ccTLD en el .IE.

DECLAN MCDERMOTT Bienvenidos a todos. Gracias. Soy el gerente de asuntos regulatorios del ccTLD .IE. Vengo de la parte de políticas. Yo no soy técnico. Esta no va a ser una presentación técnica. Si tienen preguntas técnicas sobre cómo mitigar el uso indebido, les pido que mitiguen sus expectativas respecto de lo que yo les pueda decir. Si tienen alguna pregunta para mí, también me la pueden formular en el pasillo. Si no tengo la respuesta, voy a procurarla.

El registro de .IE maneja el dominio .IE desde el año 2000. Todos los dominios que tienen que ver con .IE. Celebramos el aniversario número 25 hace un mes. Quiero enfatizar que tenemos un bajo volumen y bajas tasas de uso indebido. Tenemos registraciones de nombres de dominio que son unas 300.000. La mayoría son personas físicas. NetBeacon creo que publicó una imagen de cómo

eran los números de uso indebido de .IE. Tienen información completa al mes de agosto, que encontraron un caso detectado de phishing, si no me equivoco.

Digamos que la tasa de uso indebido es bastante baja. El volumen también. Eso lo hace la Federación de Investigación de Internet. Creo que llegamos a 0,05 % de uso indebido. En los últimos 365 días creo que subió en 100 instancias detectadas. Lo que yo quiero decir con esto es que si bien el registro es pequeño, comparado con otros, tiene una baja tasa de uso indebido, que creo que es lo que sucede habitualmente entre los ccTLD.

.IE también tiene un requisito específico que llamamos Connection to Ireland. Desde la creación de los nombres de dominio .IE, fue utilizado por personas u organizaciones dentro de Connection to Ireland. Esto tiene cuatro categorías: personas que residen en Irlanda. Pueden ser ciudadanos de Irlanda que viven en el exterior o pueden ser organizaciones con base en Irlanda, con un número CRO. Pueden ser organizaciones fuera de Irlanda que brindan servicios o venden cosas a Irlanda.

Estas son las cuatro categorías que están vinculadas con Irlanda. Según entiendo, no sé si alguien tiene un requisito exclusivo. Creo que ningún otro registro tiene un registro como Connection to Ireland, esta conexión con Irlanda.

Cuando hablamos de uso indebido, lo que queremos decir es que .IE tiene una imagen más amplia de lo que la ICANN considerada un uso indebido del DNS. Nosotros tratamos de dividirlo en tres

categorías. Uno tiene que ser el uso indebido técnico, que incluye malware, phishing, botnets. Esto tiene que ver con lo que la mayor parte de la gente llama uso indebido del DNS pero nosotros también hablamos de uso indebido del contenido, que pueden ser prácticas ilegales o contenido ilegal, como puede ser fraude o contenido sobre menores. Después, el uso indebido de registración, que es hacer registraciones de mala fe.

El mensaje principal que quiero dar es que estas definiciones son importantes desde mi punto de vista personal. Lo que resulta mucho más importante es que tenemos distintas medidas que pueden proporcionar una respuesta adecuada dependiendo de la situación. No es adecuado para que un registro empiece a definir si es un delito o si es algo ilegal o si es mala fe pero, sin embargo, si hay un juez, un regulador o un árbitro que diga: “Esto es ilegal o esto es mala fe”, entonces tiene que haber medidas implementadas como para responder a esas decisiones que sean necesarias y proporcionadas.

Me gusta esta sigla que es ATOM: Medidas Técnicas y Organizativas Adecuadas. Esta es una lista que no incluye a todas las medidas que tenemos en .IE pero lo que quiero señalar aquí es que nosotros creemos que es necesario tener estas medidas organizativas y técnicas porque no creo que exista la bala de plata. Una sola cosa que pueda evitar absolutamente todo. Puede haber suspensiones de nombres de dominio o medidas de gobierno, regulación. Creemos que todos son instrumentos y es como un martillo. Es muy necesario cuando lo necesitamos pero si quiero usar un

martillo nada más que para hacer un nido, seguramente no me va a resultar útil. Es por eso que necesitamos distintas herramientas e instrumentos para tener un enfoque mucho más amplio. Algunos de ustedes vienen del ámbito de la ciberseguridad y quizá necesitamos controles preventivos. Me gustaría utilizar otro marco también que es de otra vida de política. Creo que viene de la salud pública. Siguiente imagen, por favor.

En el mundo de la salud pública en general hablamos del tema de prevención o mitigación, pero prevención es utilizar intervenciones adecuadas para detener algo malo, para que esto no suceda en la salud de la comunidad o en el ecosistema o en una población. Esencialmente, como dije, es un nivel fundamental que habla de la prevención. Hay una intervención, que es necesaria y proporcional, para detener un efecto adverso, para que este efecto adverso no suceda. Hay distintas capas obviamente.

Esto viene de la salud pública pero me parece que se aplica a distintas áreas de política como yo lo puedo ver en lo que tiene que ver con las evaluaciones ambientales. Tiendo a utilizar este marco cuando hablo de las distintas medidas para mitigación y control.

Estas son distintas capas. Primero, la prevención primaria porque es encontrar un problema y detenerlo antes de que se transforme en un riesgo. Es decir, detener el tema o trabajar desde los 30 para evitar lo que puede suceder a los 60. Después tenemos el nivel organizativo, que es tener las políticas, las buenas prácticas de gobernanza en el ámbito gubernamental. Ver si los entornos

regulatorios o de leyes pueden ayudar a cumplir el objetivo. Si el objetivo es aumentar la seguridad, la ciberseguridad, las leyes o las regulaciones están obligando a los registradores a hacer cosas o a no hacerlas para que todo sea más seguro. Si queremos mejorar la protección de datos, ¿existen distintas políticas o regulaciones que estén implementadas para que las organizaciones hagan cosas que protejan los datos personales? En última instancia, con la prevención primaria, estamos viendo la imagen más amplia del sistema regulatorio para ver si ayuda a cumplir los resultados, si se trata de un instrumento adecuado, tenemos que tener esto y nada más.

La prevención secundaria está más cerca del problema porque es detener una amenaza que puede ser inminente. Podemos hablar de las primeras etapas de una enfermedad. Hay algunos síntomas detectados. Detectamos el problema y tenemos una respuesta rápida para que esto no empeore. En este contexto, si un sitio web se ve comprometido y se utiliza para hacer phishing, ¿hay sistemas que puedan detectar eso? ¿Hay procesos implementados para responder a eso? Si tenemos un ataque DDoS, como el Anycast, ¿existe algún control para detener ese ataque inminente?

Cuando hablemos de la terciaria es algo que ya se está dando. Por ejemplo, en el hospital hay un ransomware. Hay algo ilegal que pasó. Se trata de reducción del daño en este caso. Cuáles son los controles que están implementados para corregir o detener que este daño siga avanzando. En el ámbito de los nombres de dominio

pueden ser bajas, suspensiones de dominios si son necesarias y proporcionales.

En el último, que yo creo que la gente ni siquiera lo piensa en la salud pública, es la prevención cuaternaria, que habla de evitar las intervenciones inadecuadas. Si la prevención secundaria tiene que ver con evitar falsos negativos, la prevención cuaternaria habla de evitar falsos positivos. Intervenir cuando no necesitamos intervenir. Intervenir de una manera que no es proporcional a la situación o intervenir de una forma en la que exista un desequilibrio con los derechos fundamentales o en una forma que realmente ni siquiera está enfrentando el tema del dominio. Es por eso que necesitamos este tipo de medidas implementadas para ver cuáles son las revisiones de políticas, las evaluaciones del impacto regulatorio, etc.

Con .IE hacemos énfasis en que tenemos estas distintas medidas. Empezamos con las políticas y las prácticas más amplias, y luego comenzamos a entrar en estas medidas técnicas más detalladas. Lo principal que quiero transmitirles es que en forma individual, estas pueden tener distintas funciones pero todas van hacia el mismo objetivo, que .IE sea seguro y confiable.

A modo de ejemplo, brevemente, les quiero mostrar un protocolo que tenemos implementado. Tenemos una muy buena relación con los entes reguladores y los departamentos gubernamentales, con los colegas en esos organismos. Creo que el protocolo de la autoridad reguladora es un muy buen ejemplo.

Este es un protocolo donde, si tenemos un ente regulador, un organismo de la ley, que ha señalado que puede haber un problema, que alguien dice que es arquitecto pero no lo es, y esto infringe una ley. El ente regulador de los arquitectos dice: “Esta persona no es arquitecta”. Tenemos que tomar alguna medida. En ese caso tenemos una verificación de antecedentes, de debida diligencia donde examinamos esa solicitud. Vemos qué es lo que están pidiendo y si tenemos los fundamentos jurídicos, si tenemos suficiente información, para tomar una decisión respecto de que lo que están pidiendo es necesario y proporcionado. Nos han dado la información adecuada que la ley establece que nos tienen que brindar para esto.

Si vemos que sí, que es una solicitud proporcionada, lo que ocurre es que el registrador y el registratario reciben una notificación del caso. Si no es una situación urgente, el registratario tiene una cierta cantidad de días para resolver esa cuestión. Se les da la información de contacto del ente regulador en caso de que tengan preguntas las pueden hacer directamente porque en última instancia, lo que queremos evitar es ponernos nosotros mismos en esa posición de jueces. Esto hay que darlo de baja. Nosotros queremos ser este canal a través del cual el ente regulador cuando tiene un problema pueda ponerse en contacto con la persona con la que tiene ese problema y de esa manera puedan resolver la cuestión.

Al finalizar ese periodo, si el ente regulador nos dice que tuvieron una respuesta insatisfactoria, dependiendo de la situación

podemos tomar una medida correctiva y esto podría ser, por ejemplo, la suspensión del nombre de dominio. Diría que casi siempre lo que ocurre es que el registratario dice: “No sabía” y hace esa modificación rápidamente y todo está bien.

Si hubiera una cuestión urgente, severa, una pesadilla que avizoramos, en ese caso los entes reguladores saben y los organismos de aplicación de la ley saben que si algo tiene que darse de baja de inmediata, tienen que recurrir al proveedor de hosting.

Si bien nosotros podemos suspender los nombres de dominio, podemos tener a alguien que puede tener todavía acceso a la dirección de IP sin eliminar el contenido. Los entes reguladores y los organismos de aplicación de la ley saben que tienen que recurrir a los proveedores de hosting. Yo no tengo conocimiento de que haya ocurrido alguna vez pero, si hubiera una necesidad urgente de darlo de baja y no funciona, pueden recurrir a nosotros y ver qué podemos hacer. Por lo menos podemos dificultarle el acceso. Toco madera. Por lo que yo sé, nunca ha ocurrido esa situación. Siguiente diapositiva, por favor.

Un último marco. También tengo el gusto de mostrarles a partir del sector sanitario de la salud pública, creo que esto es algo de interés. Se llama la escalera de la intervención. Muestra las distintas maneras en las que una organización o un gobierno pueden intervenir. Está según el nivel de invasión. Cuanta más invasión, más justificación, más proporcionalidad.

Comenzamos en la base donde básicamente no hay nada para hacer. En Irlanda casi toda evaluación de impacto regulatorio no hace nada. Es como la opción por defecto con la que hay que comparar. El gobierno tiene que demostrar por qué hay algo que deba hacerse.

Luego avanzamos y podemos tener una intervención que requiere que se provea información. Aquí nos protegemos del uso indebido del DNS o del phishing. Luego podríamos facilitar alguna elección como registro. Podemos elegir el DNSSEC o bloquear el DNS. Luego tenemos el cambiar por defecto. Por defecto no vamos a publicar la información personal en el WHOIS a menos que por algún motivo alguien diga sí, quiero que lo hagan. Tienen que consentirlo de manera explícita.

Luego empezamos a entrar en un ámbito más teórico, más complicado con lo económico, los incentivos, por ejemplo. Si alguien quiere que las organizaciones tengan mejor ciberseguridad, aquí tenemos fondos para lograrlo. Por otra parte tenemos desincentivos. Justamente es la otra cara donde aumentamos las auditorías para quienes no tienen algún tipo de acreditación como la ISO, por ejemplo.

Luego tenemos la elección restringida. Puede ser A, B, C. Esto es para los registros donde uno dice que tienen que identificar la información del registratario. Esto lo hacen dependiendo de la cantidad de los estados en los que estén. La última es la de eliminar la posibilidad de elegir. Es decir, si hay algo que hay que informar,

no hay elección. Si hay una orden judicial que dice que hay que actuar en contra de ese nombre de dominio, no hay opción.

Por ejemplo, en Irlanda tenemos una orden que puede solicitar o emitir un juez de bloqueo y básicamente, si estamos en una situación de vida o muerte, y si no está violando los derechos fundamentales de un usuario de Internet y el juez está convencido de que corresponde, el juez puede pedir emitir esta orden de bloqueo por un máximo de 21 días. Luego hay que solicitar otra. Es una orden de bloqueo de acceso. La opción más invasiva, la de eliminar las opciones, se utiliza en las situaciones más extremas. Estas herramientas en forma combinada pueden ser útiles pero si no corresponden pueden tener efectos adversos.

Los principales mensajes aquí para recordar son que la mitigación eficaz no basta con tener una sola herramienta sino que necesitamos distintas medidas organizativas y técnicas. Las intervenciones deben ser apropiadas, necesarias y proporcionadas. Nosotros vimos que la colaboración significativa dentro de los reguladores, los registradores y los registros es muy útil en estas situaciones y es muy importante evitar intervenciones innecesarias o exageradas. Gracias.

TOMONORI MIYAMOTO Muchas gracias, Declan, por su presentación. Por cuestiones de tiempo vamos a aceptar una o dos preguntas o comentarios. ¿Hay

alguna pregunta? No veo ninguna mano levantada por el momento. Sí, vemos que Bangladesh pide la palabra.

DR. SHAMSUZZOHA

Dr. Shamsuzzoha, de Bangladesh. Muchas gracias por esta buena presentación. Es muy interesante ver cómo se lleva adelante la operación del ccTLD aquí, en Irlanda. Tengo dos preguntas. La primera tiene que ver con este protocolo regulatorio. Entiendo que es más de naturaleza reactiva. Depende más de lo que les dan los entes reguladores. Las medidas para mitigar el uso indebido, por ejemplo, cuando se tiene que procesar información, ¿cuál es el proceso? Esa es mi primera pregunta.

La segunda es la siguiente. Si tenemos en cuenta la proporcionalidad del sistema, si algo es proporcionado o no, ¿cuál es el mecanismo que está utilizando .IE? ¿Hay un sistema obligatorio o simplemente se basa en la buena fe o es un proceso más administrativo?

DECLAN MCDERMOTT

Tenemos distintos mecanismos de revisión de política. Tenemos un comité asesor externo de múltiples partes interesadas compuesto por distintos registradores con el gobierno ocupando un lugar permanente y también representantes de organizaciones locales que intervienen en la comunidad de Internet de Irlanda. Ese es un mecanismo para revisar las modificaciones de política o cualquier cambio que sea sustancial tiene que pasar por este

comité asesor en materia de política para asegurar que no esté poniendo en desventaja a nadie o que esto esté alineado con los valores de .IE.

También está la opción en caso de que haya un cambio significativo de política, pueden someterse a una consulta pública como lo hicimos en el pasado cuando tuvimos algunas modificaciones sustanciales de las políticas. Con respecto a su primera pregunta, en última instancia, esto va a depender del contexto específico.

Puedo hablar en nombre de .IE. Es un registro pequeño. No tiene sentido para nosotros contar con una moderación de contenido proactiva. Creo que ni siquiera podríamos hacerlo según la legislación nacional pero creo que va a depender del contexto regulatorio en el que existe ese registro y es una cuestión de encontrar el equilibrio, cuánta exposición al riesgo uno está dispuesto a aceptar. Si nos fijamos en los datos estadísticos de cuánto uso indebido hay en .IE, realmente la exposición al riesgo es muy pequeña.

TOMONORI MIYAMOTO Muchas gracias por las preguntas. Vamos a pasar a las novedades sobre el PDP. Martina.

MARTINA BARBERO Voy a hablar tan rápido como sea posible sobre este tema porque ya sé que estamos demorados. Pasemos a la siguiente diapositiva.

Tomo ya mencionó que en Praga el GAC emitió texto en el comunicado donde se le asesoraba a la junta directiva y a la GNSO en realidad que tomaran todas las medidas preparatorias necesarias antes del próximo PDP.

Esto fue seguido por un informe de cuestiones preliminar sobre el PDP sobre mitigación del uso indebido del DNS. Esto se hizo en septiembre. Luego se presentó una respuesta y les quiero dar un indicio de lo que nosotros tomamos en cuenta como importante de esa respuesta del GAC.

Más que nada, vemos que se sugiere priorizar tres brechas en materia de política. Las API no restrictas, los controles de dominio asociados y los algoritmos generadores de dominios o DGA. Los primeros dos temas, las API irrestrictas y los controles de dominio vinculados, son adecuados para el fin que persigue la política mientras que el último no necesariamente se podría abordar a través de la política.

Luego, el GAC ofreció apoyo para los dos temas que mencioné, estos dos primeros, sobre las API y los controles de nombres de dominio asociados. EL GAC quiere priorizar mecanismos que permitan avanzar con la mayor rapidez posible.

También hemos señalado que el informe de cuestiones contiene otras brechas, otras diferencias que hay que tener en cuenta. Los dos PDP que probablemente se inicien van a hacer avances significativos para el uso indebido del DNS. Sabemos que este es

un tema multifacético, muy amplio, y estos dos PDP no van a alcanzar para tratar todo lo que atañe al uso indebido del DNS.

Luego tenemos otras cuestiones identificadas en el informe de cuestiones. El GAC señaló que hay algunos que son de particular importancia y esos los enumera en su respuesta. También se dijo que el GAC quería participar en los PDP pero para eso iba a necesitar más información sobre los métodos de trabajo y la posibilidad de alternar los participantes, porque esto es lo que ha hecho el GAC en otros procesos de PDP que funcionó muy bien. Pasemos a la siguiente, por favor.

Ayer hubo una sesión dirigida por la GNSO con la comunidad sobre los PDP previstos y quiero poner de relieve alguna de las cosas que se discutieron. Con respecto a la estructura de los PDP, parece haber ciertas ideas alineadas con respecto a tener dos PDP en lugar de uno solo pero muchos de los detalles con respecto a la carta orgánica, el funcionamiento, no se trataron ayer específicamente en el debate.

También hubo apoyo de la comunidad, de pensar dos veces antes de abordar los DGA como un tema que no tiene que ver con un PDP. Esperarían que hubiera un PDP al respecto de estos algoritmos. Luego, con respecto a las API y los nombres vinculados, hubo algunas dudas con respecto a las API irrestrictas. En general, hablábamos antes de registraciones masivas en lugar de API pero ahora parece que las API son una de las formas de registrar los

dominios en forma masiva. De esa manera no resolveríamos el problema que querríamos resolver.

Con respecto a los nombres de dominio asociados, este parece ser un tema relativamente simple de abordar, aunque es importante mantener un buen equilibrio y aclarar qué controles se hacen según qué características, si es la identidad del registratario, el método de pago, mantener la transparencia en cuanto a posición de permitir que los registradores en particular utilicen un enfoque que no les dé a quienes quieren cometer uso indebido toda la información que necesitan para cometer dicho uso indebido. La siguiente diapositiva.

Esto apunta a sugerir que si estos PDP avanzaran, como es probable que ocurra en esta instancia con las cartas ya redefinidas, el GAC podría participar en ellos y según experiencias previas, algo que funciona muy bien… Perdón. Tengo que hablar más lento pero tengo que hablar rápido también porque tenemos poco tiempo. No tan rápido.

Algo que había funcionado en PDP anteriores fue tener un grupo reducido porque en el proceso de desarrollo de políticas, como saben, habrá uno o dos representantes del GAC más, posiblemente, algún suplente si se modifica la carta orgánica pero no todo el GAC puede participar. Sabemos que el uso indebido del DNS es un tema muy importante para muchos.

Una manera de asegurarnos de que todos los que estén interesados en participar puedan participar y hacer oír sus

opiniones es tener grupos más pequeños, por eso un grupo reducido o un subgrupo que prepare todo el trabajo sobre el PDP y, quien esté interesado, pueda participar e intercambiar con el representante del GAC en ese PDP. Esto funcionó muy bien para los datos de registración y creemos que podría ser el modelo que utilizaríamos para estos PDP. Pasemos a la siguiente diapositiva.

Esta es mi última diapositiva. Espero que podamos hablar un poquito. Tenemos tres preguntas para ustedes. La primera es si según las deliberaciones que mantuvimos en esta sala del GAC, pero también ayer con la comunidad, si hay algún mensaje adicional que deberíamos hacer llegar a la junta directiva, a la comunidad, con respecto a estos PDP desde el punto de vista de la estructura, el tema o ambos elementos. Nos pueden avisar potencialmente de qué les podría interesar, si estarían dispuestos a intervenir en las iniciativas de los PDP o en estos grupos reducidos porque querríamos saber quién estaría motivado para asumir este trabajo.

La segunda pregunta tiene que ver con el trabajo adicional que se tiene que hacer en términos del uso indebido del DNS más allá de los PDP. Tenemos una lista de posibles temas que todavía hay que tratar y si hay algún mensaje para transmitirle a la comunidad al respecto más allá de lo que se mencionó en el comentario público del GAC, esta es la oportunidad para que ustedes lo planteen.

La última pregunta, por supuesto, es más general. Si hay alguna otra consideración, algún otro tema que tengamos que tratar en

términos del uso indebido del DNS sobre la base de este informe de cuestiones preliminares, esta es la oportunidad para que ustedes presenten estos temas que quieran ver reflejados en estas deliberaciones. Nico, le doy la palabra para moderar lo que sigue.

NICOLÁS CABALLERO Muchísimas gracias, una vez más, por esta presentación tan detallada, Martina, Comisión Europea. Realmente este es un buen momento para que nuestros distinguidos colegas del GAC intervengan en lo que respecta a cualquiera de las tres preguntas que están aquí o cualquier otro tema. Alemania está pidiendo la palabra. Adelante, por favor.

RUDY NOLDE En primer lugar, gracias a los líderes del tema por esta excelente presentación. También por el trabajo que han realizado en estos últimos meses. Para Alemania el uso indebido del DNS obviamente que es una prioridad. En la ICANN nosotros también estaríamos contentos en cualquier capacidad que sea necesaria dentro del GAC para participar también en el grupo reducido. Somos flexibles en ese sentido.

Respecto de la segunda pregunta sobre las brechas en la política, me parece que es un poco más general y me gustaría o esperaría que el PDP o los PDP pudieran actuar como un punto de partida para un mayor trabajo. Analizar un tema y después rápidamente avanzar entendiendo que en la GNSO una vez que se abordan estos

dos temas hay más temas para seguir trabajando. No tenemos que decir: “Esperemos dos años para ver qué es lo que está sucediendo” sino poder ir tomando tema por tema uno tras otro. Estos son los comentarios que tengo para formular en este momento. Muchas gracias.

NICOLÁS CABALLERO Gracias, Alemania. Supongo que en este caso Alemania se está ofreciendo como voluntaria para la parte 1A de la pregunta. Es una broma, es una broma. Muchas gracias. Gracias, Alemania. Ahora tengo a Estados Unidos. No, perdón. India primero y después Estados Unidos. Adelante, India.

SANTHOSH THOTTINGAL Gracias, señor Presidente. Sí, nosotros estamos interesados en trabajar también en el PDP. También respaldamos este PDP con un alcance más acotado porque tiene que abordar temas de alta prioridad que fueron identificados en el informe de cuestiones preliminar, sobre todo lo que tiene que ver con el acceso a las registraciones masivas. Estos temas tienen que ver también con poder automatizar la registración sistémica. En la ICANN83 hubo un asesoramiento por consenso que tenía que ver con las acciones que se podían tomar sobre estos temas en el PDP. Gracias.

NICOLÁS CABALLERO Gracias, India. Tomamos nota. Ahora Estados Unidos.

SUSAN CHALMERS Respecto de la segunda pregunta, yo recuerdo una discusión que tuvimos hoy más temprano con ALAC sobre la transparencia y la presentación de informes donde se señaló que los requisitos para presentar informes de las partes contratadas en la actualidad no están en los contratos. Creo que hay un requisito para tener y mantener registros del uso indebido del DNS recibido por los registradores pero no para hacer una presentación de informes que sea pública sobre los informes de uso indebido cuando los han recibido y cuando han respondido a ellos.

Lo señalo porque durante la discusión intercomunitaria que fue una muy buena sesión, no está demás decirlo, se habló del cumplimiento para la verificación de los dominios asociados que podría ser eficaz desde el punto de vista del cumplimiento.

También hay un requisito de transparencia que puede ayudar al de cumplimiento. Es una intervención muy técnica pero creo que también tendría sentido para cumplimiento y también lo hemos indicado en el comentario que hicimos del GAC al participar desde el comienzo en todo esto. Gracias. Le doy la palabra a Finn.

NICOLÁS CABALLERO Gracias. Ahora tengo a Dinamarca.

FINN PETERSEN Muchas gracias por la presentación. Respecto de la pregunta uno, creo que también mencionamos que las API quizá pueden ser un

poco restrictivas y en general hablamos de registraciones masivas en el GAC pero no sé si podríamos darle el alcance al PDP para tratar de investigar cuáles son los otros métodos que una API, que puede estar dentro de este PDP de alcance acotado como para no tratar de resolver el problema incorrecto sino tener un PDP y que el resultado pueda implementarse de manera eficaz.

Por otro lado, cuando hablamos de la registración de nombres de dominio o los nombres de dominio asociados, yo veo que las verificaciones que van a realizarse son difíciles si empezamos desde cero, desde el principio. Por otro lado, si pensamos en qué hacer, tenemos que preguntarnos de qué forma cumplimiento puede analizar si están cumpliendo con el PDP o no.

Me parece que estas son otras preguntas que tendríamos que analizar. De qué forma, por un lado, no les damos la transparencia a los malos pero, por el otro lado, mantenemos los instrumentos necesarios para que cumplimiento de la ICANN pueda analizar y ver cómo están implementando este PDP ahora o en el futuro. Del lado danés, nosotros también querríamos contribuir al tema con cualquiera que sea el nombre que le quieran dar.

NICOLÁS CABALLERO Perfecto, Dinamarca. Tomamos nota. Perfecto. ¿Esto tiene que ver con la pregunta 1A? Perfecto, Finn. Ahora tengo a la Comisión Europea. Adelante, por favor.

GEMMA CAROLILLO

Gracias, Nico. Creo que en primer lugar tenemos que señalar que avanzamos mucho en los últimos años. No seguimos hablando del uso indebido del DNS porque ahora lo hablamos colectivamente. No es el GAC solo el que puede hacer algo sino que como comunidad hemos avanzado mucho. Por eso quiero expresar mi satisfacción al respecto.

En lo que respecta a la pregunta dos, porque la pregunta número uno me parece que no hay forma de escapar de ella, la Comisión ya es parte de los líderes de este tema, pero me quiero hacer eco de lo que dijo Susan, de Estados Unidos, y también Finn hizo referencia a esto. No se trata de ser brillantes sino de que el GAC ya estuvo en el momento de las enmiendas contractuales. Habló de la transparencia. Nos parece algo sumamente importante y me parece que esto no fue debidamente abordado en el momento de las enmiendas y quedó como una de las brechas de políticas porque también es parte del informe de cuestiones.

Hay otros dos elementos que fueron señalados en el informe de cuestiones como el uso de medidas proactivas preventivas. Nico hizo referencia a los algoritmos de detección. Este es otro trabajo. Esta es otra área de trabajo que deberíamos enfrentar y también en el informe de cuestiones se habla de la necesidad de hablar de la exactitud de los datos de registración, sobre todo en lo que tiene que ver con la validación con normas… Quizá me corrigió el presidente de la GNSO. Creo que se lo van a pasar ahora a la GNSO, que está hablando del uso indebido del DNS pero me parece que

hay mucha actividad que tiene que ver con este tema tan importante.

NICOLÁS CABALLERO Gracias, Comisión Europea. Sí. Realmente me pone contento el tema de los algoritmos pero también me preocupa porque tenemos que recordar que los malos también saben de la existencia de estas herramientas. No estoy hablando del ChatGPT o de la IA generativa o LLM. Estoy hablando de algoritmos muy sofisticados que hacen clustering, random forest. No voy a volver con esto, pero sí, tienen razón.

Sigue el micrófono abierto. No sé si alguien quiere hacer algún comentario, porque tenemos otros temas para abordar. No veo ningún otro pedido de palabra en la sala. Tampoco de los participantes remotos. Le voy a dar la palabra ahora a Susan, quien nos va a hablar del tema de los programas de notificadores confiables. Le doy la palabra a Susan.

SUSAN CHALMERS Como Tomo explicó anteriormente, es parte de los objetivos estratégicos del GAC en lo que tiene que ver con el uso indebido del DNS. Tenemos dos categorías generales. Una tiene que ver con el trabajo de política de la ICANN sobre el uso indebido del DNS. En ese sentido estamos alentando los PDP a que avancen.

En segundo lugar tenemos una sección de creación de capacidades y los líderes del tema han trabajado y vamos a seguir trabajando

para darles recursos a los representantes del GAC para que puedan aumentar su capacidad en este tema del DNS en general.

Ustedes pueden ver el uso indebido del DNS en general pero en la sección que ven aquí, 4.7, ven que la idea es darle mayor información y también habla de programas de notificadores confiables. Vamos a pasar entonces a la siguiente imagen.

Esta es una imagen conocida. Pueden ver que estos programas de notificadores confiables pueden utilizarse para abordar actividades de uso indebido del DNS que están por fuera del alcance de los contratos con la ICANN. En el día de hoy tenemos representantes de DotAsia y TWNIC, que están del otro lado de la mesa. Ellos nos van a hacer una presentación sobre sus programas de notificadores confiables. Les doy la palabra a ellos.

EDMON CHUNG

Gracias, Susan. Estoy aquí con Jo-Fan. Voy a hablar yo primero y después ella va a tener la palabra. Muchísimas gracias por recibirnos. Este es un tema que tengo muy presente. Vamos a hablar un poquito de historia. También creo que es muy importante si pasamos a la siguiente imagen, por favor, van a poder ver que esta es mi versión del diagrama que mostraron Tomo y Susan, donde aquí identificamos dónde se da el uso indebido del DNS, que muchas veces queda por fuera de la incumbencia de la ICANN. Vemos entonces que hay distintos componentes en la red.

Es por eso que concentrarnos nada más que en la incumbencia de la ICANN resulta insatisfactorio.

En la siguiente imagen tenemos otra visión porque aquí creo que sí nos hacemos eco de lo que dijo Declan anteriormente sobre una visión un poco más amplia del uso indebido. Aquí pueden ver cómo DotAsia lo ve. Tenemos los usos indebidos cibernéticos mayores. Hay algo más pequeño que llamamos uso indebido del DNS pero hay una parte aun menor que son los usos indebidos adecuados para los registros de dominios de alto nivel.

Esto está dentro de la incumbencia de la ICANN pero hay partes que están por fuera de esta incumbencia. Incluso lo que puede ver con CSAM y otros temas. Esta es la parte donde resulta interesante porque no es solo que tenemos que mirar. No tiene que terminar con un PDP de la ICANN.

Uno de los grandes ejemplos, si pasamos a la siguiente imagen, es nuestro trabajo con .KIDS. Esto comenzó antes de la última ronda. Sabíamos muy bien en ese momento que la misma política para .SEX quizá sea diferente que la política para tratar un uso indebido en el caso de .KIDS.

Hay algo muy interesante. Los registros comenzaron con la incumbencia de la ICANN como una línea de base para lidiar con el uso indebido pero no nos detuvimos ahí porque vimos situaciones donde iban mucho más allá y .KIDS es uno de esos ejemplos.

También quiero resaltar que cuando lanzamos .KIDS hace dos años, la plataforma de uso indebido del DNS y la tecnología que había estado dando vueltas en los últimos 15 años, resultaron muy instrumentales para permitirnos hacer cosas aun mayores para ir más allá en ese uso indebido y poner juntos una lista de observación como para hacer un seguimiento más profundo.

Como dije, ahí es donde empezamos. En el 2011. No sé si se dieron cuenta de que en ese momento sí tuvimos un foro sobre el uso indebido del DNS. Creo que fue el primero en el que participó DotAsia. Hemos estado trabajando en los últimos 15 años.

Aquí les quiero mostrar lo que tiene que ver con los notificadores confiables. Es en este punto, como mencioné, donde estamos tratando de ir más allá de los requisitos contractuales. Comenzamos con un enfoque de registro a registro. Nos podían notificar lo que estaba formalizado u otros registros formales y otros ccTLD y también otros gTLD. Empezamos con los ccTLD.

El motivo para los registros era porque queríamos mantener un nivel similar de sensibilidad de lo que podía ser la suspensión de un nombre de dominio. La capacidad de los registros de poder actuar por ejemplo en la suspensión de los dominios. Tiene un efecto mucho mayor. Queríamos entonces la misma sensibilidad de distintos registros para que ellos también pudieran analizar esto, pasarlo a nosotros en lo que nosotros llamamos una suspensión expeditiva.

Lo que se dio en los dos pilotos que tenemos en este momento con .TW y .UK y Nominet, es tener un canal de comunicación que es muy simple. Es un correo electrónico específico dedicado a esto donde compartimos las cosas. Sabemos que quien lo envía es una fuente confiable y pedimos un cierto formato de diligencia debida como para actuar rápidamente sobre esto.

Esto es lo que estamos realizando. Esperamos de aquí en adelante invitar a otros ccTLD a que se unan a nosotros. Puedo hablar de lo que pasó en el último año aproximadamente, donde estuvimos armando esto, pero en los últimos meses se transformó en una acción y existen dominios donde nosotros estamos recibiendo notificaciones respecto de esos dominios.

Una de las cosas que encontramos, que quizá lo sepan, pero lo que vemos en las situaciones de la vida real es que a veces hay phishing que tiene que ver con una región en particular. Si está dedicado a Taipéi, por ejemplo, alguno de nuestros sistemas de monitoreo no lo pueden captar pero eso sí puede ser captado por nuestros colegas en Taiwán.

Ellos sí pueden enviarnos la notificación y nosotros podemos abordar este tema. Es por eso que nos complace mucho poder trabajar con distintos ccTLD porque hay como un monitoreo de todos estos peligros y vemos cómo se puede trabajar en el ámbito internacional. Hay cosas que se nos pasan a nosotros porque pueden ser ataques o phishing que tiene que ver con una región geográfica en particular.

Habiendo dicho esto, quiero señalar que estamos explorando también otros aspectos que van más allá de la incumbencia de la ICANN. Hemos empezado con la definición de la ICANN del uso indebido del DNS pero estamos interesados en ampliar esta red de notificadores confiables a otros tipos de uso indebido. Es por eso que invitamos a otros ccTLD a trabajar con nosotros porque a través de ellos también conectamos con los cert nacionales o los equipos de respuesta nacionales. Esto nos permite también a través de los ccTLD mantener esta sensibilidad en el ámbito de los registros pero también hablar de los usos indebidos que van más allá de la incumbencia de la ICANN. Con esto termino mi presentación. Le doy la palabra a Jo-Fan directamente. Perdón, a Susan.

SUSAN CHALMERS: Perdón, Edmon. Debería haber hecho esta consulta antes de la presentación. Aquí tenemos a un representante de un registro que opera un gTLD y tenemos el CEO de TWNIC. Quería hacer esta consulta porque allí administran un ccTLD. Sin demorar la presentación de Jo-Fan Yu, ¿qué es un notificador de confianza? Creo que eso sería útil explicarlo.

JO-FAN YU: Hola. Buenas tardes a todos. Gracias por invitarnos. Estoy muy contenta de compartir esta información desde la perspectiva de un

operador de ccTLD y qué es el marco de los notificadores confiables.

Por qué pensamos que necesitamos un marco de notificadores confiables. Sabemos que hay amenazas del uso indebido del DNS que son locales pero pueden transformarse en algo global. También sabemos que hay una demanda pública cada vez mayor para tener una responsabilidad, una rendición de cuentas. Necesitamos métodos de respuesta más rápidos porque los tradicionales en general no son rápidos y se transforman en obstáculos. Necesitamos estos métodos rápidos, creíbles y transparentes.

También les quiero mostrar cuál es la perspectiva de nuestra parte. Nosotros recibimos notificaciones periódicas de nuestro gobierno sobre sitios web ilegales. Estos son datos del 2025 hasta el mes de septiembre, hasta fines de septiembre. Pueden ver a partir de estos datos que solo menos del 1 % de los sitios web ilegales en realidad llegan a nuestra jurisdicción. Hay muchos más que no están dentro de nuestro ámbito de capacidad para tomar alguna medida. Desde la perspectiva del ccTLD, creo que esto es sumamente importante considerarlo.

¿Cuál es el marco de notificadores confiables? Es un marco para tomar acciones rápidas sobre la base de la confianza y reglas preacordadas. El objetivo es manejar los casos de uso indebido serios y claros de manera más eficiente, con más transparencia y

también tenemos principios centrales: confianza, transparencia y el debido proceso.

En nuestro marco de TWNIC de notificadores confiables actual colaboramos con registros: DotAsia, con Edmon, .UK, .KR, .TOP y también con registradores. Además, tenemos uso indebido de contenido pero más que nada nos concentramos en el uso indebido del DNS, sobre todo en el phishing. Utilizamos SOP y también acuerdos para negociar con nuestros socios para incluir los principios de transparencia, confianza y el debido proceso. Eso es lo que estamos haciendo ahora en este marco.

Ustedes pueden ver a partir de esta diapositiva que sin los notificadores confiables… Recibimos datos de inteligencia de nuestro gobierno y también de los organismos encargados de la aplicación de la ley, la comunidad de ciberseguridad, de nosotros mismos y también de los ciudadanos. Luego investigamos para luego informar o notificar.

Los registradores también con los registros harán sus propias investigaciones y tomará medidas al respecto de bloquear o de suspender un dominio. En el marco de los notificadores confiables, después de que en TWNIC hayamos investigado y hayamos notificado a los registradores y los registros, entra en juego el acuerdo que está establecido con nosotros. Podemos utilizar ya esos recursos sin tener que gastar ningún recurso adicional para tomar acciones.

Cuáles son los beneficios entonces desde nuestro punto de vista. Primero, esto genera un marco para tener un intercambio de inteligencia sobre amenazas más expeditivo y también para manejar los casos de uso indebido. Reduce también la carga de investigación de los registradores y los registros. En tercer lugar, creemos que esto es muy importante. Podemos ser más proactivos porque, aunque trabajemos de manera eficiente, llegar a detectar un caso de phishing nos puede llevar varios días. De esta manera podemos tomar acción rápidamente antes de que las cosas escalen de nivel.

Estos son los datos de 2025. Todos en forma resumida en esta diapositiva. Hasta ahora hemos manejado 51 dominios en el 2025. Esperaríamos tener números más altos porque con nuestros socios empezamos a trabajar en la segunda mitad de este año. Esperamos números más altos para el próximo año.

El 78 % de los casos serán casos de phishing confirmados. Se tomó alguna medida. También el tiempo de respuesta en general es menor a dos días, entre uno y dos días por lo general. También creemos que podemos acelerar el proceso incorporando automatización. Otra cosa buena es que hasta este momento no habíamos recibido ninguna apelación. Eso tal vez muestre que el resultado es bueno. Siguiente, por favor. Siguiente. Gracias.

¿Cuáles son los desafíos para nosotros? Como los registros y registradores tienen distintos criterios, nosotros dependemos de eso en nuestros acuerdos bilaterales. Puede ocurrir que el

problema escale. Por eso tenemos este marco. Como siguiente paso, vamos a seguir expandiendo las alianzas con estos notificadores confiables y tal vez podemos desarrollar y demostrar un modelo no regulatorio exitoso para tener la cooperación de la industria y alinearnos también con las buenas prácticas de la ICANN y del GAC con respecto al uso indebido del DNS.

Este es un marco que constituye un paso crucial para poder compartir la responsabilidad de Internet entre las comunidades. Insto a todos ustedes a considerar más este tema e incluso a sumarse a nosotros. Cualquier duda, estamos a su disposición. Gracias.

SUSAN CHALMERS: Muchísimas gracias, Jo-Fan y Edmon, por estas excelentes presentaciones. Ahora quisiéramos darles la palabra a los representantes del GAC para ver si tienen alguna pregunta. Veo que la OMPI ha pedido la palabra.

BRIAN BECKHAM: Gracias, Susan. Gracias, Jo-Fan. Soy Brian Beckham, de la OMPI. Tengo una pregunta con respecto al primer punto de la última diapositiva. El tema de criterios posiblemente diferentes para los registros, los registradores y la escala. No sé si consideraron tener un marco estandarizado para resolver esa situación, para que los notificadores de confianza puedan utilizar todo lo que tienen en

una programación, en un contexto para todo el ecosistema en forma más amplia.

JO-FAN YU Gracias por esta pregunta. Sí. Sería muy útil si pudiéramos tener una plataforma para tener este tipo de negociaciones o intercambios de información, pero la dificultad en este momento reside en el nivel de concientización en la comunidad. Por lo que sabemos, si bien cada vez hay más conciencia todavía el nivel de conocimiento es bastante bajo. Cómo la comunidad puede formular un estándar, una norma, algunos criterios para compartir y tomar acción. Creo que todavía esto es un problema.

NICOLÁS CABALLERO Muchas gracias. ¿Querría responder, Edmon? Adelante.

EDMON CHUNG Simplemente quiero complementar. La respuesta breve es sí, por supuesto. DotAsia está trabajando con TW en el formato y la recolección de material que aporte pruebas, evidencias para que podamos acelerar cualquier tipo de proceso de suspensión. Trabajamos con CleanDNS y con NetBeacon y otras organizaciones para llegar a alguna suerte de norma de facto en la industria, aunque no necesariamente sea algo tan rígido.

TOMONORI MIYAMOTO Quería hacer una pregunta. Gracias por la presentación. ¿Cómo cada miembro o cada gobierno podría ayudarlos a ustedes?

EDMON CHUNG Pueden alentar a su ccTLD a que se sume a nosotros. Como mencionamos, priorizamos los registros por cuestiones de la sensibilidad de las notificaciones de baja, que es algo proporcionalmente adecuado para los nombres de dominio en los registros de primer nivel. Los aliento, los invito a que les digan a sus ccTLD que se sumen a nuestra red.

JO-FAN YU Creo que los ccTLD tienen un papel muy importante. Creo que los representantes del GAC pueden ayudar a generar conciencia e instarlos a que se sumen. Eso sería muy útil.

NICOLÁS CABALLERO Muchas gracias, Japón, por la pregunta. ¿Hay algún otro comentario o pregunta en los últimos cinco minutos que tenemos, antes de darle la palabra a Estados Unidos para algunas consideraciones respecto del comunicado? Colombia.

THIAGO DAL-TOE Muchas gracias por la presentación. Mi pregunta justamente tiene que ver con esto. Básicamente, nosotros, a nivel nacional, no tenemos que configurar nuestro propio programa de notificadores confiables. Es decir, podemos sumarnos a otros que ya existen. En

ese caso, ¿cómo lo hacemos? ¿Cuál es el proceso para sumarnos o para el proceso para aceptar nuestras solicitudes? Gracias.

EDMON CHUNG

Actualmente lo hacemos en forma bilateral porque cada ccTLD en particular puede tener requisitos levemente diferentes. Me olvidé de decir algo. Además de las notificaciones mutuas, también compartimos datos. Básicamente compartimos en forma trimestral todos los datos de suspensión con TW y viceversa pero este tipo de acuerdos podrían no incluir necesariamente esto.

Básicamente es un acuerdo, un memorando de entendimiento bilateral que establecemos entre nosotros y otros ccTLD. Con respecto a si necesitan sistemas, nuestro canal es tan simple como un correo confiable con claves de intercambio pero detrás de escena, dentro de nuestro sistema, ustedes determinan como ccTLD qué quieren tener como sistemas de backend.

NICOLÁS CABALLERO

Cómo comparten los datos. CSV son valores separados por comas. ¿Cómo se comparte?

EDMON CHUNG

CSV. Hay un código simple que explica la suspensión además de la suspensión del nombre del dominio suspendido.

NICOLÁS CABALLERO Susan, todo suyo.

SUSAN CHALMERS Muchas gracias. Tal vez podemos pasar a ver el último punto en la agenda para esta sesión. Los miembros del GAC habrán visto que hemos hecho circular previamente algunos textos para que consideren incluir en el comunicado, para ir generando un poco de reflexión antes de redactar el comunicado de Dublín en la sección sobre uso indebido del DNS.

Los responsables de este tema, por el momento, no tienen ningún asesoramiento. Estamos conformes con el asesoramiento que se ofreció en Praga y con el avance que hizo la comunidad en este sentido. Recomendamos incluir lo siguiente en las cuestiones de importancia. No las voy a leer pero las pueden ver en la pantalla. Si alguien quiere sugerir algún elemento adicional para la sección de cuestiones de importancia para el GAC, sería maravilloso. Estamos trabajando sobre texto borrador en este momento. Dejamos abierto el micrófono.

NICOLÁS CABALLERO Gracias, Estados Unidos. Como Susan indicó correctamente, tenemos abierto el micrófono. Si tienen alguna otra idea, como es habitual, siempre recibimos con agrado buenas ideas. ¿Algo que quieran agregar antes de cerrar? No veo ningún pedido de la palabra en línea ni tampoco ninguna mano levantada aquí en la sala, lo cual significa que básicamente estamos de acuerdo.

Muchísimas gracias. No necesitamos extendernos. Nos quedan dos minutos de la sesión pero no necesitamos cubrirlos. Vamos a hacer una pausa para el café ahora. De hecho, tenemos 30 minutos. Por favor, regresen a las 3:00 de la tarde en punto. Muchas gracias.

[FIN DE LA TRANSCRIPCIÓN]