ICANN83 | Foro sobre políticas – Plenario 2 de At-Large: avances en los esfuerzos de mitigación del uso indebido del DNS dentro de la ICANN
Jueves, 12 de junio de 2025 – 10:45 a 12:15 CEST

BRENDA BREWER: Para los que están en la sala, por favor, asegúrense de ir a buscar los cascos para poder usar la interpretación al francés y al español. Si ya tienen cascos, los pueden enchufar a su computadora y pueden seleccionar el idioma en el que quieran escuchar la reunión. Vamos a ir empezando en cuanto Justine nos dé el visto bueno.

Estamos listos para empezar. Esta sesión está a punto de comenzar. Por favor, empiecen a grabar. Gracias. Hola y bienvenidos a la sesión plenaria de At-Large: Impulsar los esfuerzos de mitigación del uso indebido del DNS dentro de la ICANN. Mi nombre es Brenda Brewer. Yo soy la administradora de la participación remota para esta sesión. Tengan en cuenta que esta sesión se está grabando y se rige por los estándares esperados de comportamiento de la ICANN así como por la política antiacoso de la comunidad de la ICANN. Durante esta sesión, los comentarios y las preguntas solo se van a leer en voz alta si se envían al pod de preguntas.

La interpretación para esta sesión incluye inglés, francés y español. Si desean tomar la palabra durante la sesión, levanten la mano en Zoom y una vez que se diga su nombre, los participantes virtuales

tendrán permiso para activar su micrófono en Zoom. Los participantes en la sala utilizarán un micrófono físico para tomar la palabra. Por favor, digan su nombre para los registros, el idioma en que van a hablar si no es el inglés y, por favor, hablen a un ritmo razonable. Con esto le doy la palabra a Jonathan Zuck, presidente de ALAC.

JONATHAN ZUCK Hola a todos. Muchas gracias. Gracias por estar aquí, en esta sesión plenaria intercomunitaria sobre el uso indebido del DNS. Es una sesión de ideas y hay que reiterar que es una conversación que siempre está en curso porque no hay una sesión en la que vayamos a resolver todos los problemas.

Justine me ha dicho que debo decir que es solo el principio. Estamos todavía hablando de este tema. Entiendo que hay muchas frustraciones en toda la comunidad porque cada uno tiene su perspectiva y hay cargas distintas también según el actor. Puede ser fuente de tensiones. Vamos a tener presente lo que Brenda nos acaba de decir acerca de los estándares de comportamiento. Creo que todos queremos alcanzar la misma meta y eso es lo importante de este tema. Hemos pedido que se planteasen algunas cuestiones. No podremos tener una lista exhaustiva. Conforme avancemos, podemos ir pensando en más cosas. No sé muy bien qué pasa con la agenda.

En cuanto a At-Large, no tenemos un conocimiento específico en esta área. Muchas veces informamos del uso indebido del DNS. Sí

que estamos trabajando sobre programas de pedagogía para los usuarios finales, para que las personas estén concienciadas acerca de cómo es un ataque y que sean cada vez menos vulnerables pero queríamos seguir hablando de esto y de la prevención del uso indebido del DNS o al menos reaccionar lo más rápido posible cuando se produzca.

Las dos cosas que se nos ocurren como áreas de prioridad potenciales, una son las implicaciones y las correlaciones que tienen que ver con las registraciones en masa. Entiendo que aún no tiene una definición este término pero se han realizado informes como el INFERMAL y otros estudios. Sabemos que cuando se dan muchas registraciones en el mismo momento se suele producir un uso indebido del DNS. Sabemos que se ha complicado debido al uso de la inteligencia artificial pero creo que aún podemos hacer algo para evitar esto.

En el segundo lugar tenemos lo que se llama el pivot. Es una idea que existe desde hace tiempo. Una vez que se identifica un dominio hay que identificar otros dominios asociados con ese registratario y necesita tiempo para ver cómo podemos retirar esos dominios y tomar otras medidas. Esas son nuestras áreas de interés. Creo que no hace falta hablar mucho más de esto. Creo que Mason Cole está aquí. Estaba en nuestra lista. Podemos mirar otra vez la agenda. Adelante, Mason.

MASON COLE

Buenos días a todos. Mi nombre es Mason Cole. Soy presidente por dos semanas más del CSG. Creo que tenía unas diapositivas. No sé si están disponibles. Muy bien. Gracias. Para dar un poco de contexto, yo soy también presidente de la BC y tanto la BC como el CSG son muy activos en esta cuestión. En Estambul el CSG empezó a hablar de nuevas herramientas para combatir el uso indebido del DNS.

Me alegra poder decir que hay una superposición en cuanto a las ideas en la comunidad y también lo que surgió a raíz del libro blanco por lo que compartimos ideas en lo que se refiere a lo que se ha propuesto en el seno del CSG y en el seno de otras partes de la comunidad. Por lo que ya existe un poco de consenso acerca de qué herramientas se pueden utilizar.

Voy a dar más contexto. Seguro que no constituye información nueva para muchas personas aquí en la sala pero el uso indebido del DNS es una cuestión a largo plazo. No se espera poder resolverlo en la próxima ronda de la ICANN para identificar las herramientas para luchar contra esto. Es un problema que va a persistir en el DNS. Se ha convertido en una cuestión endémica. Seguramente no se pueda erradicar.

Hemos visto un uso indebido desde las primeras iteraciones de Internet. Vi en una entrevista de Vint Cerf que dijo que había recibido su primer mensaje de spam en 1979. Por lo que si existe el spam desde hace 45 años sabemos que es un problema. El problema es real y se está expandiendo. Si miramos las cifras, la

economía de la ciberdelincuencia se estima que se eleve a 9,5 billones de dólares, por lo que es el tercer PIB más importante.

Estas son cifras del Foro Económico Mundial. Se espera que siga una tendencia al alza. Por esto la BC habla tanto del uso indebido, porque representamos a los que sufren los efectos económicos de estas actividades. También queremos decir que nunca vamos a poder definir o resolver del todo el uso indebido del DNS. Si nos remitimos a SAC 115 se dijo que las definiciones que existen en los contratos de ICANN no representan todas las formas del uso indebido del DNS que existen o que se denuncian o que dan lugar a acciones por parte de los ISP.

Nunca podrá haber una lista exhaustiva de los tipos de uso indebido del DNS. Por lo que no se espera poder definir o resolver estas cuestiones del todo. La ICANN está en una posición única para actuar contra el uso indebido del DNS y por eso estamos aquí. Próxima diapositiva. No es mi diapositiva, por favor. Próxima diapositiva. Sí. Imagino que se reformateó.

Se me pidió brindar dos temas acerca de las áreas de interés del PSWG. Brindar una declaración de problema y luego explicar nuestra razón. Jonathan ha dicho que el uso indebido ocurre a gran escala. Muchas veces hay un registratario que tiene varios dominios o un registratario que tiene varias cuentas de un registrador. Si se puede actuar a nivel de cuenta, podemos retirar una gran parte de ese uso indebido del DNS. Actualmente, actuar

caso por caso no es eficiente. No podemos saber la escala verdadera del uso indebido.

Necesitamos ayuda a nivel del registrador para tener acceso a otros nombres u otros actores maliciosos que están realizando un uso indebido y luego ayudar con la mitigación. ¿Qué políticas o cuestiones políticas se plantean entonces? ¿Cómo podemos codificar el nivel de deberes de mitigación a nivel de cuenta y cómo podemos documentar esa resolución del uso indebido al que ha denunciado? Se denuncia ante el registrador, se toman medidas o no. La persona que ha denunciado este uso indebido no sabe cuál es el resultado.

La segunda cuestión tiene que ver con los nombres de dominio impostores. Igual lo han visto en los medios. Octubre del año pasado. Vimos que un senador de los Estados Unidos envió una carta a unos registradores y a unos registros para plantearle la cuestión de los nombres de dominio impostores. Dio un ejemplo de fox-news.top. Si no lo saben, Fox es un medio que existe en los Estados Unidos y le preocupaba que se registraran nombres de dominio iguales para engañar a los consumidores y que miraran noticias falsas en la parte previa a las elecciones de los Estados Unidos. Existe este tipo de squatting y a veces los nombres son coincidencias exactas a organizaciones o marcas ya conocidas.

El problema es que se registran, se utilizan y luego se retiran tan rápido que la UDRP no es una herramienta efectiva para abordar esta cuestión. No se puede encargar de muchos nombres de

dominio al mismo tiempo. Cómo podemos crear un mecanismo para que ayuden los registradores y, más importante, cómo podemos crear un estándar para contrarrestar la suplantación de identidad.

Esto tiene que ver un poquito con la cuestión del contenido y por eso los registradores están un poco preocupados. Hay que encontrar un estándar para poder avanzar con esta cuestión de los nombres de dominio impostores. Creo que ya está. Estarán todos aliviados.

JONATHAN ZUCK: Menos mal. Muchas gracias, Mason. Ha sido de gran ayuda. Creo que Gabriel es el próximo en hablar.

GABRIEL ANDREWS: Mi nombre es Gabriel Andrews y soy copresidente del grupo de trabajo sobre seguridad pública. En el día a día trabajo para el FBI en los Estados Unidos. Nos gustaría compartir la perspectiva única de los organismos de cumplimiento de la ley. Creo que tenemos una perspectiva distinta a las personas que están en la sala. Cuando las personas denuncian ante nosotros la ciberdelincuencia, les remitimos a ic3.gov. Es un sitio que se utiliza para recopilar información acerca de los actores maliciosos y nos ayuda en las investigaciones.

Como efecto secundario nos permite tener estadísticas acerca de los delitos que están afectando a las personas. Se centra bastante

en los Estados Unidos pero sí que recibimos denuncias de todo el mundo. Nosotros creemos que las categorías principales de ciberdelincuencia son las mismas en todo el mundo. Las perspectivas y las cuestiones políticas potenciales. El fraude de inversión en criptomonedas es el delito en Internet más importante. Si no están familiarizados con esto, pueden mirar el programa de Last Week Tonight, de John Oliver, porque hizo un resumen de esta cuestión. Puede ser muy útil a la hora de proteger a su familia de este tipo de fraude. Consiste en animar a las personas a que inviertan en las criptomonedas. Esto pueden ser sus ahorros de toda la vida. Muchas veces se producen a la vez registraciones en masa de nombres de dominio. Creo que la pregunta es casi igual que la que puso Jonathan en su diapositiva. ¿Cómo podemos introducir una especie de fricción en el uso malicioso de las herramientas de registración de nombres de dominio en masa? Eso es solo para subrayar lo que sería muy importante para nosotros a la hora de abordar este delito tan importante.

En segundo lugar, de lo que más se denuncia, no en términos económicos sería el phishing. Veo aquí a amigos. Uno me preguntó ayer si teníamos la capacidad de solo mirar phishing que tuviera que ver con los correos electrónicos, o los nombres de dominio. Por desgracia creo que no es todo igual. Estos son nombres de dominio que son muy parecidos a los nombres de dominio de verdad. Lo que tendríamos que hacer es averiguar qué políticas pueden

abordar estas registraciones repetitivas de nombres de dominio maliciosos que imitan otros de verdad.

JONATHAN ZUCK: Gracias por iniciar esta conversación. Tenemos aquí reacciones de distintas perspectivas, registros, registradores y derechos humanos. Sin más le voy a dar la palabra al siguiente orador.

DENNIS TAN: Gracias, Jonathan. Soy Dennis Tan. Trabajo para Verisign pero aquí represento al grupo de partes interesadas de registro y también soy copresidente junto con mi colega Reg, que está aquí, a mi izquierda, en el grupo de trabajo de uso indebido del DNS.

Vamos a las reacciones. Primero, hay cuestiones en común. Voy a empezar por el principio. El lunes, la CPH y el grupo comunitario de uso indebido del DNS han presentado cuatro temas para el trabajo potencial para que la comunidad lo considere incluido en procesos de desarrollo de políticas. Estos cuatro temas son la idea pivot asociada a la verificación de los dominios que está presentada aquí. El segundo, ¿qué es lo que está fortaleciendo las obligaciones, los revendedores, registradores, en cuanto al uso de las API y otras herramientas de mitigación del uso indebido?

También el trabajo de los DGA botnets. De qué manera los operadores de registros de los gTLD y los potenciales de los ccTLD pueden beneficiarse de este marco en el que quizá podemos tener un marco operativo para distribuir información sobre los DGA, que

son los algoritmos de generación de dominio, que pueden generar cientos o miles de dominios que potencialmente pueden ser registrados en lote y que puedan utilizarse para operar estos ataques de phishing.

Los registradores individuales hoy tienen que ir a buscar esa información, verificarla pero lo que proponemos es un cleaning house que haga ese trabajo técnico con anticipación y que los operadores de registro de gTLD puedan evitar que ocurra este DGA.

En cuarto lugar, cómo reportar el phishing. Una y otra vez nos encontramos con que a la calidad de los informes le falta la evidencia o hay informaciones incorrectas. Cómo podemos entonces utilizar la ICANN para elevar esos estándares y llegar a la masa crítica para que los informes lleguen a las partes contratantes que sean accionables para poder así reducir los tiempos de mitigación.

En este contexto, ALAC de nuevo, a riesgo de sonar repetitivo Jonathan aquí nos habla de dos ideas de ALAC que son la correlación con el uso de registraciones masivas y el estudio de INFERMAL. Esto nos habla sobre el uso irrestricto de API para poder así crear una cuenta de registratario o nombres de dominio en escala en masa.

Estas son entonces las que se superponen con las de la CPH. Vamos a poder continuar desarrollando estas ideas. CSG es bastante similar. El número 1 tiene que ver con las registraciones maliciosas

en masa. No, perdón. Son los dominios asociados. Creo que hay una superposición también aquí. Lo podemos pasar.

En cuanto al número dos. No me traje las gafas de lectura hoy. Estoy tratando de ajustar la vista. Va a ser medio imposible. Es algo en lo que tenemos que continuar trabajando. Agradezco la idea planteada. Con CPH seguramente vamos a tener conversaciones adicionales. Gabe del PSWG nos dice que hablan de registraciones masivas y que también se superponen con las que CPH ha planteado. Nos gustaría tener más conversaciones para poder así entrar en detalle en lo que vamos a trabajar.

Respecto al número dos, quiero hacer una pregunta aclaratoria. La primera es que hay una repetición de registraciones maliciosas y la segunda es más fundacional. El phishing, los nombres de dominio con phishing para propósitos maliciosos. En las políticas y en los procedimientos hoy, ¿qué ven ustedes que falta y que no tratan el tema que ustedes están proponiendo aquí?

GABRIEL ANDREWS Creo que es más fácil responder la primera que la segunda. Para aclarar, los malos pueden venir y pueden registrar una cantidad de dominios bajo un nombre. Pueden tratar de cambiar el nombre y hacerlo una y otra vez. Expreso la idea de que a través de la conversación podamos ver en qué medida podemos detectar todo esto.

No sé muy bien si podemos tener ideas en nivel de cuenta en oposición a nivel de acción. Quizá pueda haber múltiples cuentas y eso lo podemos rastrear. El punto es que si vienen una y otra vez, ¿cómo podemos hacer que les resulte más difícil en oposición a tener una acción en cada dominio nuevo en el cual ellos quieren hacer una acción?

DENNIS TAN

Voy a ver si puedo entender el caso de uso aquí. No estamos hablando de nombres de dominio que fueron registradores en lote. Quizá cambiar una letra o no. El registro uno no funcionó. Vuelven y entonces vienen y en el registro dos cambian una o dos letras en la cadena de caracteres. Vuelven y utilizan este patrón, por así decirlo, de utilizar distintas cuentas de registratario u otras credenciales, etc. ¿Es eso?

GABRIEL ANDREWS

Sí. Cuando escuché a la Cámara de Partes Contratadas creo que una de las propuestas para tratar este pivot es que la información se pueda aplicar. Hay cierto alineamiento, me parece. Lo que estoy diciendo es que si podemos generar políticas que den respaldo a la acción a nivel de la cuenta o a nivel de los actores malos vamos a poder tener un impacto contra el delito que estamos viendo, si es que les suena bien esto.

JONATHAN ZUCK Gracias, Dennis.

REG LEVY Reg Levy, del RSG. Soy presidente junto con Luc del grupo de partes interesadas y el grupo de uso indebido de la Cámara de Partes Contratadas. Todo esto es muy interesante. Estamos contentos de que estas propuestas hayan sido presentadas. Vamos a llevar todo esto a nuestros grupos. Como ha indicado Dennis, hay mucha superposición. También se ha dicho por otro lado que lo hay y lo que estamos buscando es continuar esta conversación de cara al futuro.

JONATHAN ZUCK Gracias, Reg. Creo que Graeme quería hablar. Adelante, Graeme.

GRAEME BUNTON Hola a todos. Estoy aquí. Me llamo Graeme Bunton. Soy director ejecutivo del Instituto NetBeacon, que es parte del registro público de Internet y lo que hacemos es que Internet sea seguro para todos, focalizándonos en el uso indebido del DNS. Publicamos un documento sobre este tipo de temas hace unas semanas antes de esta reunión. Lo hicimos por un par de razones. Fundamentalmente, este es un tema que hemos debatido como comunidad durante un tiempo largo y nos parece que hay como un impulso de ver qué es lo que va a suceder a continuación después de las modificaciones contractuales que cambiaron el uso indebido para registros y registradores el año pasado y cómo

vamos a continuar de cara al futuro. Lo que queremos entonces es francamente ayudar a darle forma a esta conversación porque buena parte de todo esto puede generar una marca y entonces hemos generado ideas que hemos escrito. Eso es para el debate.

Desde mi perspectiva, la publicación de ese documento ha sido un éxito. Ha permitido que se planteen ideas y nos gustaría que la comunidad tome esas ideas y las lleve de cara al futuro. Creo que esto tiene que ver con la participación de la comunidad.

En este último punto, lo que vemos es que es importante, creo que todos queremos creer en el modelo de múltiples partes interesadas. Queremos ver el éxito en la comunidad de la ICANN y que podamos tomar un tema y hacer cosas. Cómo logramos que se hagan cosas. Queremos ver si podemos dar ejemplos de cómo puede ser un alcance más estrecho y que nos podamos familiarizar con cuáles son las ideas o cuáles no son y cómo establecemos el alcance de una manera que nos parece que como comunidad podemos tratar de enfrentar cada uno de estos temas y avanzar. Esto es muy importante para nosotros, plantear estas ideas.

No voy a entrar en detalle aquí porque creo que hemos cubierto estos temas en presentaciones anteriores asociadas a Domain Check o al pivot y cómo encontramos la manera de confirmar registraciones maliciosas. Algo que quiero destacar aquí es que estamos pensando en la diferencia entre los procesos reactivos y los proactivos para reducir el uso indebido.

Verificar otros dominios y cuentas es un proceso reactivo pero también consume tiempo. Por lo tanto, lo que nos gusta sobre este tipo de trabajo en el instituto es que para un registrador que tiene una gran cantidad de dominios y tiene que hacerlo de manera regular, esto requiere de tiempo. Es caro y esperamos entonces que todo esto pueda incentivar a los registradores a que piensen a quién le dan acceso a estas herramientas y a quién le permiten registrar grandes volúmenes de nombres de dominio.

Esta es una idea entonces interesante para que la comunidad considere por qué ayuda a reducir la escala y, además, evita que esta escala se amplíe. Las API con puertas son los que permiten que se establezcan muchos dominios y cómo podemos entonces incluir fricciones para asegurarnos de que se establecen límites.

Desde nuestra perspectiva, y esto me parece importante, nos parece que ese tipo de fricción tiene que estar basado en la reputación del cliente y no en quién es ese cliente sino más bien en qué es lo que han hecho. Creo también que hay una gran cantidad de interés en la precisión de los datos dentro de la comunidad.

Es difícil realizar ese trabajo de una manera eficiente y a tiempo. También en algunas circunstancias se incentivan cuestiones como el robo de identidad o la suplantación de identidad. Cuando pensaba en cómo hacer que esto funcione de nuevo, cómo podemos restringirlo y ser productivos especialmente en el contexto de esta comunidad, me parece que es importante centrarnos aquí en la fricción sobre la base de las actividades de los

registratarios en una plataforma. Esto podría ser cuántos dominios compraron, cuántos dominios renovaron, cuánto tiempo hace que son clientes, cuánto tiempo hace que tienen ese dominio en el periodo de gracia sin que haya sido reportado el uso indebido, cuál es el historial de los dominios informados.

Todas estas cosas no se pueden falsificar porque son las actividades que tiene el registrador en la plataforma y no tienen las mismas cuestiones vinculadas a la verificación de la identidad, a la privacidad. En eso creo que todos nos quedamos estancados. Por eso yo quiero alentarlos a que miren este tipo de enfoque, que lo tengan en cuenta como uno que puede ser igualmente de efectivo o incluso más. Siguiente diapositiva.

Los contactos de uso indebido de subdominio. Vemos que esto ocurre con los subdominios. Esta es una idea para darles a los registradores un mecanismo, una herramienta para poder hablar con los registratarios que tienen servicios, que ofrecen subdominios a terceros y ver si así se pueden copiar esas obligaciones de los registradores a los registratarios que operan servicios que ofrecen subdominios a terceros.

Aquí no hay ninguna obligación. Tiene que estar esta redacción en los términos de servicio, como registro, como registrador. No hay ninguna ejecutoriedad para hacer que se suspendan la actividad de los nombres de dominio en el tercer nivel de los gTLD porque esto podría tener enormes consecuencias que son muy difíciles de enumerar. Lo que sí tenemos es una herramienta para los

registradores, para que se acerquen a aquellos servicios que generan muchos subdominios y digan: “Este dominio está siendo abusado o tiene un uso incorrecto”.

Los mecanismos de recurso de los registratarios. Tenemos que saber que si estamos tratando el uso indebido a gran escala tenemos que estar seguros también de ver que haya dominios que son suspendidos, que no haya que sea impactado inadecuadamente. Nos pareció que esto era importante de destacar aquí también.

Los botnets y la coordinación de DGA, esto es un poco complicado cuando las LEA tienen que tratar a un botnet. Tienen que acercarse a los registradores individualmente y la ICANN tiene que poder ofrecer una función centralizada para que sea más eficiente. Esto no tiene que ser un PDP. Puede haber otras maneras en las que se lleve adelante. Por eso puedo explorarlo también. Tiene que haber una baja frecuencia pero un alto impacto. Siguiente diapositiva.

Vamos a hablar ahora de las conclusiones sobre este trabajo que he tratado de mencionar esta semana. Todos queremos avanzar en este tema. Todos queremos que haya un progreso. Para lograrlo tenemos todos que estar de acuerdo en el alcance. Tenemos todos que estar de acuerdo en que tiene que haber un progreso incremental en este tema. Es decir, no todos van a lograr lo que quieren. Eso debe quedar claro. Si queremos avanzar, tenemos que concentrarnos en pequeñas ganancias que son mejores que no tener ninguna ganancia de ningún tipo.

En líneas generales, entonces, y esto lo hemos escuchado en esta sala, hay cuestiones claras donde las modificaciones que estamos planteando crean obligaciones claras para los informes de uso indebido individuales. Estamos viendo modificaciones en el ecosistema en base a todo esto.

Sin embargo, queda claro también para nosotros, especialmente a partir de los datos que hemos visto en nuestros servicios de mapeo o de los informes que el uso indebido ocurre a gran escala. Vemos grandes campañas de uso indebido. ¿Cómo podemos nosotros como comunidad avanzar en tratar responsablemente y de manera segura el uso indebido a gran escala? Eso es lo que yo tenía para decir. Les agradezco.

JONATHAN ZUCK: Muchas gracias. Creo que está ya tratando temas como la mediación y otros temas. Adelante.

FARZANEH BADII: Soy miembro del grupo de partes interesadas no comerciales. Nos importa la libertad de expresión, el acceso al conocimiento, a los derechos de los registratarios pero los usuarios finales de Internet también deben tener acceso a todo este conocimiento y que se defiendan sus derechos humanos.

Nos importa la cuestión del uso indebido del DNS. Hay que hacer algo. No obstante, no estamos de acuerdo con esta sensación de urgencia que se retrata cada vez en la ICANN. Cada vez que se nos

presentan las estadísticas de manera general esas estadísticas no son delitos que han ocurrido como algo que venga directamente del uso indebido del DNS. Puede ser que no tengan nada que ver con la ICANN.

En cuanto a la mitigación del uso indebido del DNS, es algo muy importante para nosotros porque, como defensores de los derechos humanos, algunos de nuestros miembros pueden verse impactados porque hay ataques de phishing que son iniciados por actores estatales y quieren conseguir sus datos. Si hacemos bien la mitigación del uso indebido del DNS puede proteger los derechos humanos.

Poner cifras y estadísticas y decir que estamos sumergidos en el uso indebido del DNS y que muere Internet, no me parece el enfoque adecuado porque así vamos a tomar decisiones demasiado rápido. Tampoco han sido muy drásticas las recomendaciones que hemos oído aquí pero sean cuales sean las recomendaciones debe estar en el alcance de la ICANN y también debe tener en cuenta los derechos humanos.

¿Cómo afectamos a los derechos humanos de los registratarios y los usuarios de Internet cuando mitigamos el uso indebido? Ya existen varias herramientas en la sociedad para evaluar el efecto sobre los derechos humanos y esto no debe producirse después de los hechos. Debe también ocurrir antes a la hora de mitigar.

Tengo un compañero que dice que cuando nos centramos en el acceso al remedio, ¿es antes de la muerte o después? Exagero un

poquito. Lo que tenemos que hacer y Graeme también lo ha dicho, por ejemplo, cuando queremos una solución nunca debe dar lugar a la identificación de registratarios de nombres de dominio. Es de suma importancia para el NCSG que los registratarios puedan mantener sus datos anónimos. Es importante para el usuario de Internet y también para el registratario de un nombre de dominio.

La privacidad es importante. Además, es algo que puede afectar a la libertad de expresión. Cuando suspendemos un dominio malicioso o un dominio secuestrado o un dominio que ha sido comprometido, a la hora de suspenderlo puede ser que también suspendamos el acceso a una cierta información o a una campaña que se está llevando a cabo.

Mason habló de los nombres de dominio impostores. Esto no constituye el uso indebido del DNS. Esto tiene que ver con el contenido y en la NCSG queremos que la definición del uso indebido del DNS sea algo técnico y que se incluya en el contrato. Por ejemplo, las noticias falsas no constituyen un uso indebido del DNS y la ICANN no puede intervenir en ese campo porque realmente la ICANN no regula la libertad de expresión.

Tengo algunos comentarios sobre lo que dijo Graeme. Voy a intentar ser breve. Tengo algunas recomendaciones. Agradecemos los esfuerzos de NetBeacon. Tenemos que estudiar de manera cautelosa sus recomendaciones y tener después un debate acerca de cómo se pueden realizar evaluaciones desde los derechos

humanos para ver cómo se pueden poner en marcha estas soluciones sin afectar a los derechos humanos.

Por ejemplo, en cuanto a las asociaciones de los subdominios, puede tener un efecto desproporcionado cuando se trata de un retiro o de la suspensión de un nombre de dominio pero tampoco quiero decir mucho más porque aún no hemos tenido estas conversaciones. Eso es todo.

JONATHAN ZUCK Muchas gracias, Farzi. Gracias por traer su propia perspectiva. Se trata de encontrar el equilibrio adecuado y hacer todo lo posible para alcanzar los esfuerzos requeridos y minimizar las consecuencias para los usuarios finales. ¿Alguien del panel quiere responder a lo que se ha dicho? Adelante.

GABRIEL ANDREWS Sí. Tomé unas notas cuando hablaba Graeme. Soy Gabriel Andrews, del PSWG. Si no me equivoco, el número cinco tiene que ver con el papel de la ICANN con respecto a los botnets y el compartir esta información con las partes contratadas y dar directrices acerca de cómo actuar. Sí, podríamos explorar esto con ustedes, con las partes contratadas en la medida de lo posible.

El punto número dos acerca de introducir fricciones sobre las API y las registraciones maliciosas. Ahora hablo a título personal. No hablo como representante del GAC ni del PSWG. Mi primera reacción al leer el informe INFERMAL, mi reacción inicial es que hay

que conocer las políticas para los clientes, etc. pero creo que es importante dar un paso atrás y pensar que lo importante aquí es prevenir el daño y si hay maneras de llegar a esa prevención de daños, a fin de cuentas da igual qué camino se haya elegido. Lo importante es prevenir los daños. Cómo podemos llegar a estas ideas para llegar a esa meta y que sean funcionales y en eso estaría contento de colaborar con ustedes. Muchas gracias a todos y a las otras partes contratadas.

EUNICE ALEJANDRA PÉREZ COELLO Voy a hablar en español. Mi nombre es Eunice. Yo tengo una duda con respecto a las estadísticas que están presentando. Si adicionalmente están tomando en cuenta estos registratarios que ofrecen nombres de dominios para IP dinámicas. Si le están dando un seguimiento.

En lo particular, yo tengo uno de los servicios. Estos registratarios a veces ofrecen estos dominios en línea, nombres de dominio. Tú registras tu IP y prácticamente creas tu nombre de dominio y puedes conectar diferentes dispositivos, en específico pueden ser dispositivos orientados a la Internet de las Cosas.

Mi duda es si se hace este monitoreo con respecto a estos registrars o si no los consideran como registrars. Además, si estamos tomando en cuenta que, como usuario final, a veces no tenemos el conocimiento de que tenemos que implementar medidas de

seguridad utilizando este tipo de servicios porque están generando vulnerabilidades. Esa es mi pregunta. Gracias.

JONATHAN ZUCK ¿Quién quiere responder a esta pregunta?

GRAEME BUNTON Muchas gracias por la pregunta. Creo que puedo aportar una parte de eso porque los proveedores de servicios de subdominios tienen que ver con nuestro libro blanco. Una parte del trabajo potencial tiene que ver con estos servicios que ofrecen los subdominios pero para esas piezas dinámicas del DNS. No tengo muy buen ejemplo para esta comunidad. Quizá Brian me puede echar una mano aquí, porque viene de .ORG, que es nuestra organización madre.

Creo que un 40 % del uso indebido que se produce en .ORG vino de un proveedor de servicios de subdominios. Estamos hablando de 1 de 11 millones de proveedores de servicio que representó el 40 % del uso indebido. Esto es común. Esto ocurre en otros TLD. ¿Cómo podemos garantizar que se asuman responsabilidades entorno a esto entonces?

Veo aquí a Michele Neylon. Tuvimos una conversación. Voy a parafrasear un poco lo que dijo Michele. La idea era la siguiente. Si uno opera un servicio en Internet que es utilizado por terceros, puede o va a ser usado de manera indebida. Un requisito básico para ofrecer un servicio utilizado por terceros es que haya un contacto de uso indebido y también unos procesos de uso

indebido. No importa si son subdominios o URL porque las personas siempre van a usar estos servicios de manera indebida. Tenemos que ver si los proveedores asumen la responsabilidad para esto. En cuanto a los botnets y a la hora de usar esos servicios, quizá se pueden poner en peligro los dispositivos del Internet de las Cosas. Eso no entra en el alcance del trabajo que realizo.

EUNICE ALEJANDRA PÉREZ COELLO: Gracias. Voy a hablar otra vez en español.

ALAN WOODS: Antes estaba en los registradores pero ahora soy responsable jurídico de una empresa. Escuchando esta conversación, puede ser bueno tener la perspectiva de alguien que esté entre los registros y lo que se ve desde fuera. Estamos analizando los efectos y las mediciones de lo que ocurre en las mediciones sobre el uso indebido del DNS y qué podemos aprender, y cómo podemos aplicar eso a los próximos pasos con respecto al uso indebido del DNS.

Creo que lo ha dicho muy bien. Hay muchas estadísticas. Cuando estudiamos el problema siempre miramos las estadísticas. Esta semana hemos visto unas estadísticas muy impresionantes, que muestran la escala de la cuestión y cuando empezamos así solemos llegar a unas conclusiones de manera precipitada y la

comunidad tiende a enfatizar el papel del registro, de los registradores a la hora de prevenir eso.

Hubo una lista de los registradores que han sido utilizados para las registraciones en masa. Esto se llama un registrador de último recurso. Está allí a efectos de monitorizar los DGA, etc. Hemos visto 7.000 registraciones en masa y eso no es bueno.

Si retiramos esos dominios, vamos a afectar al trabajo de las fuerzas de seguridad. Quiero decir otra cosa. En nuestra empresa utilizamos unas 60 fuentes para nuestros registratarios. Hay mucho ruido. Nuestros clientes quieren que tomemos las medidas adecuadas y que sea tomada por la parte adecuada en el momento adecuado por lo que hay una escalada basada en la evidencia.

Hubo una revisión. No voy a decir nombres pero hubo 220.000 informes que vinieron de un informador. Solo un 1 % de estas denuncias, de estos informes, venían con evidencias. Lo que quiero decir es que nos tenemos que centrar en garantizar que no seamos alarmistas, que miremos bien las fuentes y que las medidas sean adecuadas por parte de los registros y de los registradores.

Hay un registro que ha salido en los medios últimamente a raíz de las modificaciones contractuales. Tengo que decir que no debemos solo retirar las listas de bloqueo y retirar estos nombres de dominio en masa porque solo retirar estos nombres de dominio porque figuren en la lista de bloqueo es casi igual que hacer lo contrario. No todo les incumbe a los registradores y a los registros.

Tenemos que trabajar conjuntamente en todo el ecosistema de la ICANN.

JONATHAN ZUCK La próxima sesión, uso indebido del DNS. Con tranquilidad.

FARZANEH BADII Estoy de acuerdo con lo que ha dicho Alan. El mero hecho de que exista un enlace de phishing no quiere decir que ya se haya producido el daño. Falta esto en nuestras conversaciones. El número de denuncias o de enlaces de phishing, claro que existe un riesgo mayor, pero es importante hablar con los términos adecuados porque aún no se ha producido el daño si no se ha utilizado el enlace de phishing. Cuando somos alarmistas, igual las soluciones pueden ser un poco deficientes. Yo creo que tenemos que hacer una sesión que se llame una mitigación del uso indebido del DNS respetando los derechos.

JONATHAN ZUCK Sabemos que se hace mucho daño pero mucho dinero también pierde gente que pierde completamente todos sus ahorros. Hay algo que nos debe alarmar. No debemos ser muy simplistas ni muy directos en la forma de reaccionar pero no debemos olvidarnos que hay un verdadero daño que está ocurriendo. Adelante, Michele.

MICHELE NEYLON

Retomando lo que se estaba diciendo aquí y también lo que decía Alan. Nosotros, los que participamos en ICANN, la mayor parte de nosotros queremos una Internet usable, segura y estable. Una donde hay un equilibrio en el ecosistema, donde hay cosas buenas y va a haber también una cierta cantidad de cosas malas.

Lo que hemos visto en los últimos años es que el foco se ha convertido en busquemos el uso indebido, vamos a cazar ese uso indebido y si la única herramienta que tenemos es un martillo, todo va a ser un problema. Tiene que haber un pivot en la mentalidad de esta conversación porque sí ocurren cosas malas, sí hay fraude que impacta en mis clientes, en mi familia, mis amigos, mis enemigos también. Hay muchas cosas malas que ocurren pero si lo miramos en términos de cómo mejorar toda la experiencia en vez de estar constantemente buscando el uso indebido.

El problema es que si buscamos el uso indebido constantemente y no lo hacemos desde la perspectiva de cómo mejorar la experiencia general, todo se convierte en una prisión, en una forma de ejecutar a un delincuente en lugar de cómo hago para que todo sea más cómodo y haya una mejor experiencia. No sé si entiende adónde voy, Jonathan.

Si los usuarios pasan de usar dominios a plataformas y aplicaciones, hemos perdido todo control sobre todo esto. No hay forma de rastrearlos. Podemos directamente tirar la toalla. Seguramente no es lo que a nosotros nos gustaría. Muchos de nosotros hemos visto de qué manera Internet ha incorporado

cosas muy buenas. Hay pequeñas empresas que ahora pueden existir por la Internet. No podrían haber existido hace 5-10 años. Si lo único que hacemos es hacer que sea cada vez más difícil que la gente se conecte online y que utilice Internet, va a dejar de usarla. Gracias.

JONATHAN ZUCK

Gracias, Michele. Obviamente aquí estamos tratando de llegar a mercados que aún no se han abierto y, por ejemplo, la delegación africana a la ICANN, que es la de AFRALO y los representantes de África, ellos hablan del uso indebido del DNS y simultáneamente hablan del crecimiento del mercado en África.

Uno de los problemas principales en África es la falta de confianza en la infraestructura de Internet y por eso tenemos que garantizar no crear un ambiente que sea conducente a que la gente salga del sistema de nombres de dominio. No sé cuál es la mejor manera.

Estamos tratando aquí de tener una conversación equilibrada y al mismo tiempo hay conversaciones que están ocurriendo desde hace mucho, mucho tiempo y a la gente le parece que tiene que seguir trayéndolas, planteándolas porque no les parece que vayan a ningún lado esas conversaciones.

Creo que tiene que haber más fluidez en ambos lados de la ecuación para que este tipo de utopía que usted acaba de describir sea el lugar al que vamos. Como usuario final, como registratarios,

la mayor parte de la gente lo que quiere es usar Internet y su uso de Internet está sufriendo en este momento.

MICHELE NEYLON: Esta es la clave. Si lo miramos desde la perspectiva del usuario, si conectarse a Internet es muy, muy, muy difícil, puede serlo. No, no me refiero a eso. No dije eso. Conectarse a Internet. Si eso se convierte en algo muy difícil, que en algunos lugares puede ocurrir, y estoy seguro de que algunos de ustedes han viajado a países donde para conectarse en un aeropuerto o en un hotel al wifi hay que dar mucha información, y esto lo escuchamos cada vez. ¿Por qué me estás pidiendo esto? ¿Por qué te tengo que dar lo otro? Ya te di esto. Ahora estás buscando más información.

Esto establece barreras y no quiere decir que sea un free for all. Tenemos que encontrar un equilibrio razonable. Equilibrar la protección de los usuarios, porque los usuarios no saben lo que hacen muchas veces y tenemos que equilibrarlo. Es decir, que no haya actividades criminales. No es solamente focalizarse constantemente en arrestar a gente y buscar el uso indebido cada vez. Deberíamos ver cómo lograr este equilibrio. Si fuese fácil, muchos de nosotros no tendríamos más trabajo. Por eso no es fácil. Gracias, Michele.

JONATHAN ZUCK: Le doy la palabra a James Galvin. ¿Está James aquí en la mesa? Ahí está. Muy bien.

JAMES GALVIN Soy James Galvin. Enlace de SSAC a la junta de la ICANN. A partir de lo que ha dicho Michele, el equipo ha sugerido que es un ambiente utópico, un lugar utópico al cual llegar. A mí lo que se me ocurre es que lo que nos está diciendo Michele podría perfectamente ser un elemento de una campaña ciber que ALAC y el SSAC quieren desarrollar, por eso lo que quería es que esto fuese otro punto para un debate adicional.

JONATHAN ZUCK Gracias, James. La otra parte es la de los usuarios. Gabriel.

GABRIEL ANDREWS Quisiera responder a Michele y a Farzi, y a ambos en realidad. Sin ser alarmista, el punto de vista aquí es que, como funcionarios de seguridad pública, los números son los números pero si puedo dejarles un mensaje, las ideas propuestas aquí pueden ser muy productivas para que las trabajemos pero el mensaje es que parece que estas ideas no abordan estos daños y realmente esperaba que productivamente podamos reducir la cantidad de daño que se le hace a los clientes, a los amigos en el mundo. Creo que hay una forma productiva de generar una colaboración y es un momento de reconocer todo esto. Esto era lo que quería decir.

JONATHAN ZUCK Gracias.

EUNICE ALEJANDRA PÉREZ COELLO: Voy a hablar otra vez en español. Gracias. Creo que esta sesión es muy interesante. El tema que mencionaron acerca de los derechos humanos creo que involucra mucho la parte de la educación. Educación a los usuarios finales. Estamos buscando maneras de cómo resolver o mitigar estas vulnerabilidades o ataques que se tienen y no estamos pensando en la manera en cómo vamos a concientizar a los usuarios finales porque a fin de cuentas, están utilizando tecnologías que tal vez desconozcan que hay ciertas vulnerabilidades que pueden tenerse. Creo que el hecho de que el grupo del SSAC pueda trabajar junto con ALAC para que se vaya manejando este tipo de sensibilización y capacitación a los usuarios finales es una de las maneras que puede disminuir estos ataques o las estadísticas que se tienen. Es prácticamente la capacitación al usuario final, que finalmente es el que usa el recurso. Gracias.

JONATHAN ZUCK: Sí. Vamos a tratar de lograrlo. Este es un debate con múltiples facetas.

REG LEVY: Gracias, Eunice. Sé que usted ha planteado un tema muy importante porque gran parte de lo que hacemos aquí en la ICANN es muy general y no aborda directamente los temas que tiene un usuario de Internet. La Internet de las cosas, acceder a Internet y

las vulnerabilidades implícitas en situaciones donde el dispositivo que uno tiene, tiene una contraseña de administrador y uno se conecta al wifi del hogar. Esta es una manera directa de acceder a la cuenta bancaria y todas esas cosas que uno no entiende.

Yo he tenido que educar a mi esposo en que tenemos que tener tres redes de wifi en la casa. Una es para los invitados, otras es para las cosas que usamos en la casa. Lamentablemente no es algo que podamos tratar aquí, en la ICANN. Aquí en ICANN tenemos un alcance muy específico para operar a nivel de que los usuarios finales no entienden, no tienen ni idea de lo que hacemos nosotros aquí y lo que espero es que podamos tener soluciones a estos problemas pero no sé realmente de qué manera podemos ayudarlos hoy.

JONATHAN ZUCK Gracias, Reg. Tiene la palabra Amrita. Claire.

CLAIRE CRAIG Soy Claire Craig, una de las vicepresidentas de ALAC. Gracias por esta conversación. Esto es más un comentario que una pregunta. Agradezco escuchar las distintas perspectivas de las distintas personas que están aquí en la sala. Lo que quisiera ver en este punto es que una de las cosas que a nosotros en la comunidad de At-Large nos preocupa es el interés de los usuarios finales.

Como resultado de esto, debemos tener un abordaje más equilibrado en lo que se refiere a la manera en la que los usuarios

finales se ven afectados cuando acceden a Internet. Qué ocurre especialmente en las regiones subatendidas. Voy escuchando aquí la conversación de registros y registradores, y lo difícil que puede ser para algunos de ellos. Me gustó mucho la presentación del grupo de seguridad pública porque aquí se plantean las verdaderas amenazas. Lo mismo que nos mencionó NetBeacon. Cuáles son las amenazas para los usuarios finales.

Nosotros aquí, en ALAC y en At-Large, planteamos algunas de estas amenazas, las ponemos sobre la mesa. Lo que tratamos de hacer a nivel de las RALO es hablar de la educación que ustedes mencionan pero debemos poder trabajar con las otras comunidades para garantizar que los usuarios finales tengan el tipo de apoyo que necesitan. Gracias.

JONATHAN ZUCK Amrita.

AMRITA CHOUDHURY Gracias, Jonathan. Queremos nosotros que la Internet sea abierta y que pueda ser usada por todos. Queremos proteger a los usuarios finales y queremos proteger sus derechos. Cuando esos derechos son abusados queremos que haya remedios. Lo que queremos también es estar de acuerdo en que tiene que haber una innovación que tiene que permitirse.

¿Qué hacemos entonces? El uso indebido que ocurre en los dominios no son cuestiones de nombres de dominio sino de

contenido. La gente que está por fuera de esta reunión no entiende todo esto. Uno puede decir que esto no es su cuestión pero cómo lo simplifica, cómo podemos diferenciar y decir: “Esta es mi responsabilidad y yo hago todo esto”.

Quizá el uso indebido del DNS, cómo podemos articularlo. Cómo podemos mejorar. Cómo podemos respetar la privacidad y a la vez educar. También mejorar lo que tienen que hacer registros y registradores. Todo esto tiene que estar claramente expresado en lo que se refiere a la aplicación de la ley, para que ellos sepan que esto es lo que se hace, esto es lo que se hizo o esto es lo que se hará.

Sabemos que hay cosas que no funcionan. Sin duda hay usos indebidos que son rastreados pero hay lugares en particular donde hay ciertos dominios donde siempre ocurre ese uso indebido. Hay tendencias. Ustedes saben más que yo cuáles son esas tendencias o de dónde proviene el uso indebido. Como dijo Farzi, los derechos de los usuarios se deben proteger, incluso los derechos de las personas porque cuando miramos los mercados, que no tienen tanta educación y yo vengo de esa región, hay una gran cantidad de personas que va a venir a Internet y que no sabe qué hacer. No sabe con quién tienen que contactarse. Incluso si se contactan con los registradores, no tienen los recursos.

¿No estamos acaso tratando de que dejen de disfrutar de Internet? No me parece que sea un tema que podamos resolver fácilmente pero al menos debemos estar abiertos a este debate y, si hacemos algo, cómo hacemos que sea fácil para otros. Incluso dentro del

ecosistema de la ICANN sabemos que esto ha ocurrido o eso se está haciendo.

No es que no se haga nada y sí, a veces hay cuestiones que se magnifican, hay cosas que de 10 se hacen 100 y entonces tenemos que mirar al impacto y no a los números, cómo está afectando, cuál es el impacto. No son los números los que cuentan sino el impacto de ese uso indebido o lo que sea que hayamos hecho. Muchas gracias.

JONATHAN ZUCK Quiero recordarles a todos que hablen un poco más lentos para nuestros intérpretes. No quiero mencionar ningún nombre, Amrita. Gabriel, por favor, hable despacio. Es el siguiente orador. Adelante.

GABRIEL ANDREWS Si era el siguiente, era una mano anterior.

JONATHAN ZUCK Muy bien. El siguiente entonces es Tijani.

TIJANI BEN JEMAA Primero muchas gracias a NetBeacon por el trabajo que han hecho. Se lo agradecemos mucho. Creo que la palabra clave aquí es el equilibrio. Sí, los usuarios finales tienen que tener la mitigación del uso indebido porque así se protegen los derechos como usuarios, como Farzi lo ha dicho, pero no toda notificación de uso indebido del DNS tiene que llevar a una acción. La verificación de esta

notificación creo, es la nota principal en la cadena de mitigación de uso indebido. Debemos poder lograr que esta nota sea muy eficiente. No queremos que haya un abuso del uso indebido del DNS y ahí debe haber un equilibrio y esa es la palabra clave aquí que debemos poder encontrar. Muchas gracias.

JONATHAN ZUCK: Creo que en eso estamos de acuerdo.

FARZANEH BADII: Sí. Hay muchos acuerdos pero son más alineamientos que equilibrios. La privacidad, la libertad de expresión, la seguridad. Todo esto puede crear entornos seguros para que el usuario final pueda operar y tener acceso. Como dije, la mitigación del uso indebido es muy importante para nosotros. No es solamente la seguridad del usuario final lo que está en juego sino que también están los derechos humanos en riesgo y tiene que haber una mitigación del uso indebido, un usuario que pueda tener un acceso al conocimiento, información sobre algo. Estas son las cosas que cuando hablamos de los usuarios finales y, como dije, nos importan mucho los usuarios finales porque no solamente hablamos de los registratarios de nombres de dominio.

Todo esto es para decir que el uso indebido del DNS no ocurre al nivel donde el acceso a Internet es imposible. No estoy diciendo que nadie discuta eso pero nuestras políticas y lo que nosotros generemos puede tener un impacto en hacer que mantener los

nombres de dominio sea tan difícil que todo el mundo va a pasar a las plataformas y va a haber gente que va a decir por qué hay tanta concentración de redes sociales, por qué está ocurriendo esto, por qué hacemos tan difícil que la gente pueda tener su sitio web y que opere por sí mismo.

JONATHAN ZUCK Muchas gracias, Farzi. No tengo la sensación de que vayamos demasiado rápido en esta área. Las recientes modificaciones contractuales se surgieron por primera vez hace 16 años por lo que creo que la comunidad no está sobrerreaccionando a esto. Es cierto que hablamos mucho del tema y eso quizá puede molestar un poquito pero no creo que en la comunidad de la ICANN hayamos creado un entorno que vaya por mal camino. Sí que diría eso. Las cosas no van tan rápido aquí en la ICANN. Creo que hay que evitar una sobrecorrección aquí. Hadia. También quiero decir que hay un micrófono portátil. Si alguien del público quiere hacer una pregunta o un comentario también lo puede hacer.

HADIA ELMINIAWI Gracias. Espero que estemos todos de acuerdo. Creo que estamos todos de acuerdo en que la seguridad y privacidad de los usuarios finales son igualmente importantes. Si estamos de acuerdo en eso, lo que necesitamos y según ha dicho Farzi creo que necesitamos un enfoque alineado, un enfoque alineado que tenga en cuenta esos factores. Muchas gracias.

JONATHAN ZUCK Greg Shatan.

GREG SHATAN Gracias. Creo que debemos evitar ser alarmistas en los dos lados de la cuestión. No queremos un Internet que sea imposible utilizar y tampoco queremos uno que no sea seguro. ¿Qué es lo que queremos? Queremos un entorno que sea seguro y que sea fácil de operar. Espero que eso no sea un equilibrio imposible de alcanzar.

Creo que es el equilibrio al que tenemos que llegar. La facilidad del uso sin la misma facilidad de uso indebido. Si algo se convierte en algo demasiado importante, otros puntos van a resentirse y no se van a tratar, por lo que hay que tener cuidado con, por ejemplo, esta preocupación de que todo el mundo se vaya a las plataformas. Siempre va a haber razones por las cuales usar Internet pero es cierto que hay una razón por la que no querríamos estar en Internet y es porque existen fraudes. Esta preocupación es bastante importante. Espero que podamos seguir trabajando hacia ese equilibrio.

JONATHAN ZUCK ¿Alguien más en la sala? Tampoco tenemos que seguir la sesión. Ahora tenemos la comida. Creo que ha sido una conversación tranquila, sin prisas. Justine, ¿quería decir algo?

JUSTINE CHEW

Sí. Ya que tenemos tiempo, si ven la agenda, en principio tengo que dar un resumen de cinco minutos pero ha sido una conversación tan enriquecedora que dejé de tomar apuntes. Podría resumir algo de lo que he escuchado. Tiene que haber un equilibrio, por supuesto. La comunicación es importante. Lo que ya están haciendo las partes contratadas quizá es un poco desconocido por lo que la comunicación vendría bien en ese entorno. Desde la perspectiva de los usuarios finales, por lo menos en ALAC, en At-Large, no queremos ser poco razonables. Por eso estamos todos aquí. Es una conversación de múltiples partes interesadas.

Desde la perspectiva de la política contra el uso indebido del DNS, siempre hablamos de que vamos a ver qué hacen los buenos registradores y registros. Vamos a ver si podemos pasar esas cosas a la política para que todos los actores del ecosistema puedan aprovecharlos. Es decir, que no solo hay actores maliciosos. Creo que estamos todos llegando a esa conclusión.

Es cierto que algunos, por el lugar del que proceden, quizá tienen otras ideas pero las sugerencias son muy buenas, sobre todo con respecto al título de la próxima sesión. Vamos a tenerlo todo en cuenta. Siempre acabamos con títulos muy largos para estas sesiones. Sí que me gustaría darles las gracias a los panelistas que vinieron aquí a hablar con nosotros y a todas las personas que han aportado su grano de arena a esta conversación.

JONATHAN ZUCK A comer.

[FIN DE LA TRANSCRIPCIÓN]