ICANN77 | Foro sobre políticas – Debate del GAC sobre el uso indebido del DNS y nuevas tecnologías
Miércoles, 14 de junio de 2023 – 10:45 a 12:15 DCA

JULIA CHARVOLEN: Hola. Bienvenidos a la sesión sobre uso indebido del DNS y tecnologías emergentes en la reunión ICANN77. Esta es una sesión del GAC. En esta sesión, nos regimos por el estándar de comportamiento esperado de la ICANN y esperamos que presenten las preguntas en el formato correspondiente. Hablen claramente y a un ritmo razonable para permitir una interpretación adecuada y silencien sus demás dispositivos al tomar la palabra. Tenemos distintas funcionalidades disponibles en la sala de Zoom y en la barra de herramientas, y ahora le doy la palabra al presidente del GAC, Nicolás Caballero.

NICOLAS CABALLERO: Hola. Bienvenidos a la sesión sobre mitigación de uso indebido del DNS. Tenemos a Susan Chalmers de la NTIA. Tenemos a Karel Douglas, de Trinidad y Tobago y de la autoridad de telecomunicaciones también de ese país. También tenemos a Lorraine Kapin, de la Comisión Federal de Comercio de los Estados Unidos, que también es copresidente del grupo de trabajo de seguridad pública del GAC, junto con Chris Lewis-Evans, que trabaja para el organismo nacional de lucha contra el delito en el Reino Unido y que también copreside este grupo de trabajo. Contamos con Russ Weinstein, de la división de dominios globales y estrategias de la ICANN, y a Peter Jansen de EURid.

Vamos a ver el temario del día de hoy. Primero tendremos una reseña de las enmiendas contractuales sobre el uso indebido del DNS que se han propuesto, y las amenazas a la seguridad del DNS que intentan resolver. Luego escucharemos a EURid, luego también hablaremos acerca del taller de desarrollo de capacidades del GAC sobre uso indebido del DNS para lo cual le daré la palabra a Karel, del grupo de trabajo de regiones subatendidas y luego tendremos un debate del GAC para determinar los pasos a seguir. Ahora entonces le doy la palabra a Chris.

CHRIS LEWIS-EVANS: Muchas gracias. Quisiera que Russ nos diera una reseña de las enmiendas contractuales y luego voy a explicar qué significa esto desde el punto de vista de la seguridad pública y los mecanismos pertinentes.

RUSSEL WEINSTEIN: Hola. Soy vicepresidente de Cuentas y Servicios en el equipo de Dominios Globales y Estrategias de la ICANN. Eso significa que estoy a cargo del relacionamiento con nuestros registros y registradores y que también coordino la mitigación de las amenazas al DNS y el programa pertinente dentro de la ICANN. Es un placer estar aquí con ustedes. Muchas gracias por recibirme.

Antes de empezar a ver las enmiendas contractuales y de qué se tratan, quiero ver cuál es el contexto y el origen de todo esto. Como saben, el uso indebido del DNS es un tema de mucho interés desde años en la comunidad de la ICANN y hemos avanzado mucho sobre todo en cuanto al tema de las mejores prácticas y todo lo realizado por la comunidad en

cuanto al tema contractual, pero, evidentemente, tenemos que seguir trabajando.

Las partes contratadas presentaron una propuesta ante la ICANN y ante toda la comunidad para realizar cambios a los contratos de manera tal de crear la obligación de interrumpir el uso indebido del DNS. Y la comunidad de la ICANN también habló acerca de qué más se puede hacer desde el desarrollo de políticas para mitigar el uso indebido del DNS. Comenzamos con estas enmiendas contractuales, que son muy puntuales y específicas.

Esto es lo que queremos hacer. Queremos generar estas enmiendas contractuales que sean significativas y que creen obligaciones significativas para registros y registradores para mitigar el uso indebido del DNS. Se las vamos a presentar también. El tema es crear un nuevo nivel de obligaciones para registros y registradores.

Hemos presentado esto previamente, así que les voy a dar una reseña. Quiero decirles que tienen la sesión grabada de la semana de preparación para esta reunión donde presentamos estas enmiendas contractuales, y también lo presentamos ante algunos de los miembros del GAC el día sábado. Ahora bien, en resumen, los cambios son los siguientes: comenzamos con las obligaciones existentes, los acuerdos de registros y registradores. Lo que hicimos agregar obligaciones, no hemos modificado nada. En estas enmiendas aclaramos que tienen que ser accesibles los contactos para reportar uso indebido del DNS en las páginas web de registros y registradores.

Entonces, ahora, registros y registradores, pueden utilizar un formulario en sus sitios web en contraposición a direcciones de correo electrónico porque, como sabemos, si publicamos una dirección de correo electrónico en una página web, eso genera correo electrónico no deseado o spam, y eso complica la tarea que están haciendo registros y registradores para justamente identificar los reclamos pertinentes y actuar al respecto. Además, tenemos una funcionalidad en la cual registros y registradores tienen que hacer un acuse de recibo de un reclamo por uso indebido o de una denuncia de uso indebido. Esto también es uno de los requisitos que hemos agregado.

También incorporamos la definición de uso indebido del DNS para reincorporarla a estos contratos, y se genera la nueva obligación de mitigar o interrumpir o detener el uso indebido del DNS. Ahora bien, estas enmiendas contractuales simplemente se traducen en un par de párrafos agregados a cada uno de los contratos, pero también le hemos agregado un texto preliminar a modo de asesoramiento. Ese texto preliminar tiene 15 páginas y allí se explica qué significan estos nuevos requisitos, cómo se los exigiría y cómo se los podría implementar. Incluso hemos agregado algunos ejemplos, así que los invito a todos a leer este documento de asesoramiento que es realmente muy útil como complemento para las enmiendas contractuales.

Ahora vamos a hablar de las dos obligaciones clave. Primero, agregar la definición de uso indebido del DNS al acuerdo de registro y al acuerdo de acreditación de registradores. El uso indebido del DNS significa el uso de malware, botnets, phishing, pharming y spam cuando se lo utiliza como un mecanismo para generar otras formas de uso indebido del DNS

que figuran en esta lista. Nosotros vemos que todo esto se remonta a distintos documentos publicados por el comité asesor de seguridad y estabilidad. Lo que vemos aquí en esta pantalla es el resultado del consenso logrado en la comunidad acerca de lo que sí constituye el uso indebido del DNS, y es un buen punto de partida.

Ahora que sabemos qué es el uso indebido del DNS, vemos que la obligación principal es la siguiente para los registradores. Cuando un registrador tiene evidencias concretas de que un nombre registrado y que tiene el patrocinio de un registrador se está utilizando para uso indebido del DNS, este registrador debe actuar diligentemente para mitigar las acciones o tomar las acciones necesarias para justamente interrumpir o detener este uso indebido del DNS en este nombre registrado.

Entonces vemos que todas estas acciones de mitigación se deben focalizar en justamente interrumpir el uso de ese nombre registrado para uso indebido del DNS o bien detenerlo por completo. Igualmente, tenemos casi la misma obligación para los registros, pero le agregamos algunas consideraciones para el rol específico de los registros en contraposición al rol de los registradores, porque uno está más cerca que otro de los clientes que registran los nombres. El registro tiene prácticamente la misma obligación, pero tienen que, como mínimo, referir el caso y con las evidencias pertinentes al registrador para así activar las obligaciones del registrador o bien adoptar acciones de mitigación por cuenta propia. Puede hacer una u otra de estas acciones, y esto es realmente muy muy importante para los registros. Estas son las obligaciones principales que hemos incorporados a los acuerdos. Y

ahora le doy la palabra a Chris, a menos que alguien tenga alguna pregunta.

CHRIS LEWIS-EVANS: Voy a presentar dos diapositivas y luego vamos a pasar a un segmento de preguntas y respuestas. Quiero hablar acerca del impacto de estos nuevos textos en lo que respecta a la seguridad pública, cómo podemos actuar, cómo pueden los registros y registradores actuar sobre la base de las evidencias que nosotros les presentamos, y tenemos que ver si realmente esto abarca absolutamente todo.

Nosotros en el seminario de desarrollo de capacidades recibimos preguntas tales como ¿esto abarca el phishing a través de SMS?, ¿abarca esto?, ¿abarca lo otro? Bueno, vemos en esta diapositiva una captura de pantalla de un mensaje enviado por SMS que dice que hay que activar una cuenta o suspender una cuenta, y luego vemos que hay un enlace para que alguien haga clic en ese enlace. Esto es phishing, constituye uso indebido del DNS y sucede a diario. Y aquí vemos la comprobación de que no es un enlace fidedigno. Entonces, nosotros, si recibimos una denuncia, tenemos que poder decirle a la persona pertinente “esto es phishing” y “esto es uso indebido del DNS”.

Ahora bien, el texto dice que debemos actuar diligentemente y tomar las acciones correspondientes. Ahora bien, si se trata de un dominio registrado maliciosamente, podremos suspender ese dominio y también pueden recomendarnos que contactemos a quien está a cargo del servicio de alojamiento o “hosting” de ese dominio. Ahora bien, si recibimos lo mismo por correo electrónico, también está dentro de este

uso indebido del DNS siempre y cuando haya un nombre de dominio en el cual tengamos que ingresar. A veces tenemos mensajes en los cuales se le agrega una palabra al nombre del dominio.

El ejemplo a la derecha es justamente un caso de este tipo. Este es un servicio que utilizan muchísimas personas, y justamente lo que se espera es que lo hagamos. A veces nos avisan que vamos a recibir un paquete de un servicio minorista, entonces decimos "uy, me está llegando un paquete, tengo que ingresar a este sitio", y justamente es ahí donde se quedan con nuestras contraseñas. Con lo cual es bueno ver que estas enmiendas aportan claridad para poder identificar todas estas instancias de phishing. Creo que fue en la reunión 76 de la ICANN que vimos o hablamos acerca de que gran cantidad de delitos se cometen a través de ataques de phishing, con lo cual el hecho de incluir al phishing en estos textos que se han incorporado es algo realmente muy bueno porque nos permite actuar.

Entonces, esto es clave para muchos gobiernos en este momento en ransomware. ¿Está incluido el ransomware en lo que ustedes han leído? No se lo menciona, pero sí es una forma de malware con lo cual está incluido. Por ejemplo, si un dominio entrega malware o software malicioso que resulta en el cifrado de un dispositivo o de una persona, esto queda incluido también. Veo que hay muchos gobiernos en este momento que están enfrentándose a este riesgo. También vemos que estos ataques de ransomware apuntan a distintas entidades dentro de su país, incluyendo entidades comerciales.

Vamos a ver el spyware. Sí, porque queda incluido. El spyware es otra forma de malware. Ahora, con respecto a los virus troyanos, sí, este es

otro tipo de malware con lo cual queda incluido. Siempre y cuando esté vinculado a un nombre de dominio. También tenemos adware, que es otra forma de malware. Entonces queda incluido.

Vemos que muchas de las vías que utilizan los delincuentes para afectar a sus víctimas, muchos de estos mecanismos quedan incluidos en las definiciones que nos acaban de compartir, así que, desde nuestra perspectiva, este es un muy buen paso para que los registradores tengan mayor claridad acerca de en qué casos deben actuar. Creo que es un muy buen paso y que nos lleva hacia otro nivel. Y ahora pasamos a las preguntas y respuestas.

NICOLAS CABALLERO: Muchas gracias, Chris. Antes de darle la palabra a Peter Janssen de EURid, quiero ver si hay preguntas o comentarios en la sala.

GULTEN TEPE: Sí, tenemos a alguien Taipéi chino y a Kavouss Arasteh de Irán.

NICOLAS CABALLERO: Sí, adelante.

KEN-YING TSENG: Soy del Centro de Información de Taiwán y soy delegada representando Taipéi chino. Con respecto a las enmiendas a los contratos en materia del uso indebido del DNS, creo que el lenguaje está bien formulado con respecto a este equilibrio delicado porque no es fácil interpretar el futuro, entonces esto te muestra lo importante que es el asesoramiento,

ya que servirá como referencia para las partes en el futuro a la hora de implementar las disposiciones en materia de uso indebido del DNS. Pero tengo preguntas acerca de la interpretación del lenguaje.

He visto el término reasonable/razonable, y esto aparece muchas veces. Me gustaría saber entonces si la interpretación de esta palabra razonable debe ser desde la perspectiva del registrador o registro o de la ICANN. Esa es mi primera pregunta. Mi segunda pregunta tiene que ver con temas transfronterizos. En la situación de uso indebido del DNS, muchas veces el perpetrador y el denunciante a veces pueden encontrarse en jurisdicciones distintas, entonces me gustaría saber si hemos considerado las cuestiones transfronterizas a la hora de imponer obligaciones a los registradores y a los registros, y también el tema de las barreras culturales y lingüísticas. Gracias.

CHRIS LEWIS-EVANS: Le doy la palabra a Russ.

RUSSEL WEINSTEIN: Muchas gracias por su pregunta. La primera pregunta tiene que ver con el término razonable. Para interpretar esta palabra, la obligación a la parte contratada, le corresponde a ella para ser razonable, y luego también a la ICANN a la hora de tomar las decisiones para ver si se han tomado decisiones razonables con base en los muchos años de experiencia en este campo, y también con estas disposiciones contractuales, así que creo que la ICANN tiene la discreción suficiente para hacer cumplir estos contratos.

CHRIS LEWIS-EVANS: En cuanto a la cuestión sobre las cuestiones transfronterizas, es cierto que puede haber hasta tres jurisdicciones, incluso cinco o seis. Esto se ha visto ya en otros casos. El lenguaje no permite que las agencias de cumplimiento de la ley entre y que diga "hay que hacer esto". Existe un proceso, jurisdicciones, tribunales, etcétera. Pero lo que sí que permite son solicitudes transfronterizas para ver las evidencias aportadas y luego tomar las medidas adecuadas con base en la consideración de estas evidencias. Hablando con registros y registradores, sé que agradecen mucho que aporten las agencias de cumplimiento de la ley, evidencias de buena calidad, así que cuando esto se aporta, se agradece y comienza allí una conversación acerca de qué más tiene, podemos tomar más medidas. El lenguaje permite acciones transfronterizas y esto también dependerá, por supuesto, de las evidencias.

NICOLAS CABALLERO: Irán, le doy la palabra.

KAVOUSS ARASTEH: Muchas gracias, Chris, y a todos. Si me lo permiten, dos casos me ocurrieron a mí. Hace dos meses recibí un mensaje del Secretario General para que yo acudiera a su oficina a las 9 de la mañana. Lo miré, lo comprobé y vi que realmente no me llegó del Secretario General del ITU. ¿Qué tipo de uso indebido es este?

En el segundo caso, recibí un mensaje de Christina no sé qué y pensaba que se trataba de alguien que trabajaba en un grupo de la ICANN. Luego

descubrí que realmente no se trataba de una Christina que conociera, sino de otra. Me gustaría saber qué categoría de uso indebido es esto, ¿y debo denunciar esto?, ¿debo notificarlo?, ¿y a quién? Lo que hice fue cambiar mi contraseña enseguida. Muchas gracias.

LAUREEN KAPIN: Sí, son ejemplos excelentes. Nos muestra las posibilidades de comunicaciones en este espectro que pueden ir de irritantes a constituir uso indebido, dando pie a consecuencias económicas o incluso emocionales. Si, por ejemplo, se trata de un fraude de romance, por ejemplo. No obstante, no sé si eso constituiría el uso indebido del DNS, porque no se ha producido un daño, simplemente irritación. Pero me gustaría hacer hincapié en un punto porque nos interesa a todos protegernos.

Un mensaje de "hola" puede ser el primer paso en algo que se hace más difícil, quizás un fraude de impostor. Es bueno borrar estos correos y no seguir el camino hacia la divulgación de información sensible o quizás dar acceso a la computadora. Entonces, para esos casos concretos, no constituiría un uso indebido del DNS, si bien es irritante.

NICOLAS CABALLERO: Malasia pide la palabra. Le doy la palabra al señor Mohamed Afiq.

MOHAMED AFIQ: Muchas gracias. Primero que todo, estas enmiendas son muy positivas y es hora de que mitiguemos mejor el uso indebido del DNS, así que, en este respecto, leído los documentos, y no sé si existen otras

obligaciones y prohibiciones o disposiciones, pero sí que me pregunto en cuanto al operador del registro, el registrador y en cuanto al cumplimiento contractual, me gustaría saber cómo se determinaría la posición final que se adopte cuando surja una controversia.

NICOLAS CABALLERO: Muchas gracias. Le doy la palabra a Russ.

RUSSEL WEINSTEIN: Sí, estoy intentando entender bien la pregunta. ¿Le importaría volver a hacerla?

MOHAMAD AFIW: Si hay una discrepancia cuando es el registro o registrador que hace la evaluación y si existen contradicciones en la conclusión acerca de si se utiliza para el uso indebido del DNS o no, así que, si hay un desacuerdo entre el registrador y el registro o el equipo de cumplimiento contractual, ¿qué podemos hacer en estos casos para determinar si realmente se trata de uso indebido del DNS?

RUSEL WEINSTEN: Muy bien, muchas gracias. Si usted le pasa sus evidencias al registrador y cree que se trata de un uso indebido del DNS y el registrador piensa que no, pues esto se puede pasar al departamento de cumplimiento contractual. Se realizará una evaluación de su reclamo estudiando las evidencias y podemos validar si algo se está posteriorizando para el uso indebido del DNS y luego hablaríamos con el registrador para superar

este problema, y pedir una rectificación. Creo que esto es lo que preguntaban.

NICOLAS CABALLERO: Sí, adelante, señor Afiq.

MOHAMAD AFIQ: Entonces estaba usted diciendo que el departamento de cumplimiento contractual tendrá la última palabra, o quizá determinará cuándo se trata de uso indebido del DNS.

RIUSSEL WEINSTEIN: Sí. El equipo de la ICANN de cumplimiento podrá aportar nuestra opinión a la parte contratada, la parte contratada podrá hacer lo mismo y trabajaremos juntos para decidir quién tiene razón. Además, las medidas tomadas por la parte contratada, quizá no cumplen con las expectativas de la persona que tiene el reclamo. Pero si se considera que las medidas son razonables y se lee el asesoramiento, allí se explica los diferentes tipos de uso indebido del DNS, por ejemplo, los nombres de dominio comprometidos, y puede ser que el registrador tome otro camino para resolver el asunto y quizás usted no está satisfecho con las medidas, pero esto no tendría por qué dar pie a un cambio de rumbo.

NICOLAS CABALLERO: Muchas gracias. Japón.

NOBUHISA NISHIGATA: Muchas gracias. Agradecemos todos los esfuerzos realizados de cara a las enmiendas. Tengo una pregunta. Y es la siguiente: el contrato actual antes de las enmiendas no prohíbe que las partes contratadas tomen medidas voluntarias para luchar contra acciones maliciosas cuando se trata del uso indebido del DNS, así que la pregunta es, como Russ acaba de decir, que a veces las medidas tomadas para luchar contra la actividad ilícita o maliciosa y la reacción del registrador no siempre va a cumplir con las expectativas de uno.

Vemos en las industrias japonesas un poco de frustración, así que agradecemos las enmiendas para ser útiles a la hora de interrumpir o detener el uso indebido del DNS, así que muchas gracias.

NICOLAS CABALLERO: Muchas gracias al delegado de Japón. Le doy la palabra a Chris o a Russ.

RUSSEL WEINSTEIN: Sí. Pido disculpas. Creo que no he entendido muy bien la pregunta. ¿Puede repetirla?

NOBUHISA NISHIGATA: Sí. Si miramos el borrador de enmiendas, vemos que las partes contratadas tienen que tomar medidas, pero si volvemos a mirar el contrato actual, ya pueden tomar medidas adecuadas las partes contratadas, es decir, acciones voluntarias, por ejemplo, retirar el servidor, si es necesario, aunque no se trate del uso indebido del DNS.

RUSSEL WEINSTEIN: Esta enmienda codifica qué es el uso indebido del DNS y cuáles son los requisitos con respecto a la interrupción y detención del uso indebido del DNS. En el contrato actual se utiliza otro término y esto seguirá siendo válido a nivel más amplio. El registrador tiene más discreción a la hora de abordar estas cuestiones y aun tendrán que tomar acciones. Pero lo importante es que hay una respuesta adecuada.

NOBUHISA NISHIGATA: En cuanto a los registradores, ¿existe un contrato existente? ¿Tenemos un punto de partida? Por ejemplo, los abogados. Si hay una investigación, quizás pueden decir ciertas cosas. Si piensan que es necesario tomar una decisión.

RUSSEL WEINSTEIN: No hay nada en el contrato que prohíba que tome las medidas adecuadas.

NICOLAS CABALLERO: Muchas gracias. Tengo a la República Democrática del Congo. Tiene usted la palabra.

BLAISE AZITEMINA: Muchas gracias. Me gustaría darle las gracias a Chris. Tuvo en cuenta muchas cosas de las que hablamos el domingo. En cuanto a los entornos móviles, ahora se considera una cuestión del uso indebido del DNS. Esto era una preocupación para las regiones subatendidas. Creo que estamos avanzando. Tengo una pregunta. A menudo, los

proveedores de servicio de internet, tenemos un problema que no es malicioso. Pero no sé si esto sería quizás una excusa para los proveedores de servicio de internet. Obligan a sus usuarios a suscribirse a ciertos servicios, pero no es algo voluntario por parte del usuario. El usuario se encuentra con que se ha suscrito a algo, quizás tiene que pagar una cuota para usar servicio A o servicio B, y el usuario no se acuerda de haberlo hecho. Y cuando se pone en contacto con el proveedor, dicen que esto forma parte de las condiciones generales. Y si estas actividades no son maliciosas, no se consideran phishing, malware, etcétera, pero no se hace con la voluntad expresa del usuario. ¿Qué se puede hacer al respecto?

CHRIS LEWIS-EVANS: Esto quizá se trataría de spam. En cuanto a la definición del uso indebido del DNS, es cierto que no se trata de una actividad maliciosa, así que no constituiría uso indebido del DNS y quizás sería un problema de protección de datos personales con respecto a lo que usted comentaba de los proveedores de servicio de internet.

LAUREEN KAPIN: Además, lo que usted menciona parece ser una cuestión de protección del consumidor. No necesariamente entra en el uso indebido del DNS, pero sí es una cuestión importante, porque no hay que cobrarle a la gente cosas que no saben de qué se tratan o sin su consentimiento.

NICOLAS CABALLERO: Le doy la palabra a Gemma, de la Comisión Europea.

GEMMA CAROLILLO: Gracias, señor presidente. Trataré de ser muy breve. Quiero retomar lo que han dicho otros colegas, especialmente el colega de Japón. En primer lugar, estamos muy contentos de ver el avance en esta iniciativa. Esto es algo realmente crítico, y el éxito de esta iniciativa será muy importante para el funcionamiento general del modelo de la ICANN, si se quiere, para toda la comunidad, para que toda la comunidad se reúna y pueda hacer algo en conjunto. Es por este motivo que queremos hacer un aporte constructivo en esta sesión y participamos en el taller el día sábado y también participamos en el período de comentario público porque queremos trabajar de manera constructiva.

Permítanme mencionar algunas cosas que hemos compartido en el taller de desarrollo de capacidades también. En primer lugar, como dijo el colega de Japón, dada la importancia de la celeridad en la respuesta al uso indebido del DNS, ¿qué pueden hacer los registros y registradores para monitorear este uso indebido del DNS de manera proactiva? Nosotros creemos que hay muchas buenas prácticas en la industria y nos gustaría que se las incluyera en los contratos, o al menos que se las considere.

En segundo lugar, agradecemos el documento que complementa a las enmiendas contractuales. Es muy muy útil, pero sería muy bueno también asegurarnos de que las disposiciones contractuales con respecto a la exigibilidad de las obligaciones queden claras también. Es muy importante para todas las partes interesadas que esto quede en claro. Y, por último, hay una parte muy importante que tiene que ver con la transparencia en los contratos. Los registros y registradores deben

tener una rendición de cuentas y deben informar acerca de sus acciones en cuanto al uso indebido del DNS.

Creemos que aumentar el nivel de transparencia es importante para que haya claridad en cuanto a las políticas que se están aplicando y para informar acerca de lo que se realiza, es decir, informar. Hemos tenido estos casos de uso indebido, hemos procedido de tal o cual manera. Esto nos ayuda a comprender estos contratos y su implementación en cuestiones prácticas o lo que hace la práctica. Gracias.

CHRIS LEWIS-EVANS: Muchas gracias, Gemma. El monitoreo proactivo es algo muy difícil de lograr. Lo que sí sugeriría para la próxima etapa de resoluciones contractuales, lo que sugeriría es formular este comentario para que se lo tenga en cuenta en la próxima ronda de acciones. Con respecto a la claridad en cuanto a lo que puede hacer el departamento de cumplimiento contractual, creo que nosotros como GAC podemos formular este comentario de manera tal de que el documento de asesoramiento refleje lo que ha dicho Russ, de manera tal que la comunidad esté al tanto de todo esto. Eso es lo que quiero compartir con respecto a lo que usted ha planteado.

RUSSEL WEINSTEIN: Muchas gracias por su comentario. Esperamos que todo esto quede claro en las enmiendas y en el documento complementario, pero, por supuesto, que cumplimiento contractual puede, si se quiere, rescindir el contrato de un registro o registrador si vemos que no actúa de conformidad con estos requisitos. Esto es lo que estamos tratando de

hacer justamente, elevar el nivel de cumplimiento, asegurarnos de que todos cumplan y poder, justamente, proteger a la industria. De manera tal de que no haya malas interpretaciones o interpretaciones erróneas acerca de la exigibilidad de estos contratos.

NICOLAS CABALLERO: Gracias, Chris, Russ, Comisión Europea. No voy a recibir más preguntas en virtud del tiempo disponible. Toma la palabra Peter Janssen.

PETER JANSSEN: Muchas gracias. Buenos días a todos. Veo que ya están mis diapositivas en la pantalla. Soy Peter Janssen, soy gerente general de EURid, es una organización belga sin fines de lucro que se encarga del dominio de alto nivel .eu que vemos ahí en pantalla en distintos códigos de escritura, justamente en respecto a los distintos idiomas que se hablan en la Unión Europea. Hoy voy a hablar acerca de la mitigación y la prevención del uso indebido del DNS que hacemos nosotros en carácter de registro. Podría hablar durante horas para tratar este tema en profundidad, pero sé que debo ser breve.

Me han dicho que siempre hablo mucho y muy rápido, así que les pido disculpas por adelantado a los intérpretes cuyo trabajo es muy arduo. Les agradezco desde ya por su labor. Bien. Hice un pequeño diagrama de lo que para mí es el proceso de registración y delegación. Como ustedes saben, en este proceso tenemos al registratario, que será el futuro titular del nombre de dominio que se pone en contacto con un registrador y utiliza interfases de los registros para transmitir esa solicitud del registratario al registro.

Entonces, una vez que el registro, EURid en este caso, recibe el pedido del registrador, realiza una serie de verificaciones. Nosotros en EURid tenemos algunos criterios de elegibilidad, por ejemplo, tener un domicilio en la Unión Europea o ser ciudadano de los Estados miembros. Esto lo verificamos automáticamente, y una vez que hacemos todas estas verificaciones, entonces ahí se registra el dominio y pasa a formar parte de nuestra base de datos de registraciones. Obviamente, que este proceso es más detallado. Aquí les doy el panorama general de cómo se registra un nombre de dominio. Posteriormente, podemos ir a nuestro sitio web y vemos que ese dominio está registrado y nadie más lo puede registrar.

Ahora bien, esto no significa que el dominio ya esté activo en internet, porque ese paso es la delegación. Aquí vemos algunas letras en el diagrama y ahí vemos entonces el proceso de delegación del nombre de dominio. Ahí pasamos a la base de datos y tomamos todos los datos necesarios en lo que respecta al DNS y lo insertamos en lo que nosotros denominamos el archivo de zona. Tenemos .eu en código de escritura latino, cirílico y griego. Este proceso de delegación del nombre de dominio inserta el nombre de dominio en este archivo de zona y justamente nos aseguramos de que todo funcione bien a nivel técnico. Y luego entonces lo transmitimos a los servidores que están en el segundo nivel y eso hace que el dominio empiece a funcionar y que se pueda hacer el proceso de resolución de este nombre de dominio. Estos son los procesos de registración y delegación.

Si vemos la delegación del nombre de dominio, vemos que justamente se extraen los datos de la base de datos de registraciones, como les dije

en la diapositiva anterior, y que luego todos esos datos se propagan en el segundo nivel de toda esta estructura. Nosotros le agregamos una funcionalidad a esta delegación del nombre de dominio.

NICOLAS CABALLERO: Disculpe que lo interrumpa, Peter. Debe hablar un poco más despacio, por favor.

PETER JANSSEN: Sí. Me lo esperaba. Les pido disculpas. Voy a tratar de hablar un poquito más despacio. Entonces, en este proceso de delegación de nombres de dominio, extraemos los datos de la base de datos de registraciones, los insertamos en el archivo de zona. Pero nosotros le agregamos una funcionalidad, y cuando se hace la delegación, tenemos una pregunta o surge esta pregunta que es: ¿deberíamos delegar este nombre de dominio? Y eso se basa en los atributos de este nombre de dominio. Si este nombre de dominio potencialmente puede ser malicioso, entonces tratamos de anticiparnos a esta situación. Tratamos de detectar una registración maliciosa de un nombre de dominio.

Si este motor de decisiones decide que potencialmente estamos ante una registración maliciosa, se retrasa la delegación. Es decir, técnicamente, el dominio está registrado, nadie más lo puede registrar, pero no funciona en internet. Entonces, no puede haber uso indebido del DNS a través de ese nombre de dominio. Luego tenemos el proceso de validación en el cual el registratario tiene que validar sus datos. Si se

trata de una entidad maliciosa que tiene la intención de dañar, entonces esa validación no se va a realizar porque el actor malicioso no quiere ser detectado. En ese caso, suspendemos a ese dominio.

Ahora bien, si el motor de decisión dice "ok, está todo bien, no hay nada sospechoso aquí", entonces, obviamente, el dominio se delega. Este motor de decisiones se define por un acrónimo APEWS que es el Sistema de Alerta Temprana y de Predicción de Uso Indebido. Es decir, cuando se registra un nombre de dominio, se pude predecir si tiene un fin malicioso. Lo que hacemos es utilizar distintos modelos de aprendizaje automático, vamos entrenando a estos modelos con distintos atributos, también los datos de registratario, dirección, correo electrónico, etcétera.

Nosotros también tenemos una cuestión aleatoria que tiene que ver con el nombre de dominio. Nosotros, por ejemplo, vemos que quizás un nombre de dominio nos pueda llamar la atención, entonces también tenemos un factor aleatorio. Y también, por supuesto, trabajamos con los servidores de nombres dentro del DNS. Ahora bien, ¿cómo funciona todo este modelo predictivo?

Por un lado, tenemos una lista de nombres de dominio que se utilizan con fines maliciosos para enviar spam, phishing, etcétera; y, por otro lado, tenemos los datos de registración de nombres de dominio correspondientes a esos dominios, pero también a otros dominios que se utilizan de buena fe.

Toda esa información se ingresa en un sistema de capacitación automático a diario que genera distintos factores que nos permiten

predecir qué sucederá con este nuevo dominio que se está registrando y nos puede decir si potencialmente puede ser malicioso o no.

Ustedes se preguntarán, ok, está bien, están tratando de predecir esto, qué tan bueno puede ser un dominio o no. ¿Qué pasa con esto? Bueno, aquí tenemos un gráfico y en el eje horizontal vemos enero de 2019 y vemos al final de este eje horizontal enero de 2022. Y en el eje vertical vemos la cantidad de nombres de dominio registrados mensualmente y qué porcentaje es detectado por nuestro sistema, porque pueden ser potencialmente maliciosos.

Ustedes pueden sacar varias conclusiones de este gráfico. Primero, vemos que la mayoría de los dominios se registran de buena fe y los nombres se delegan como de costumbre y no hay ningún problema. En segundo lugar, si vemos el rango de 2018 a 2019, vemos que ha sucedido algo con respecto a la cantidad de nombres de dominio indicados como dominios maliciosos, y lo que puede haber pasado es que nuestro sistema desalentó a una serie de actores maliciosos a que registren estos nombres con estos fines. Entonces vemos que este sistema, que es totalmente automático, permite evitar que se registren determinados dominios con fines maliciosos.

Vemos a veces que suben marcadamente la cantidad de estos dominios. En ese caso, hacemos el estudio pertinente y vemos que los actores maliciosos lo que tratan de hacer es pasar por alto o sortear nuestras medidas de protección y entonces nosotros la reforzamos.

Entonces, este modelo predictivo que se utiliza en el aprendizaje que se realiza a través de máquinas o el aprendizaje automatizado, este

modelo tiene que ser mejorado todo el tiempo. Por una parte, lo que hacemos es ver qué cantidad de dominios encontramos verdaderamente, y luego tenemos que ver la precisión de todos estos dominios que detectamos en cuántas oportunidades realmente se hizo una registración maliciosa.

Nosotros lo que hacemos es dejar actuar al sistema en tiempo real, y cuando predice una registración maliciosa, no hacemos nada, permitimos que avance la registración y más adelante verificamos si ese nombre de dominio efectivamente se utilizó de manera maliciosa. Y vemos que tuvimos una precisión mayor al 80%. Esto significa que en 4 de 5 de casos esos dominios se utilizaron para algún fin malicioso que tiene que ver con el uso indebido del DNS, como phishing, por ejemplo.

Ahora bien, estos sistemas no son perfectos. Nosotros tenemos que elegir entre cantidad o precisión, y esto es lo que estamos tratando de solucionar en este momento. Nosotros queremos lograr la mayor seguridad posible. Si marcamos a un dominio como malicioso, queremos que efectivamente resulte así, con lo cual queremos optimizar la precisión. Ahora bien, si marcamos un nombre de dominio como malicioso, pero lo registra un usuario de internet normal de buena fe, ahí tenemos un falso positivo. En ese caso, como vimos, el registratario es contactado y se lo invita a que valide sus datos de registración. Tenemos distintos tipos de métodos de verificación que permiten que los registratarios fácilmente verifiquen sus datos, entonces, ante un falso positivo, eso no es lo peor que puede pasar porque simplemente podemos verificar nuestra identidad como registratarios y no hay problema.

Bien. ¿Dónde podemos utilizar este sistema? Nosotros lo utilizamos en una instancia posterior a la registración y previa a la delegación, es decir, antes que el dominio pase al archivo de zona, es decir, si no lo delegamos, el dominio no se puede utilizar y no causa ningún daño, eso es bueno.

También lo podemos utilizar antes de la registración, es decir, evitar la registración si este dominio está marcado como un posible dominio malicioso, tenemos que actuar con la celeridad suficiente, pero, por supuesto, siempre está el riesgo de los falsos positivos y si no permitimos la registración, evitamos que esa persona pueda acceder a ese dominio, por eso permitimos que el dominio se registre, pero seguimos con las verificaciones previas a la delegación.

Luego podemos tener una instancia que es posterior a la registración y posterior a la delegación, por ejemplo, en el caso de dominios registrados hace 10 o 20 años podemos ver si son maliciosos o no porque ahora tenemos mucha más información disponible que permite fácilmente verificar si estos dominios son maliciosos o no.

Y, por último, tenemos un proyecto muy interesante en el cual estamos trabajando que se llama Cross TLD, o sea TLD relacionados, por ejemplo, tenemos a .EU y sus tres códigos de escritura dentro del mismo registro, pero vemos que los mismos actores maliciosos registran nombres en otras extensiones de este TLD, entonces tendríamos que ver qué información podemos recabar al comparar los datos de todas estas extensiones de estos TLD, estamos trabajando con otros ccTLD en Europa para lograr un sistema conjunto de información de los registros

para que todos los registros puedan trabajar mejor en los casos de uso indebido.

Obviamente surge el tema del GDPR, de la privacidad de los datos porque le estamos dando datos de registración de distintas jurisdicciones a un mismo sistema, lo que hacemos es anonimizar los datos, por ejemplo, mi nombre Peter Janssen, se codifica de esa manera que es ilegible para los seres humanos, entonces nosotros de esa manera podemos registrar los datos y los modelos de aprendizaje automático no se fijan si se trata de Peter Janssen o de esa cadena de caracteres que vemos ahí, simplemente tienen que detectar patrones.

Ya estoy llegando al final de esta presentación, lo que estamos haciendo es ver si podemos mejorar aún más esta detección de estos posibles dominios maliciosos en distintos TLD sin tener que utilizar información que es privada porque básicamente esta información es aleatoria a lo que respecta a los seres humanos. Con esto entonces ya terminé mi presentación, gracias por su atención, recibiré sus preguntas.

NICOLAS CABALLERO: Muchas gracias, es realmente fascinante y creo que debido al tiempo que nos queda solo podemos aceptar dos o tres preguntas más, pero tendríamos que escucharlo más la próxima vez. Muchas gracias a Peter por esta explicación tan detallada, ¿hay alguna pregunta o comentario en la sala o quizás en la sala de Zoom? No veo a nadie, así que, le vuelvo a dar la palabra a Susan o a Karel.

KAREL DOUGLAS: Muchas gracias. Soy representante de Trinidad y Tobago, sé que tenemos unos minutos más, así que, voy a ser muy breve, tenía apuntes, pero voy a hablar sin mirarlos, será más fácil. Vemos una foto aquí en la diapositiva, ¿esto les da una idea de lo que hicimos el 11 de junio? Que fue nuestro día de capacitación, ¿por qué tenemos este día?

Es para permitir a las personas recién llegadas y las que llevan más tiempo, a saber, cuáles son las cuestiones para entenderlas y también para dar sus aportes, es importante que el mayor número de personas posibles pueda contribuir, nos centramos en dos cuestiones, primero, en el uso indebido del DNS y la otra era el proceso de comentario público.

Este proceso de comentario público se utiliza como proceso de consulta y era importante que los miembros del GAC entendieran estos procesos y qué pasos se dan, también el uso indebido del DNS es muy importante, recibimos aportes muy buenos, hubo presentaciones muy interesantes acerca de los procesos y para unir estas dos cuestiones críticas hicimos sesiones en paralelo, los participantes se dividieron en grupos según el idioma que querían usar, teníamos el grupo de francés, español, árabe, chino e inglés.

Entonces la idea era que las personas pudieran hablar en estos grupos lingüísticos estos temas, sé que no tenemos mucho más tiempo. Un entregable crítico de esto era que ahora tenemos cinco personas voluntarias que van a asistir al proceso de comentario público en materia del uso indebido del DNS, en los grupos se habló del proceso en sí, pero también las cuestiones entorno al uso indebido del DNS y voy a

mencionar una de las preguntas que se hizo entorno a la definición, pasamos bastante tiempo hablando de esto.

Esto con rapidez son aspectos importantes, explorábamos estas cuestiones y sabemos que se suele definir según el contexto y cuando se trata de vida o muerte puede ser un tiempo razonable, puede ser cuestión de segundos, pero si estamos hablando de algo que no sea de vida o muerte, podemos estar hablando de semanas. Sabemos que las definiciones son bastantes vagas o amplias, así que, dependerá mucho de cada caso.

En la foto que tenemos vemos aquí a Nigel en el grupo lingüístico inglés, esto fue lo que hicimos hace unos pocos días, tuvimos esas conversaciones y esperamos que esto trascienda a un documento sobre las cuestiones entorno al uso indebido del DNS y a las cuestiones contractuales.

Este taller se hace bajo el grupo de regiones subatendidas, yo estoy involucrado, también lo está Tracy Hackshaw y Susan Chalmers. Queremos que en el futuro se incorporen más personas, la idea es juntar a todos y que estén todos involucrados en esto, así que, muchas gracias y espero no haber ido demasiado rápido.

NICOLAS CABALLERO: No podemos aceptar preguntas, así que, le voy a dar la palabra a Susan Chalmers.

SUSAN CHALMERS: Muchas gracias. Voy a ser muy breve, ICANN ha abierto un comentario público sobre las enmiendas propuestas al contrato, el 13 de julio es la fecha final, es un plazo bastante ambicioso y aquí vemos cómo se va a realizar el proceso, hoy comenzamos a solicitar aportes de los miembros del GAC en un documento de Google, habrá preguntas rectoras, no hemos tenido tiempo de mirarlo hoy.

Luego el siguiente paso es el grupo reducido, los comentarios que ha mencionado Karel y gracias a esos comentarios se pudo realizar un primer borrador con base en estos aportes, vamos a circular el borrador entre los miembros del GAC, se van a realizar comentarios y esperamos que para el 13 de julio tengamos ya el documento final, así que, aliento a todos los miembros del GAC a participar sobre este tema tan importante.

NICOLAS CABALLERO: Muchas gracias. Laureen, ¿le gustaría agregar algo?

LAUREEN KAPIN: Sí, si podemos pasar a la siguiente diapositiva. Se nos acaba el tiempo, pero Nico nos ha otorgado unos cinco minutos más para que podamos sembrar semillas, por así decirlo, no vamos a ver todas las flores crecer, pero durante la sesión de elaboración del comunicado del GAC tendremos tiempo para hablar más de esto, estas son las semillas, las consideraciones para el proceso de comentario público.

En su punto de vista, ¿cuáles son los aspectos positivos de estas enmiendas? Se ha hablado mucho de esto y la exigibilidad de esto está

muy bien tener el lenguaje, pero lo importante es que se pueda exigir que piensen acerca de la definición propuesta del uso indebido del DNS, esto supongo que es como los tres osos, no sabemos si es demasiado flexible, demasiado poco flexible, etc.

El asesoramiento de la ICANN sobre las enmiendas nos da muchas ideas, muchas orientaciones muy buenas y este documento podría evolucionar conforme gane más experiencia el equipo de cumplimiento y vea lo que podría ser útil, es suficientemente informativo a la hora de hablar de estos términos como términos accionables, con rapidez, etc., ¿y quién asume la responsabilidad de hacer qué? Pido disculpas si estoy hablando muy rápido.

Próxima diapositiva. Y también se ha señalado como el primero de muchos pasos en este tema complejo, es importante pensar en qué viene después, una idea que se ha discutido y también ha recibido apoyo por muchos en la comunidad de la ICANN. Es esta idea de PDP muy selectivos, muy concretos acerca de cuestiones muy concretas, por ejemplo, podría haber un PDP sobre cuál es la mejor manera de tratar el phishing, cuál sería una respuesta adecuada. Esto es a modo de ejemplo.

Pueden considerar cuál sería el objeto de trabajo de política en el futuro con respecto al uso indebido del DNS y no solo el qué, sino el cuándo, se tendría que realizar antes de la próxima ronda de los nuevos gTLD, o quizás no, el papel de los compromisos voluntarios de registro y también del interés público, cómo tratamos a los que vuelven a realizar actividades maliciosas, quizás los registratarios podrían ser los actores

que realicen actividades maliciosas y luego las cuestiones de los plazos del cronograma.

Esta lista no es exhaustiva, la idea es que vayan pensando con respecto al comentario público. Ahora les doy el tiempo para reflexionar y sé que todos van a participar para que el aporte del GAC sea lo más fuerte y positivo posible.

NICOLAS CABALLERO: Muchas gracias, Laureen, muchas gracias a Karel, Susan, a Chris; que ya no está aquí, a Russ y a Peter, Nos han dado mucho sobre qué hay que reflexionar. Si hago una pregunta rápida quizás tengamos tiempo y si no es el caso, cerramos la sesión, muchas gracias. Vamos a cerrar la sesión ya, vamos a hacer un receso de unos cinco minutos, Rob, ¿me puede confirmar si es así?

GULTEN TEPE: Si podemos seguir.

NICOLAS CABALLERO: Nuestra próxima sesión tiene que ver con las tecnologías emergentes y los objetivos de esta sesión tienen que ver con la creación de una lista de tecnologías sobre las cuales el GAC quisiera saber más y también establecer prioridades al respecto, también queremos identificar y hablar de alternativas para los marcos de información que podría usar el GAC para utilizar y compartir información y contenido de cara al futuro. Muchas gracias a Karel, Susan y Laureen.

Entonces queremos crear una lista de temas tecnológicos, los miembros del GAC antes de ICANN77 expresaron su deseo de hablar de tecnologías que podrían afectar a internet y al DNS en el futuro, y tenemos algunas sugerencias, tenemos tres, Blockchain, raíz alternativa del DNS y la inteligencia artificial. La idea es conversar sobre otros temas que podrían surgir, me parece que el representante de Taipéi, China tiene algunas ideas, no sé si quiere hablar ahora o quizás es solo un informe oral, ¿cómo quiere proceder?

KEN-YING TSENG: Muchas gracias, puedo presentar de manera breve mis reflexiones y por qué he propuesto estos temas. Yo creo que todos los que están en esta sala ya han notado que las tecnologías emergentes son cuestiones muy importantes, la Web3 y el Blockchain son temas muy importantes, y a finales de 2022 el chat GPT se hizo muy importante, la inteligencia artificial domina las discusiones en todo el mundo.

Así que, por eso estoy proponiendo al GAC y a la ICANN que consideren estas cuestiones con respecto al sistema de DNS, por ejemplo, en cuanto a la inteligencia artificial creo que la presentación de Peter es muy buen ejemplo, la ICANN y otras partes relacionadas ya están adoptando la inteligencia artificial para combatir el uso indebido del DNS, podríamos indagar más en eso.

La inteligencia artificial podría luchar contra amenazas de seguridad o quizás podría ser al revés, podría contribuir a estas actividades. Estas son mis reflexiones preliminares, gracias.

NICOLAS CABALLERO: Muchas gracias. ¿Hay algún comentario o alguna reacción a lo que ha comentado Ken-Ying? Si no es así, ¿podemos pasar a la siguiente diapositiva, Gulten? Entiendo que esto es para Alisa… Ah, Julia.

JULIA CHARVOLEN: Sí, tenemos al delegado de Irán que ha levantado la mano.

NICOLAS CABALLERO: Por favor sea breve y vaya al grano, gracias. Irán, tiene la palabra. Irán, tiene usted la palabra, por favor adelante.

JULIA CHARVOLEN: Sí, tenemos al delegado portugués.

KAVOUSS ARASTEH: Espero que me oigan bien, pido disculpas. Quería saber, ¿qué quieren decir con DNS alternativo?

NICOLAS CABALLERO: Ken-Ying, ¿quiere contestar a esta pregunta? Pregunta, ¿qué quiere decir exactamente cuando habla del DNS alternativo? Me parece que era así la pregunta.

KEN-YING TSENG: Me parece que el DNS alternativo quiere decir otros identificadores web que no sean los identificadores normales a los que estamos acostumbrados en la ICANN, creo que para Blockchain y Web3 tienen

sus propios identificadores web, que son parecidos a nuestro sistema actual que tiene varias capas, no obstante, no pasan por nuestros registradores y registros. Esa es la comprensión que tengo, yo no sé si algún otro participante podría arrojar más luz sobre ese tema.

NICOLAS CABALLERO: Muchas gracias. Países Bajos.

ALISA HEAVER: Con respecto a los sistemas alternativos de nombres de dominios y del DNS alternativo tengo tres preguntas… ¿Está bien?

NICOLAS CABALLERO: Sí, sí, pido disculpas, también pedía la palabra Portugal, pero, primero, vamos a oír a los Países Bajos y después vamos a Portugal.

ALISA HEAVER: Entonces me parece que hay pregunta preparada y espero que todos los miembros del GAC estén en la sala de Zoom, y que puedan responder a esta pregunta que está en la sala de Zoom. Tiene que ver con, si saben, ¿qué son estos sistemas alternativos de nombres de dominios?

NICOLAS CABALLERO: Portugal, tiene la palabra.

ANA NEVES: Voy a hablar en portugués, por supuesto. Quisiera mencionar… Bueno, estoy esperando que todos se pongan los auriculares para recibir la interpretación. Yo estoy plenamente a favor de la intervención de la delegada de Taipéi, China, es fundamental tener sesiones de capacitación para entender el impacto de las tecnologías emergentes en el DNS, sería muy interesante ver esto en el GAC y tener la posibilidad de ver cuál es este impacto, de qué se tratan.

Estas tecnologías emergentes son importantes y tenemos que entender cuál será su impacto a futuro para lo cual es necesario tener este debate aquí en las sesiones del GAC.

NICOLAS CABALLERO: Ahora le doy la palabra a Nigel Hickson del Reino Unido.

NIGEL HICKSON: Gracias, Sr. Presidente. Voy a retomar lo que ha dicho la delegada de Países Bajos y no sé si quisiera agregar algo más la colega Alisa.

ALISA HEAVER: Con todo gusto voy a continuar, pero no quiero quitarle la palabra a nadie.

NICOLAS CABALLERO: Continúe, por favor, delegada de Países Bajos.

ALISA HEAVER: Bueno, muchas gracias. No sé si tenemos los resultados de la encuesta, espero que la hayan respondido antes de la pregunta de Kavouss. Muy bien, el 53% de los encuestados respondieron que sí y el 47% respondió que no. Bueno, básicamente la mitad del GAC nunca oyó hablar de este tema.

Ahora podemos pasar a la segunda pregunta de esta encuesta.

NICOLAS CABALLERO: Continúe, por favor, delegada de Países Bajos.

ALISA HEAVER: Veamos entonces la segunda pregunta de la encuesta.

JULIA CHARVOLEN: Ya podemos ver la segunda pregunta de la encuesta.

ALISA HEAVER: Muchas gracias, mientras respondemos esta segunda pregunta, quizás le podemos dar la palabra a Nigel o a Brian.

NICOLAS CABALLERO: Muchas gracias. Ahora le doy la palabra a Brian.

BRIAN BECKHAM: Soy Brian Beckham de la OMPI. Muchas gracias, Sr. Presidente y colegas. Con respecto a este tema quiero mencionar algunas cuestiones de interés, en septiembre tendremos la octava ronda de diálogos de la

OMPI sobre propiedad intelectual y nuevas tecnologías, que buscan la intersección entre la inteligencia artificial y la propiedad intelectual, por ejemplo, nosotros tenemos una versión archivada de la séptima ronda de diálogos de la OMPI en la cual hablamos acerca del metaverso, la tecnología de Blockchain, los NFT y el internet de las cosas.

Ahora en abril la asociación internacional de marcas comerciales publicó un libro blanco sobre estas tecnologías, sobre Web3, sobre distintos dominios, etc. Ahora bien, en este documento se dice que hace falta la confianza de los consumidores para justamente hablar y trabajar en colaboración con la OMPI, y de esta manera entonces con la confianza de los consumidores se pueda utilizar todo esto y se le pueda adoptar para los distintos ecosistemas de tecnologías digitales emergentes, los NFT y el metaverso.

Justamente nosotros tuvimos que trabajar en el cybersquatting, tuvimos que trabajar en la primera política de consenso del ICANN acerca de todo este tema y ustedes recordarán que la ICANN tiene planeado revisar la UDRP, esta política de consenso, y básicamente o en concreto lo que quiero decir es que, ayer en la reunión de la IPC anunciamos que Namebase, que opera uno de estos dominios de la raíz alternativa del DNS, está adoptando la UDRP de manera voluntaria para la resolución de conflictos en esta raíz alternativa del DNS.

Nosotros creemos que esto es un buen punto de partida para próximas rondas de diálogos sobre este tema. Gracias.

NICOLAS CABALLERO: Muchas gracias, Brian. Ahora le doy la palabra al colega del Reino Unido, Nigel, adelante.

NIGEL HICKSON: Muchas gracias. Quiero hacer hincapié en la importancia de esta sesión, no vamos a abarcar todos los temas en el tiempo que nos queda porque ya estamos llegando a la pausa para el almuerzo, pero bien, quiero retomar lo dicho por la delegada de los Países Bajos, en tanto que esto amerita una sesión más extensa en nuestras próximas reuniones, y seguramente lo programaremos de esta manera.

Creo, principalmente, que este tema de la tecnología Blockchain y de la raíz alternativa del DNS es muy importante, como también lo es la inteligencia artificial, sin embargo, los dos primeros temas nos competen más a nosotros y son más pertinentes en cuanto a su importancia. Gracias.

NICOLAS CABALLERO: Gracias al delegado del Reino Unido. Ahora le doy la palabra a la representante o al representante de China, luego Países Bajos y luego el colega sentado aquí conmigo.

GUO FENG: Muchas gracias, Sr. Presidente. Esta sesión es interesante, con respecto a la optimización de estas sesiones si vamos a hacer sesiones similares, por ejemplo, en Hamburgo, sugiero que tengamos expertos en el ámbito de la tecnología aquí en las sesiones para que nos expliquen estas cuestiones desde el punto de vista de la tecnología. Nosotros, en

la mayoría de los casos aquí en el GAC, venimos del mundo del desarrollo de las políticas, así que, quisiera sugerir esto en esta instancia.

NICOLAS CABALLERO: Muchas gracias al delegado de China. La idea era identificar temas, generar un temario y luego ver si el GAC deseaba avanzar en el tratamiento de estos temas o no. Ahora bien, si acordamos estos temas, entonces podemos estructurar una sesión, les pido disculpas por la falta de tiempo, apenas nos restan cinco minutos. Ahora tiene la palabra la delegada de Países Bajos.

ALISA HEAVER: Bueno, tenemos los resultados de la segunda pregunta de la encuesta. Tenemos tres respuestas, bajo, medio y alto, la mayoría de los encuestados reconoce que no sabe demasiado acerca del tema. Ahora pasamos a la siguiente diapositiva, por favor.

Muy bien, no voy a leer todo el texto que vemos en pantalla, pero básicamente dice: "¿De qué se trata o qué es la raíz alternativa del DNS?" Y quisiera también recomendarles a mis colegas que lean un informe publicado por la OCTO en abril de 2022, me resultó muy interesante y después de leerlo me interesé en este tema. Así que, tengo una tercera pregunta, que es: "¿Desean tener capacitación sobre este tema?" Pero básicamente esto ha quedado respondido a la luz de las intervenciones previas de todos mis colegas, de todas maneras, lo pueden responder.

Lo que yo quería sugerir es lo siguiente. Introducir el tema, que todos lean sobre este tema y espero que para la próxima sesión sobre este tema todos hayamos leído el informe para poder tratarlo en profundidad.

NICOLAS CABALLERO: Gracias. Ahora le doy la palabra al representante de Suiza y le pido que sea breve, por favor, Jorge.

JORGE CANCIO: Soy Jorge Cancio, representante de Suiza, y voy a ser muy breve. En caso de que al GAC le interese la inteligencia artificial, lo que está haciendo el consejo de Europa es lo siguiente.

Thomas Schneider, quien fuera presidente anterior del GAC está presidiendo un comité en el consejo de Europa sobre este tema y con todo gusto podrá acercarse a conversar con nosotros en el GAC si a ustedes también les interesa.

NICOLAS CABALLERO: Por supuesto, esos ería definitivamente muy positivo. Ahora le pregunto a la representante de Países Bajos si quiere agregar algo más.

ALISA HEAVER: Ayer hablé con John Crain, el director de tecnologías de la ICANN, y él con todo gusto también nos ayudará a desarrollar los talleres de capacitación, creo que esta es una muy buena noticia y espero que todos participen en esos talleres. Gracias.

NICOLAS CABALLERO: Gracias, Países Bajos. Aquí está Ola Bergström, el vicepresidente que me acompaña y que proviene de Suiza, Ola, tiene la palabra.

OLA BERGSTRÖM: Muchas gracias, Sr. Presidente. Creo que tenemos que pasar al cómo implementar todo esto después de haber tratado estos temas, obviamente tenemos diferentes enfoques, opciones, herramientas, tenemos que considerar la frecuencia con la cual trataríamos estos temas, también creo que debemos ver qué sería lo más adecuado para nosotros dentro de un enfoque flexible, dado que no hay una única solución que sea la ideal para todos.

Obviamente que estamos interesados en todos sus comentarios, pero no podemos ahondar más en ellos, seguramente los retomaremos más adelante.

NICOLAS CABALLERO: Sí, definitivamente, muchas gracias, Ola. ¿Alguien tiene alguna pregunta o algún comentario antes de cerrar esta sesión? Tanto en la sala como en la sala de Zoom. Gulten, ¿me puede ayudar al respecto? ¿Gulten? ¿Julia?

GULTEN TEPE: El representante de China quiere tomar la palabra.

GUO FENG: Gracias, Sr. Presidente. Quiero retomar lo que dijimos al inicio de la sesión, hablamos del segundo tema, que es Blockchain, quisiera agregar los NFT también. Como ustedes saben, se basa en la tecnología Blockchain y es un identificador muy especial porque creo que los NFT son muy especiales y valdría la pena estudiarlos también.

NICOLAS CABALLERO: Muchas gracias al representante de China, vamos a agregar los NFT a nuestra lista de temas a tratar. Estamos a solo dos minutos de hacer nuestra pausa, quisiera saber si alguien más desea formular algún comentario o alguna pregunta… Si nadie solicita la palabra, entonces damos por concluida esta sesión, les agradezco mucho su participación, estaremos, nuevamente, aquí a las 13:45 hora local. Que disfruten del almuerzo, gracias.

[FIN DE LA TRANSCRIPCIÓN]