MONTREAL – Sesión de política de At-Large: fase 2 del EPDP
Domingo, 3 de noviembre de 2019 – 10:30 a 12:00 EDT
ICANN66 | Montreal, Canadá

ORADOR DESCONOCIDO: Van a poder escuchar lo que digan Alan y Hadia sobre el EPDP.

HADIA ELMINIAWI: Hola a todos. Bienvenidos a la próxima sesión.

ALAN GREENBERG: Para aquellos que no me conocen, soy Alan Greenberg. Soy uno de los dos miembros. Parece que hay eco en algún lugar. Soy uno de los dos miembros designados por ALAC para trabajar sobre el EPDP. Si lo llaman EP-DP los vamos a expulsar de la sala. Es un E-PDP, un PDP expeditivo. Solo respondo a las personas que usan el micrófono. Mi colega en esto es Hadia. Tenemos dos suplentes: Holly y Bastiaan.

La agenda es bastante simple. Vamos a hablar un poco sobre cómo llegamos hasta aquí. La fase uno del EPDP tuvo lugar entre mediados y fines del año pasado hasta principios del 2019, de este año. Ahora estamos en la fase dos. Esto es poco común en un PDP. En general, un PDP tiene un tema, un conjunto de informes, un informe final y después desaparece. Nosotros tenemos dos partes. Cada una incluirá informes, recomendaciones, la aprobación de la junta directiva y después se pasará a la próxima etapa. Quizá tengamos una fase tres.

Vamos a hablar un poco sobre la fase uno, fase dos. El SSAD, el sistema estandarizado de divulgación… Es una presentación muy breve. Solo tiene 10 diapositivas. No vamos a hablar de esto en detalle. Espero que tengamos mucho tiempo para preguntas y respuestas. La próxima diapositiva, por favor. Los antecedentes. Hay legislación sobre privacidad sancionada en Europa y en otros lugares. Existe desde hace muchos años. La ICANN en algún momento tuvo esto en cuenta y el foco de la legislación de privacidad de la ICANN ha estado básicamente en WHOIS porque a pesar de que hay muchos aspectos de la ICANN donde debemos preocuparnos por la privacidad, y si prestan atención verán que hay muchos cambios en la ICANN, muchos temas y muchas áreas donde hay que tildar un casillero con respecto a la privacidad pero el WHOIS es un tema especial por los requerimientos de WHOIS. De hecho, si volvemos al momento en que se creó la ICANN, uno de los mandatos era tener un WHOIS que tuviera información pública sobre los registratarios y sobre la forma de ponerse en contacto con ellos.

Muy poco tiempo después de que esto se implementara, los proveedores de servicios de privacidad y representación empezaron a buscar la forma de ocultar cierta información con un costo adicional. El GDPR entró en vigencia en 2017 y es una modificación de las leyes y normativas anteriores. La diferencia en este caso es que con dos años de demora había multas o penalidades muy importantes. A pesar de que las multas dependen de la infracción pueden ser tan altas como un 4% de los ingresos globales. No la rentabilidad, los ingresos. Ese es el margen de rentabilidad para muchas empresas. Este es un tema importante.

Repentinamente se volvió un tema del cual la ICANN se tenía que preocupar porque las partes contratadas, especialmente las que están en Europa, tenían un interés financiero, un interés creado. No querían tener que pagar penalidades o multas. Para resolver el tema, la junta directiva adoptó lo que se llama la especificación temporaria. Este nombre es curioso pero sigue lo que está establecido en los contratos de la ICANN. Si ven los contratos que tiene la ICANN con las partes contratadas, hay un contrato básico y después especificaciones que son anexos donde hay ciertos detalles específicos asociados a cada contrato. Esta es una especificación que debía agregarse a los contratos pero iba a ser temporaria. Por eso se llamó especificación temporaria y modificaba los contratos para que pudieran cumplir con el GDPR. Permitía a las partes contratadas ocultar información que de lo contrario tendrían que haber hecho pública y hablar de estos detalles.

En esta especificación temporaria los contratos con los registros permitían que una especificación temporaria tuviera vigencia durante tres meses solamente y podría ser renovable pero renovable hasta un total de 12 meses. Básicamente dice que la junta puede implementar políticas en casos de emergencias cuando los procesos normales no evolucionan tan rápidamente pero esto solo puede tener una vigencia de un año. El PDP acelerado establecía que había que crear un plan para tener una política real para remplazar la política temporaria dentro del año. En cierta medida esto no se hizo.

Nosotros creamos una política, la presentamos a la junta para que la junta la aprobara en la fecha establecida pero de esta manera las

partes contratadas no hubieran tenido tiempo para implementarlo. Estamos hablando de escribir código en muchos casos. La política también decía que las partes contratadas tienen aproximadamente un año y un poco menos para implementar todo esto. En el ínterin estamos adoptando una política que es comparable a la especificación temporaria. No es una especificación temporaria pero es una política que tiene la misma redacción que la especificación temporaria. Esto se iba a utilizar durante el periodo de transición en el que todavía estamos y que termina el 29 de febrero de 2020. En esa fecha todas las partes contratadas deberán cumplir con la política de fase uno.

Esa es la situación actual. Algunos puntos que no pudimos cerrar o definir, estos se llevarán a la fase tres. La parte más importante de fase dos, es decir, ahora que los registradores y registros están cumpliendo con el GDPR, estamos trabajando con una gran cantidad de información. El GDPR permite que esta información expurgada sea comunicada a ciertos terceros en ciertas condiciones. Ahora nuestro desafío es crear un sistema que permita hacer esto o tenemos que hacer lo que estamos haciendo hoy en día. Si ustedes quieren información, tienen que dirigirse a un registro o registrador que hacen todo por sí mismos. No hay uniformidad. En algunos casos no hay respuestas con respecto a esa información expurgada. Vamos a hablar un poco de eso de aquí en más pero esa es la situación actual. Ahora le voy a dar la palabra a Hadia, que les va a dar una descripción general de la implementación de la fase uno. Si hay algo que no mencioné en mi introducción, por favor, dígalo primero.

HADIA ELMINIAWI: No, en realidad no dejó de mencionar nada. Como dijo Alan, fue necesario que la comunidad llegara a una política de consenso que remplazaría a la especificación temporaria. Para hacerlo, el EPDP para los gTLD, se forma un equipo que iba a trabajar sobre este tema. Esto fue adoptado por el consejo de la GNSO en marzo. La fase uno del EPDP pudo desarrollar una política de consenso que fue adoptada por el consejo de la GNSO en marzo 2019. Posteriormente, la junta directiva adoptó una resolución adoptando 27 de las 29 recomendaciones. El EPDP presentó 29 recomendaciones, dos de las cuales no fueron adoptadas. Las que no fueron adoptadas fueron la recomendación 1, objetivo 2, que se refería al propósito de la ICANN de mantener la estabilidad y flexibilidad del DNS. La junta no adoptó esta recomendación en parte porque una parte de esta recomendación se consideró una actividad y no un propósito. En todos los casos este es un tema que debía ser resuelto en la fase dos.

La segunda recomendación que no fue adoptada por la junta directiva es la que tenía que ver con el campo de nombre de organización, donde había una opción de eliminar o expurgar el cambio con el nombre de la organización si se enviaban pedidos sobre los sujetos de los datos con respecto a los datos de ese campo. La junta consideró que eliminar esa información podría tener un impacto negativo sobre el sujeto de los datos ya que podría llevar a que una organización perdiera sus derechos sobre ese nombre.

Como dijimos, tenemos una nueva política de registración de gTLD. Adoptamos una política temporaria basada en la especificación temporaria, y la fecha de entrada en vigencia que se prevé para la

política de fase uno es el 29 de febrero de 2020. Esto no significa que los registradores o los registros no lo puedan implementar antes de esa fecha pero esa es la fecha límite para que todos estén cumpliendo con las nuevas políticas. ¿Podemos pasar a la próxima diapositiva, por favor?

Lo que tratamos en la fase uno fueron los propósitos para el procesamiento de los datos, las bases legales para el procesamiento de los datos, qué datos deben recabarse, durante cuánto tiempo deben conservarse y qué elementos de datos podrían divulgarse y comunicarse en caso de que hubiera un pedido legítimo aprobado. Lo que no definimos es quiénes son los encargados del procesamiento de datos, quiénes son los controladores. También un tema que surgió es que hay evidencia de que las políticas que desarrollamos quizá no sirvan en algunos casos actuales pero esto se debe a que todo el trabajo del EPDP, la fase uno y la fase dos, no se ha terminado. Un aspecto importante que debemos considerar aquí es que fue necesario desarrollar estas políticas por supuesto por cumplir con el GDPR pero también les da a los sujetos de datos más transparencia y la capacidad de controlar sus datos, tener control sobre sus datos porque pueden saber qué datos se piden, para qué propósitos, quién los pide, quién los comunica y en qué casos estos datos pueden ser compartidos con terceros.

Esto en realidad mejora los aspectos de privacidad del sujeto de datos y lo que buscamos en la fase dos es mejorar aun más la protección de los datos personales del sujeto de datos y también permitir que las solicitudes legítimas de datos puedan llegar a destino y reciban datos

precisos que puedan utilizar en pos de sus intereses legítimos. Esto es de interés para Internet y los usuarios de la Internet porque si hablamos de la seguridad de DNS y la seguridad de los sitios web y la estabilidad de la Internet, esto afecta directamente a los usuarios finales y creo que es aquí donde nosotros, ALAC, debemos involucrarnos cuando participamos en este EPDP. Nosotros estamos centrados en los derechos de los sujetos de datos pero también buscamos tener en cuenta los derechos de los usuarios finales. Le voy a dar la palabra a Alan ahora.

ALAN GREENBERG: Uno de los aspectos interesantes es que esto surgió en el último día. Es el último punto. Como dije antes, desarrollamos una política que ahora está implementada en forma temporaria para que a las personas que creen que tienen derecho legítimo a acceder a los datos les explique la forma de acceder a esos datos. Lo que surgió recientemente es que hubo un caso donde alguien presentó un reclamo con respecto a un sitio web en Europa y presentaron un reclamo a su oficina de protección de datos. Esa oficina de protección de datos analizó el caso y dijo: “Aparentemente esto es un problema pero para resolverlo tenemos que saber quién es el registratario” y pidieron esa información al registrador para que comunicaran la información. El funcionario de protección de datos consideró las motivaciones y lo que decía la legislación en cuanto a en qué condiciones se podía comunicar la información y consideraron que la solicitud era válida pero el registrador se negó a dar la información.

Ahora se presentó ese reclamo al departamento de cumplimiento contractual de la ICANN.

En resumen, quiero decir que hay implementaciones en cuanto a la forma de interpretar las políticas que tenemos. A veces nosotros pensamos de manera diferente pero a veces el comisionado de protección de datos dice: “No estamos cumpliendo si presentamos la información como se dice según la legislación”. Alguien mencionó también que hay otros 40 reclamos que se quieren presentar al departamento de cumplimiento contractual de la ICANN. Una vez alguien dijo esto y quizá me equivoque con los detalles pero esto se parece bastante a lo que pasó.

Hemos creado una estructura que no está funcionando. Incluso lo dicen los funcionarios de protección de datos que en principio están de acuerdo pero que en realidad dicen que somos demasiado exigentes, demasiado protectores de la información porque la legislación de protección de datos se aplica solamente a las personas físicas. Nosotros les hemos dado a los registros y registradores el derecho de aplicar eso también a las personas jurídicas, a cualquier persona. Esto se aplica solamente en ciertas áreas o zonas pero les hemos dado a los registradores y registros el derecho a ignorar las ubicaciones geográficas y a aplicar esto en forma universal.

Esto lo mencionó uno de los representantes de los registros, que es de Donuts. Los registros no reciben muchos pedidos pero los nuevos gTLD son registros amplios, *thick*, que tienen toda la información. Aquí está el funcionario de protección de datos de Donuts que recibe todas las

solicitudes. No recibe muchas. Quizá algunas por año. Unas 70 por año pero empezó a procesar estas solicitudes y una parte importante del proceso tiene que ver con lograr un equilibrio, ver las necesidades en pugna de los beneficios de dar la información al que la solicita versus la protección del registratario, la privacidad del registratario.

Cuando la persona de Donuts presentó ese informe hace un mes, de las 100 solicitudes que había resumido, nunca tuvo que hacer esta prueba de equilibrio, lograr este equilibrio, porque de las solicitudes que resultaron ser válidas que tenían toda la información correcta, que no eran formularios con espacios en blanco, a todas esas solicitudes no se aplicaba el GDPR porque eran personas físicas o por la persona geográfica a la que se aplicaban. No hacía falta considerar eso. Este tema de lograr el equilibrio se debatió mucho pero en el caso de la persona de Donuts no tuvo que buscar este equilibrio. Es un entorno interesante. La próxima diapositiva, por favor.

Las cuestiones que tuvo el ALAC en la fase uno tienen que ver con esta distinción entre personas jurídicas y naturales o físicas, que en nuestro caso pensamos que se sobreaplicaron. Luego la diferenciación geográfica. No todas las reglas se aplican de manera uniforme a todos. Hubo consenso en ALAC para que se identificara esto como una cuestión. Luego, el campo de la organización. Aquí también surgieron algunas inquietudes. Estuvimos dispuestos a aceptarlos hasta que la junta planteó que no. También el tema de los registradores, que quieren la opción de suprimir información. Ahora hay una guía de implementación que puede decir que el registrador puede suprimir la información pero tiene que mantenerla reservada. Si alguna vez surge

una cuestión de propiedad, la pueden recobrar pero no será proporcionada ni siquiera cuando haya una solicitud de acceso. Como dije, las indicaciones de política no funcionan ni siquiera en la implementación actual. Esto es un problema a futuro. Siguiente diapositiva.

Es el comienzo del trabajo de la fase dos. Aquí le paso la palabra a Hadia, a menos que ella tenga algo que decir. Estoy reservando el tiempo para preguntas para después. Lo haremos cuando terminemos la presentación, que está por la mitad más o menos. Agrupamos todas las preguntas al final. Hadia.

HADIA ELMINIAWI: Gracias, Alan. Aquí estamos. Comenzamos la fase dos del EPDP que principalmente trabaja sobre identificar quiénes pueden tener acceso a los datos y bajo qué circunstancias pueden divulgarse estos datos, los campos de datos que se divulgarán en relación con cada una de las solicitudes… No olviden que las solicitudes se corresponden con un propósito y dependiendo del propósito se determinan los campos de datos. Los medios a través de los cuales un usuario puede presentar una solicitud al sistema, los medios a través de los cuales él puede recibir efectivamente una respuesta en caso de que la respuesta sea que puede tener acceso, cuáles son los medios luego de divulgación…

Primero, para determinar quién puede tener acceso al sistema en este trabajo consideramos distintos casos de uso posible. Los distintos grupos interesados presentaron casos de uso posibles. Por ejemplo, el ALAC presentó dos casos de uso. Qué pasaría por ejemplo si un usuario

final de la Internet solicita los datos de un nombre de dominio y el otro, el caso de los organismos de defensa del consumidor. Otros grupos presentaron casos de uso de la vida real. Todo esto es para determinar los distintos usos que puede tener el sistema. Cuando hablamos de los medios de presentación de una solicitud o los medios de divulgación, aquí estamos hablando de un sistema. Un sistema a través del cual los solicitantes o los usuarios pueden presentar una solicitud y esta solicitud sería evaluada. Dependiendo de la evaluación se toma la decisión de divulgar o no los datos y de cuáles serán los campos de datos que se divulgarán.

La fase dos del EPDP también se refiere a aquellos temas que fueron postergados de la fase uno tales como la distinción entre personas jurídicas y físicas. Ese es un ejemplo. Eso es algo de lo que hablamos ayer. En ese sentido está el estudio y dependiendo de los resultados del estudio que se está realizando vamos a seguir considerando el tema. ¿Podemos mostrar la siguiente diapositiva, por favor?

Al analizar los distintos medios de presentación de las solicitudes y los medios para hacer la divulgación, aquí nuevamente estamos considerando el sujeto de datos. Nosotros pensamos que elementos importantes son que el interesado, que el sujeto de datos, tenga control de los datos. En primer lugar, tenemos que ver cuáles serán los datos que serán recopilados. Si el interesado sabe cuáles son los datos que están en manos y de quién y cuál es el periodo de retención, ahí se puede definir qué datos se pueden divulgar.

En el EPDP 2 en relación con el sistema de acceso estandarizado queríamos ir con esto un poquito más allá. Al tener un sistema estandarizado que puede responder efectivamente a las solicitudes, el sistema es más previsible. Así el usuario sabe con exactitud bajo qué circunstancias pueden compartirse los datos con otros. Esto es muy importante para nosotros. ¿Por qué es importante tener un sistema estandarizado? Si tenemos 2.500 registradores y cada uno aplica sus propios términos a la hora de recibir una solicitud de divulgación de los datos de un nombre de dominio, esto generaría inconsistencia y también el sistema perdería previsibilidad. Aquí lo que estamos evaluando o queriendo tener es un sistema transparente y previsible.

Por otra parte, en lo que hace a los solicitantes, debemos garantizar que el sistema sea consistente. Un sistema en el que los solicitantes puedan recibir respuestas a sus solicitudes. Como dijo Alan, tal como estamos ahora y aun cuando hayamos completado la fase uno, los solicitantes que presentan solicitudes con fundamentaciones legítimas aun así no reciben los datos por el tema del GDPR. Los grupos, las partes interesadas, no son las de ICANN las que plantean el problema sino el GDPR. Después de trabajar elaboramos este sistema estandarizado y queremos hacer incluso un modelo de acceso unificado porque podemos tener un sistema estandarizado de acceso y divulgación pero aun así tendremos un sistema distribuido porque todos los datos, como ustedes saben, residen en los registros y registradores. Aun cuando podamos tener estándares, es decir, un sistema estandarizado, la distribución no será unificada. Tampoco será óptima porque será el registro o el registrador el que tendrá que

aplicar los estándares y la forma en que se aplican podrá diferir según la institución. La idea es tener un modelo de acceso unificado. Todavía no sabemos cómo será este modelo. Ni siquiera sabemos si es factible. No obstante, es lo que procuramos tener. Con esto le devuelvo la palabra a Alan.

ALAN GREENBERG: Gracias. Siguiente diapositiva. El título de esta diapositiva es necesario que lo explique para aquellos que no hablan inglés. El elefante en la habitación es una expresión en inglés que se refiere a aquella cosa que todos saben de qué estamos hablando, que no se puede ignorar tal como no podemos ignorar, imagínense que hubiera un elefante en esta sala, pero nadie habla de esto o se ignora el tema porque es muy difícil o algo por el estilo. El elefante en esta sala es que si vamos a tener un método de acceso estandarizado con uniformidad, cómo lo hacemos.

Recordarán que en la fase uno dijimos que todavía no habíamos determinado quiénes eran los responsables del tratamiento, que es una definición técnica en la ley de protección de datos. Es aquella entidad responsable de controlar las cosas, del procesamiento de los datos. Este responsable del tratamiento es el que divulga los datos. Supongamos que hubo una reclamación, puede haber una penalidad que se imponga al responsable del tratamiento, incluso acciones jurídicas. Por ahora hablemos solamente de las penalidades impuestas por las autoridades europeas de protección de datos. En un modelo simple de acceso estandarizado, ICANN estaría a cargo de esto

y decidiría si se divulga o no la información. Si hay un problema, el registrador o el registro pagarían la penalidad o la multa. Eso no lo van a aceptar. No vamos a hablar de una multa del 4% de los ingresos brutos en el peor de los casos. No vamos a tomar esa decisión.

Si no tenemos este tipo de cosas, por lo menos en algunos casos, entonces número uno, volveremos literalmente al proceso manual y los procesos manuales no son prácticos para muchos tipos de solicitudes. Si alguien tiene una marca… Tomemos cualquier marca aleatoria al azar. La marca Facebook, por ejemplo. Hay muchísimas personas que prestan atención al dinero que gana Facebook y se preguntan: "¿Podríamos sacar un poquito de dinero legal o ilegalmente?" Hay muchos nombres de dominio que se asemejan a Facebook con otros códigos de escritura. Se pueden usar otras técnicas para convencer a la gente de que uno es Facebook. Se pueden aplicar otros nombres. Podemos incluso hablar de empresas que nos gustan, no de Facebook.

Para proteger este tipo de marcas que pueden tener miles de hits, miles de entidades que quieren usar lo nuestro, esta marca, ese es un tema. Otro tema es ciberseguridad. Sabemos por ejemplo que la gente que maneja botnets y cosas así puede registrar 10.000 nombres de dominio con una sola pasada. Puede haber muchísima información que uno quisiera conseguir para luchar contra este tipo de cosas. Estamos hablando de volúmenes que pueden ser altísimos. Es necesario encarar estos temas rápidamente y no ponerlos en una lista que va a una cola que vuelve la respuesta tres meses después. Hay una necesidad de tener un sistema que sea parcialmente automatizado.

También habrá decisiones que habrá que tomar manualmente porque siempre preguntas qué hacer pero la pregunta es si hay alguna autoridad centralizada, podrá tomar estas decisiones y asumir la responsabilidad.

Recuerden que hablamos del encargado del procesamiento. En este momento existe la presunción generalizada de que tanto la ICANN como nosotros definimos política. No podemos evitar ser un controlador, un responsable del tratamiento porque definimos las normas pero también los registros y registradores pueden ser responsables del tratamiento, ya sea conjuntos, independientes. Eso todavía no está claro. La pregunta es si la ICANN puede tomar esta decisión y asumir la responsabilidad. ¿Está la ICANN dispuesta a asumirla? Aparentemente la indicación que se percibe es que sí, que ahora esto lo permitirá la normativa sobre protección de datos. Estamos viendo cómo construir un sistema pero todavía ni siquiera sabemos si es lícito o si va a ser aceptado. En este momento está siendo puesto a prueba. La ICANN presentó varias preguntas a la autoridad europea de protección de datos. Esperamos que nos den respuestas y ciertas guías pero mientras tanto vamos tratando de construir un sistema bajo la presunción de que nos van a permitir hacer alguna de estas cosas o todas ellas pero no estamos seguros.

¿Dónde estoy? Es claro que en lo que hace a las solicitudes por razones de ciberseguridad o en el mismo sentido de propiedad intelectual estas tienen que seguir ciertos patrones. Si evaluamos 100 de ellas, de esas solicitudes, si todas son del mismo nombre de dominio y uno puede demostrar que es el propietario de una marca, podemos

desarrollar sistemas de computación para que desarrollen estos patrones también. Es concebible que lleguemos a ver que este tipo de decisiones pueden tomarse de una manera automatizada para algunas clases de solicitudes. Quizá para aquellas solicitudes de gran volumen. Eso es lo que nosotros queremos.

Siempre habrá algunas solicitudes que son subjetivas y habrá que tener decisiones tomadas por seres humanos. ¿Cómo se van a procesar estas? ¿Podemos aceptar todas ellas de una misma manera unificada en lo que hace a su registro y a su seguimiento? Luego el tema del equilibrio con las partes contratadas. Las partes contratadas no solo tienen la información del WHOIS sino también la información de sus clientes. Ellos tienen mucha más información sobre quién es el registratario que no es parte del WHOIS y esas informaciones nunca van a salir del registrador. Siempre habrá un gran número que bajará a este nivel. La pregunta es: ¿Podemos tomar la parte superior solamente y asegurarnos de tener un sistema de reporte y seguimiento uniforme? Ese es el gran trabajo esencial con el SSAD. Esperamos tener una respuesta más o menos para enero de la autoridad de protección de datos. Esperemos que esté en su agenda de la reunión de diciembre al menos. En enero quizá estemos en mejor situación de saber si lo que queremos hacer es posible, es lícito o que está fuera de lugar.

También hay otras cuestiones. Una de las cuestiones que ha surgido es si uno como persona jurídica, o sea, una empresa, uno pone la información de contacto. Dice: joanna@icann.org, por ejemplo, y esa información se da a conocer y hay un reclamo, ¿ante quién reclama uno? Reclama ante la persona que dio a conocer el dato o reclama

ante el registratario o la entidad jurídica que hizo la registración y que entró al dato. No hay una respuesta definitiva. Las distintas autoridades en Europa tienen distintas visiones, perspectivas diferentes. Tenemos uniformidad y eso se sabe. Podremos saber que si es una entidad jurídica, esta información se podrá dar aun cuando sea información personal porque es una persona jurídica. Por supuesto, hay que culpar a alguien pero no será a nosotros. Como dije entonces, las distintas entidades jurídicas tienen distintas visiones en Europa. Esto constituye un reto. Siguiente.

Vamos a recapitular entonces por qué nos interesa todo esto a nosotros. Los usuarios finales necesitan tener confianza en la Internet. En este momento el último número en julio, éramos 4.300 millones de usuarios. La confianza es importante. Hay mucho fraude, phishing, spam, todo tipo de cosas que usan muchísimo los nombres de dominio. Algo interesante que surgió en nuestras conversaciones es que uno de los usos más típicos es si uno hace phishing o malware distribuido a menudo lo que hace es entrar ilícitamente en el sitio web de una persona, se añade un software y se hace un phishing. La manera más sencilla de tratar el phishing es cancelar, bajar el sitio web pero ahora se está cancelando un sitio real que tiene un propietario real. Puede haber un club local, por ejemplo, y lo que solían hacer los hackers era contactar a las autoridades locales de los distintos clubes. Es muy interesante. A veces estas cosas funcionan al revés. Son contraproducentes porque no sabemos con quién estamos hablando. Es un desafío.

Los organismos de defensa del consumidor necesitan acceso y la remediación muchas veces depende del tiempo críticamente. Aquí como conclusión es que la gente no va a confiar en la Internet si no puede hacer clic en un vínculo y asumir que va a funcionar. Esto también se aplica al uso indebido del DNS. Si no se puede creer que va a funcionar, uno no va a depositar la confianza y no lo va a usar. No es que la gente vaya a dejar de usar la Internet pero es que el sistema no va a funcionar. Hadia, no sé si usted tiene algo más que agregar al respecto. Entonces vamos a abrir para preguntas. Espero que alguien haya llevado una lista adecuada de las personas que quieren hablar.

GREG AARON: Primero tenemos a Holly, Olivier, Tijani y John. Vamos a comenzar con Holly.

ALAN GREENBERG: Tenemos media hora. Imagino que es bastante tiempo pero tratemos de ser breves.

HOLLY RAICHE: Creo que usted mencionó que quizá haya alguna duda con respecto a que los organismos de protección del consumidor serían algunos de los que tendrían acceso a los datos.

ALAN GREENBERG: Yo dije que la protección del consumidor es un tema importante. Estamos hablando de los usuarios del SSAD que deberán ser

acreditados. Es decir, habría que buscar una forma de identificarlos o saber algo sobre ellos. Yo sospecho que los organismos de protección del consumidor gubernamentales y los privados también son grupos que podríamos acreditar y en los que podríamos tener confianza de que van a cumplir las normas. Si se les da información, se da información bajo ciertas condiciones muy estrictas. Es decir, solo se puede utilizar para los fines para los que se solicitó. Hay que destruir esa información cuando ya no es necesaria. Hay toda una serie de condiciones. Yo quisiera asumir y alguna gente del GAC también quisiera asumir que los departamentos de protección del consumidor serían uno de los grupos que van a terminar teniendo acceso a los datos. No les puedo dar una garantía, sin embargo.

HADIA ELMINIAWI: Hay algo que no mencionamos en la presentación. Ahora lo que estamos viendo es un sistema basado en la acreditación. Estamos viendo cómo se podría crear un sistema donde cada usuario del sistema debe estar acreditado, ya sea una entidad o una persona que pide la información a título individual. Deberán estar acreditados para poder utilizar el sistema. Sin embargo, estar acreditado no significa que van a tener acceso a los datos u obtener los datos. El tema es que para usar el sistema hay que estar acreditado.

GREG AARON: Tijani, ¿quiere responder?

TIJANI BEN JEMAA: Yo sugiero que Hadia y la otra persona recojan todas las preguntas y las contesten todas juntas al final. Si no, no habrá tiempo.

GREG AARON: Le doy la palabra a usted, Maureen. Olivier.

OLIVIER CRÉPIN-LEBLOND: Gracias, señor Presidente. Tengo dos preguntas muy breves. La primera tiene que ver con lo que estuvo hablando sobre la lista de correo electrónico del EPDP. Hay muchos emails que entran allí y una oposición muy clara con respecto a cualquier tipo de automatización del sistema. Yo entiendo que básicamente esto está destruyendo el sistema en sí mismo, como usted explicó correctamente. ¿Hace falta consenso de todo el grupo para pasar la automatización o por lo menos para que parte de la automatización funcione?

ALAN GREENBERG: Haga la segunda pregunta y después respondo.

OLIVIER CRÉPIN-LEBLOND: La segunda pregunta tiene que ver con… Me la acabo de olvidar. Vuelvo a pedir la palabra después.

ALAN GREENBERG: En primer lugar, hay personas en el grupo que tienen posiciones muy diferentes. Hay algunas personas que creen que nunca vamos a poder desarrollar un sistema con ningún tipo de automatización. Puede ser

asistencia, ayuda en la automatización que nos diga: “Esta persona sí está acreditada” pero siempre será una persona física que tomará la decisión en todos los casos. Hay otros que opinan que una vez que se recibieron mil pedidos y son todos parecidos y dijimos: “Sí, ¿hay que analizar el siguiente millón de pedidos en forma manual?” No sería lógico hacer siempre las mismas cosas y esperar respuestas diferentes.

¿Necesitamos consenso pleno? Bueno, es lo que buscamos de hecho. En última instancia, el PDP, como todos los PDP, tiene reglas con respecto a la definición del consenso. Depende del presidente y hay otros procesos que definen eso pero tratamos de llegar a una solución que todo el mundo pueda aceptar. Gracias.

OLIVIER CRÉPIN-LEBLOND: Acabo de recordar mi segunda pregunta y tiene que ver con el escenario de casos de uso, un tema que trató la comunidad y algo que nosotros sugerimos. Los usuarios finales deberían poder consultar información. ¿Qué pasó con esos escenarios? ¿Fueron útiles? ¿Se utilizaron o fue simplemente un ejercicio que no sirvió para nada?

HADIA ELMINIAWI: Yo diría que fueron útiles, en especial nuestro caso de uso. Pudimos presentar un caso real para decir que no estábamos hablando de usuarios que tienen curiosidad, que están tratando de ver quién registró este nombre de dominio o el otro. Yo diría que sí, fueron útiles. No estoy segura sobre si incluyeron los casos de uso o no pero sí, fueron útiles. Trabajamos con grupos de usuarios y también de esto

surgió muchas recomendaciones en relación a las salvaguardas, con respecto a los pedidos, qué se debe incluir en el pedido y cómo deben darse las respuestas.

ALAN GREENBERG: Creo que se decidió que esto va a formar parte del trabajo que hicimos pero no va a estar en el informe final porque los casos de uso no se diseñaron para ser completos y abarcativos. En algunos casos podrían llevar a error o confusión.

GREG AARON: Tijani.

TIJANI BEN JEMAA: Muchas gracias. Alan, no entiendo bien su ejemplo de que una autoridad de protección de datos aceptara que se publicaran datos no públicos cuando el registrador se negó a informarlos porque el GDPR dice que los que recaban, procesan, transfieren, etc. los datos son los que designan al DPO. En el encargado de protección de datos está dentro del registrador. El registrador tiene los datos. El registrador recaba los datos, los procesa. No entiendo cómo funcionaría eso. Esa sería mi pregunta.

ALAN GREENBERG: El que pide la información no es el encargado de protección de datos del registrador. Estoy hablando del organismo de protección de datos del país. No es una persona que trabaja para el registrador.

TIJANI BEN JEMAA: Entonces el encargado de protección de datos según el GDPR está designado dentro de la entidad que recaba los datos.

ALAN GREENBERG: Me referí a un pedido de la autoridad de protección de datos del país que interpretó la ley y consideró que este era un pedido razonable y el registrador no estuvo de acuerdo.

OLIVIER CRÉPIN-LEBLOND: Creo que Alan habló de oficina de protección de datos.

TIJANI BEN JEMAA: ICANN es el responsable del tratamiento de datos porque los datos no están en manos de la ICANN. Están manos de los registradores. La ICANN deberá soportar las sanciones porque es el responsable del tratamiento pero no tiene los datos. Yo creo que esto va a ser un tema muy difícil. Tengo otro punto muy importante que tiene que ver con el responsable del tratamiento de datos. Perdón, me olvidé de lo que iba a decir.

ALAN GREENBERG: No hay duda de que la ICANN es responsable del tratamiento. Nosotros estamos aquí y redactamos las políticas. No hay forma de que no seamos los responsables del tratamiento de datos. ¿Somos los

responsables únicos? ¿Compartimos esta responsabilidad? Son buenas preguntas.

GREG AARON: Humberto.

HUMBERTO CARRASCO: Gracias, Alan. Voy a hablar en español.

HADIA ELMINIAWI: Con respecto a la pregunta de Tijani… Es un comentario. Ustedes deben saber que cuando hablamos de responsabilidad hay diferentes responsabilidades en relación a diferentes acciones. Si hablamos de responsabilidad en relación a la comunicación, esto es diferente según estemos comunicando datos a través de la ICANN u otra entidad o si estamos divulgando información a través de los registradores. Cuando hablamos de la toma de decisiones, la responsabilidad corresponde a los responsables de la actividad. Cuando hablamos de transferir la responsabilidad de las partes contratadas a la ICANN, por ejemplo, o a otra entidad, no estamos hablando de transferir toda la responsabilidad. Estamos hablando de transferir la responsabilidad respecto de ciertas acciones o actividades pero el primer grupo sigue siendo responsable de ciertas acciones.

ALAN GREENBERG: Cuando hablamos de cambiar la responsabilidad, esto es un resumen que se refiere a ciertos términos legales que no incluyen esas palabras.

HUMBERTO CARRASCO: La verdad es que yo quiero agradecer la presentación. Creo que resumió bastante bien la problemática. También tenía como primera pregunta el tema de la responsabilidad. Yo creo que no cabe la menor duda de que ICANN, al dictar la política, tiene algún grado de responsabilidad que corresponderá determinar en algún caso concreto que se produzca, cuál es. Distinto también de las partes contratantes. Pero no hay duda a mi juicio de que sí tiene algún grado de responsabilidad.

Lo que sí me causa un poco de temor, no puedo decirlo de otra forma, es que todo este trabajo que se ha hecho depende un poco de las consultas que usted hace, y me refiero como ICANN, a la Comisión Europea. Dependemos de la respuesta de ellos para ver cuál es la decisión que vamos a adoptar. Estamos trabajando sobre supuestos que dependiendo de la respuesta que nos den vamos a tener que variar la dirección o las alternativas que estamos tomando y eso en realidad produce mucha inseguridad. Me refiero a inseguridad de todo tipo. Se han gastado recursos, se ha gastado tiempo. Aun así, podemos tener consejo de expertos desde el punto de vista legal con distintas culturas porque le garantizo que la opinión de un abogado en Estados Unidos va a ser completamente diferente a la opinión de un abogado en la Unión Europea.

Yo pregunto si eso, estando desde afuera, por supuesto que debe haber sido tomado en cuenta por ustedes pero lo que en realidad me preocupa es que lleguemos a fin de año y no tengamos certeza de cuál

va a ser realmente el resultado del camino a seguir dependiendo de lo que nos diga la Comisión Europea. Esa es mi gran cuestión.

ALAN GREENBERG: No está claro que vayamos a recibir una respuesta que nos sirva. Quizá no recibamos una respuesta que nos sirva. Quizá haya una respuesta que rechace ciertos puntos pero que nos diga que otros puntos estén correctos. Ahora, trabajar así tampoco sirve mucho. No queremos crear algo, crear un sistema complejo y después escuchar que nos diga: "Esto no es lícito". Esperemos que esto no pase. La forma en que están trabajando los encargados de protección de datos y la junta de protección de datos de la Unión Europea no es dar respuestas iniciales sino dar respuestas después. Estaban presentando normas y documentos. ¿Todo esto es muy complejo? Sí. ¿Hay un camino claro a seguir? No. ¿Podemos elegir otra cosa que no sea seguir adelante? No. No tenemos otra opción.

HADIA ELMINIAWI: Usted dijo correctamente que ICANN org mandó una pregunta a la junta de protección de datos de la Unión Europea sobre el GDPR y esa respuesta influye sobre nuestras decisiones de políticas. Dicho esto, si nos dicen que esto no es posible desde el punto de vista legal, no es lícito, descartaremos esa opción y cuando redactemos la política no haremos estas cosas que nos dijeron que no se pueden hacer. Eso sería muy útil. Por otro lado, si nos dicen que esto es lícito, esto no significa que sea la política que vayamos a implementar o a redactar. Tiene sentido que se adopte de todos modos.

Otra vez, esa información influye sobre nuestras decisiones en materia de políticas pero no las define estrictamente. Estamos esperando las respuestas y sí, quizá la respuesta nos cambie completamente lo que estamos haciendo o aporte algo a lo que estamos haciendo.

ALAN GREENBERG: Hay opiniones divididas aquí. Hay algunas personas a las que no les importa lo que diga la oficina de protección de datos de la Unión Europea.

GREG AARON: Seun, tiene la palabra.

ALAN GREENBERG: Nos quedan 20 minutos.

SEUN OJEDEJI: Muchas gracias. Algunas de mis preguntas ya fueron respondidas pero simplemente quiero pedir un poco más de información. El trabajo del grupo ha considerado el GDPR en detalle y creo que en lo que se refiere a la Internet, este es uno de los grupos que estudió más en detalle el GDPR a nivel global. Quería confirmar simplemente si bien el GDPR es muy bueno, quizá esperábamos que hubiera dicho algo diferente. Si bien pienso que el EPDP no iba a incluir esto dentro de su alcance, quisiera saber si hay un grupo dentro de la ICANN que esté pensando en posibles mejoras al GDPR. No sé si esto estaría dentro del ámbito de la ICANN. Personalmente, creo que hay algunas cosas que veo en el

GDPR… No sé si cuando se redactó el GDPR se tuvo en cuenta específicamente la Internet. Quiero ver si se está considerando esta ventana, si se está pensando en eso. Yo creo que el grupo actual está trabajando mucho y si su trabajo ayuda a mejorar el GDPR, esto sería muy positivo.

ALAN GREENBERG: Escuché a personas que entienden esto decir que la Comisión Europea cuando redactó el GDPR no tenía ni idea de cómo operaba el WHOIS ni sabía que no era una única base de datos que manejaba la ICANN. Hay otras personas en puestos similares que dijeron: "Por supuesto que la Comisión Europea sabía todo esto". Se está trabajando en la Comisión Europea en este momento para analizar una revisión para el 2025-2026. Esto no va a resolver nuestros problemas. ¿Estamos trabajando con estos grupos y personas? Hay personas de la Comisión Europea trabajando en el EPDP. Sospecho que quizá participen de esas actividades aunque nunca les pregunté. Creo que nadie de la ICANN está trabajando con ellos de manera explícita por lo menos en la actualidad pero se está tratando este tema, se está hablando de las revisiones y por supuesto toda legislación de este tipo deberá ser revisada.

SEUN OJEDEJI: Yo sugiero hacer un seguimiento de lo que pasa en ese proceso para ayudar a mejorar el GDPR para cuando surja la nueva versión.

ALAN GREENBERG: Creo que las personas de ciberseguridad de diferentes países de Europa que están luchando para sobrevivir son los que deben asesorar a sus gobiernos sobre los cambios necesarios en esta legislación.

SEUN OJEDEJI: Si nosotros no queremos participar, está bien.

MATTHIAS HUDOBNIK: Hadia y Alan, muchas gracias por la información actualizada que nos dieron. Tengo dos preguntas. La primera es la siguiente. Quisiera que ustedes nos digan, desde un punto de vista realista, si opinan que creen que podemos llegar a un modelo de acceso unificado al final. La segunda pregunta tiene que ver con el modelo de acreditación. ¿Hay un modelo que ya exista? Hay uno que ha presentado WIPO, o que presentaron las autoridades de aplicación, hay otro que presentaron Pricewaterhouse. ¿Cree usted que hay algún modelo ya aceptado? ¿Algunas tendencias que nos indiquen si vamos en esta dirección o en aquella? Gracias.

HADIA ELMINIAWI: Gracias por las preguntas. ¿La primera pregunta era?

MATTHIAS HUDOBNIK: Mi primera pregunta tenía que ver con el modelo de acceso unificado, si es posible o no.

HADIA ELMINIAWI: Mi opinión personal es que si es lícito tener un modelo de acceso unificado, el desarrollado por el grupo técnico y el que fue presentado ante la junta de protección de datos de Europa, si esto es lícito, sí. Existen grandes probabilidades de que esto sea adoptado e implementado. Quiero decirles que los que van a apoyar esto más explícitamente, si es lícito tenerlo, van a ser las partes contratadas porque ya no serán responsables por la divulgación de los datos. Seguirán siendo responsables por los demás aspectos del procesamiento pero de esa parte ya no serán responsables, si es que logramos este modelo unificado. No lo sé. Depende de las respuestas que recibamos de la junta de protección de datos europea. Si este sistema les quita la responsabilidad con respecto a la divulgación de los datos. Si no resulta así, entonces no. No creo que este sistema se implemente porque podemos tener diferentes modelos de acceso unificado y diferentes modelos para un sistema estandarizado de acceso. Podemos tener un sistema de acceso estandarizado distribuido o centralizado. Por ejemplo, puede haber un sistema único a través del cual se reciben las solicitudes y quizá también se comuniquen las respuestas pero distribuido porque cada parte contratada debería decidir si divulgar o no la información. Hay muchos modelos posibles. La Junta de Protección de Datos Europea recibió la pregunta con respecto a un modelo específico pero hay muchos modelos posibles. Una vez más, yo creo que tendremos un sistema estandarizado para acceso y comunicación. ¿Qué forma tomará este sistema? No sabemos. Hay diferentes tipos de modelos.

MATTHIAS HUDOBNIK: La segunda pregunta tenía que ver con el modelo de acreditación.

HADIA ELMINIAWI: Lo que hemos tratado de hacer es desarrollar políticas para un modelo de acreditación que se utilizara como modelo estandarizado de acceso y divulgación. No hablamos todavía de qué entidades podrían formar parte de este modelo o qué entidades podrían ayudar aquí. Estamos estableciendo principios amplios diciendo que habrá que contar con una autoridad de acreditación. ¿Quién va a ser esta autoridad? No sabemos pero creemos que podría ser la ICANN. Dicha autoridad de acreditación deberá acreditar a una entidad para que acredite a los usuarios o para que acredite a muchos. Se podrían poner en contacto también con otras entidades para que hagan la acreditación pero estamos estableciendo los lineamientos generales, definiendo quién debe ser acreditado. Como dije antes, estamos viendo que todos los que utilicen el sistema deben estar acreditados y estamos hablando de usuarios u organizaciones. Esta sería mi respuesta.

ALAN GREENBERG: En resumen, vamos a tener un sistema. Si va a estar automatizado o no, no sabemos. Va a haber acreditación pero cómo funcionará esta acreditación todavía no sabemos. Estamos trabajando sobre el tema. Se nos está acabando el tiempo. Les pido que las preguntas y respuestas sean muy breves.

GREG AARON: Tenemos cinco personas que pidieron la palabra. Vamos a tratar de hacer todas las preguntas y respuestas en estos cinco minutos. Tenemos una lista de varias personas.

JAVIER RUA JOVET: Gracias, Hadia y Alan. No es un tema de fondo sino de proceso. Un proceso del tipo expeditivo, ¿se espera que vaya a constituir la base de futuros procesos PDP 3.0? ¿Es este o es una medida de tipo extraordinario?

ALAN GREENBERG: El PDP expeditivo es uno de los múltiples procesos de desarrollo desarrollados pero es la primera vez que se usa. Algunos piensan distinto pero no necesariamente es algo que se use cuando hay un cataclismo con estructuras específicas. Se usó porque hay algo que es muy importante hacer pero no es controversial. Eso importante pasar por alto procesos que son de un PDP tradicional que tardan un año, un año y medio. Aquí no hay, por ejemplo, necesidad de informes de cuestiones u otros informes. Es un proceso que puede usarse tanto para cosas cataclísmicas como triviales. Es una de nuestras armas. PDP 3.0, yo no voy a hablar de eso en este foro.

JOANNA KULESZA: Es una tarea gigantesca. Felicitaciones. Es sorprendente. Espero que el ejercicio del ATLAS III salga bien. Gracias. Me impresiona la conversación que hubo en la sesión anterior y no estoy haciendo profecías ni nada por el estilo pero pregunto qué pasa si no lo

logramos. Qué pasa si no conseguimos un modelo unificado. ¿Se está considerando? O dando vuelta a la pregunta, ¿sería más fácil si de alguna manera fragmentáramos la red, tener GDPR en la Unión Europea y otros marcos? Es una pregunta tonta. Me puede decir: "Joanna, eso no va" pero gracias igual.

ALAN GREENBERG: Hay 175 normativas en curso o aplicadas. No vamos a volver atrás a tener más privacidad. El mundo cambió. Nos guste o no, es así. El mundo cambió. Estamos trabajando con el GDPR porque es un marco conocido y divulgado pero no es el único. Esa es una realidad. ¿Qué pasa si nosotros no logramos ningún tipo de acceso estandarizado? Bueno, lo que pasa hoy. Uno va al registro, el registrador puede responder o no con distintas normas. El mundo va a seguir andando. Bien o mal pero las chances es que tendremos un ingreso centralizado. Probablemente con cierto nivel de acreditación porque esto les va a ayudar al registro y al registrador en sus respectivas decisiones, por lo menos a saber quién es usted, si es alguien confiable o promete una serie de cosas. Saber si usted es una buena persona o no. Tendrá algún tipo de organización aun cuando no sea un proceso de decisión centralizado. Si no se consigue, el mundo seguirá dando vueltas. Habrá más o menos malware, lo que fuera, la gente de propiedad intelectual se va a rasgar las vestiduras, quizá porque no podrá hacer acciones legales. El mundo va a seguir andando.

HADIA ELMINIAWI: La verdad es que yo no veo que terminemos con nada. Sin duda va a haber algún producto final, ya sea un sistema uniformado o estandarizado. Cuán uniformizado o cuán estandarizado, de eso estamos hablando.

BARTLETT MORGAN: Primero felicitaciones por el enorme trabajo realizado. Muchísimo trabajo. Hay que decirlo. Pero rápidamente ahora, mucho de lo que oía antes tiene que ver con el tema de la responsabilidad que tiene la ICANN como responsable del tratamiento. Recuerdo que hace dos meses se hablaba del ID de moda. Hay que aclarar entonces el nivel de responsabilidad que tiene la ICANN como responsable del tratamiento.

ALAN GREENBERG: Nosotros no hemos determinado quién es el responsable conjunto, el independiente o qué. Hay algunos reclamos que dicen que para muchos de los datos recopilados, la ICANN es el único responsable. Por supuesto, no todos están de acuerdo. En definitiva, las reclamaciones tendrán que ver con el hecho de si los comisionados de datos europeos están de acuerdo o no.

BARTLETT MORGAN: Es como el huevo y la gallina. Como usted dijo antes, son 170 y pico normativas distintas. Cada una tiene una visión distinta de la noción del encargado del tratamiento, si existe o no. Es una pregunta difícil.

ALAN GREENBERG: Son normas distintas. Además, son distintas personas las que interpretan las mismas leyes. Pueden tener distintas visiones. La Autoridad Europea de Protección de Datos está haciendo este intento de aportar cierta unificación o consistencia en este universo de países europeos pero eso todavía no está garantizado.

GREG AARON: Tijani.

TIJANI BEN JEMAA: Muchas gracias. No me imagino poder vivir en un mundo sin ningún modelo estandarizado o unificado porque, en definitiva, la ICANN tiene ciertas responsabilidades que podrán ser afectadas por lo que ocurra si hay un problema con el registro o el registrador. Que cada uno tenga su propia norma, su propia forma de hacer el acceso, no me parece que ICANN pueda subsistir con eso.

ALAN GREENBERG: En definitiva, siempre habrá casos complejos que será una cuestión de criterio y es el registrador el que aplicará ese criterio al final, hasta qué punto va a actuar de manera similar a los otros registradores este nivel de consistencia, quién lo sabe.

GREG AARON: Dev.

DEV ANAND TEELUCKSINGH: Hola. Felicitaciones. Me hago eco por el enorme trabajo realizado. Mi pregunta, intentando entender, las direcciones IP, ese tipo de cosas, el WHOIS y las direcciones IP, hay un sistema de quién tiene o no acceso a la dirección IP. ¿El EPDP considera este aspecto también o eso ya está resuelto, ya está manejado? A ver, qué está pasando.

ALAN GREENBERG: Eso no lo estamos analizando. Estamos analizando el WHOIS de nombres de dominio gTLD solamente. Los distintos organismos tienen distintas posiciones. Están los ccTLD europeos, que publican información personal. Los RIR han decidido que hay razones legítimas para publicar información personal en algunas partes de su WHOIS de direcciones IP. Hay otras decisiones, hay otros abordajes que según la normativa varían. La verdad es que no estamos considerando eso. La gente ha planteado esos ejemplos de por qué no podemos hacer ciertas cosas. En general, a la gente no le importa lo que nosotros hagamos.

GREG AARON: Gracias por todas las preguntas. Alan, no sé si usted tiene algún comentario final.

TIJANI BEN JEMAA: Un último comentario. Los ccTLD están fuera de esta discusión porque la ICANN no tiene ningún contrato con ellos. No es un tema para la ICANN.

ALAN GREENBERG: Gracias por todos los comentarios.

HADIA ELMINIAWI: Gracias.

ALAN GREENBERG: Hemos terminado 30 segundos antes.

MAUREEN HILYARD: Yo también quiero hacerme eco de los agradecimientos de la comunidad At-Large hacia ustedes por el enorme trabajo que han realizado. Absolutamente excelente. Muchas gracias por ello. La próxima sesión es una sesión de trabajo de At-Large con almuerzo.

GISELLA GRUBER: Es almuerzo para los líderes y los viajeros financiados y otros participantes que estén aquí. Les invito a que se sirvan el almuerzo ahí atrás. Si alcanza, vamos a invitar a todos los demás.

MAUREEN HILYARD: Por favor, vayan a buscar el almuerzo. Vuelvan. Nos organizamos y empezamos entonces con la sesión sobre el ATRT3 y la revisión del NomCom. Van a ser una presentación durante el receso para el almuerzo. Gracias.

[FIN DE LA TRANSCRIPCIÓN]