KOBE – Sesión de participación de la comunidad: grupo de análisis técnico sobre acceso a los datos de registración sin carácter público
Lunes, 11 de marzo de 2019 – 13:30 a 15:00 JST
ICANN64 | Kobe, Japón

RAM MOHAN: Buenos días. Vamos a comenzar con la sesión del grupo de análisis técnico de acceso a los datos de registración sin carácter público en un par de minutos. Gracias.

Buenas tardes. Soy Ram Mohan, el coordinador del grupo de análisis técnico de acceso a los datos de registración sin carácter público o TSG-RD. Tenemos unos 90 minutos para esta sesión. En la sesión esperamos dedicar 45 minutos de los 90 para hablar acerca del proceso que hemos atravesado y para presentarles un modelo técnico preliminar para ver cuáles son sus comentarios y sus aportes. Nuestra expectativa es que esta sea una sesión interactiva. No es la única sesión. Tuvimos una sesión ayer con el grupo de EPDP. Más tarde hoy y mañana nos reuniremos con muchos otros grupos también para mostrarles lo que hemos hecho hasta ahora.

Habiendo dicho esto, vamos a ver nuestra agenda. Tenemos pensado cubrir estos temas y esperamos tener mucho tiempo para responder cualquier pregunta que puedan tener. Creo que hay gente aquí que también se ocupa de recibir los comentarios

de participantes remotos. Vamos a responder esas preguntas también. Vamos a comenzar entonces con una especie de introducción acerca del grupo de análisis técnico propiamente dicho. Para establecer las bases y el contexto para explicarles cómo comenzamos y qué hacemos, le voy a dar la palabra a Göran.

GÖRAN MARBY: Gracias. Antes de comenzar quiero agradecerles a los miembros del grupo por el gran trabajo que han dedicado a lo largo de los últimos tres meses. Viéndolo de afuera siempre siento que es una bendición tener voluntarios que hagan este trabajo. ¿Por qué existe este grupo? En primer lugar, hablamos de algo que es interesante desde el punto de vista legal y que tiene una solución potencialmente técnica. Algunos temas que voy a repetir y que seguramente ya me escucharon decir 100 veces antes, la ley de GDPR es muy específica con respecto al rol de los procesadores y aquellos que controlan los datos, los que tienen los datos y toman decisiones acerca de los datos. Estas personas son quienes son responsables en función de GDPR. En nuestro mundo, estas son las partes contratadas. ICANN org, como entidad legal, no tiene la base de datos.

Sé que esto será una sorpresa para ustedes. Para nosotros, desde hace tiempo, es obvio que es difícil tener un modelo de

acceso unificado con un solo vehículo porque las partes contratadas como personas tienen esa responsabilidad legal. ¿Qué significa esto? Aun si tuviéramos una política… Quiero decirles que Steve Crocker ha estado trabajando para mí a lo largo de los últimos tres meses. Me encantó decir esto. Les pido disculpas.

Este es el supuesto que las partes contratadas tienen que tomar decisiones individuales. Comenzamos a analizar diferentes soluciones para ver cómo reducir la responsabilidad legal de las partes contratadas en relación con GDPR. No sé si recordarán que en Barcelona recibí una carta de casi todas las partes contratadas, creo, que dijeron: "¿Por qué no van a averiguar si hay alguna solución potencial para reducir la responsabilidad legal a fin de crear un modelo de acceso unificado?" Si no cambiamos la interpretación actual de la ley por parte de los DPA, va a ser muy difícil tener un modelo de acceso unificado porque ICANN org no puede hacer cumplir algo que va más allá de la ley. La ley siempre va por encima de la ICANN.

El contexto en el que comenzó este debate fue cuando hablamos también dentro de la Comisión Europea acerca de diferentes alternativas. Comenzamos a ver si ICANN podía ser el lugar donde se hicieran las preguntas. Lo que establecimos, que está basado en RDAP, es que ustedes vienen a ICANN org con una

pregunta. Esa pregunta se transfiere de manera segura de acuerdo con los principios del GDPR a las partes contratadas. Los únicos que pueden responder esa pregunta son mediante una respuesta que vuelva a la ICANN. Eso parece ser muy sencillo pero nos dimos cuenta de que también necesitábamos conocimientos técnicos profundos para que desarrollar este modelo.

En lugar de que nosotros dentro de ICANN org nos sentáramos a desarrollar un modelo, yo decidí pedir a Ram que reuniera un grupo con especialización técnica para que analizara este tema. Ahora, por supuesto, la pregunta es qué va a pasar después de esta presentación. En primer lugar, espero ver cuáles son sus aportes con respecto a la solución que ellos desarrollaron. Posteriormente, lo que vamos a hacer es lo siguiente. Esta es una parte de todo el sistema. Este es el punto de intercambio. En forma paralela o de costado tiene que haber alguien que reconoce quién puede hacer las preguntas lo que en términos generales llamamos servicios de acreditación. Hay mucha forma de acreditación. Por ejemplo, tenemos EUROPOL. Hay partes de la comunidad que también buscan diferentes formas de tener cámaras de acreditación. Nosotros sugerimos hace mucho tiempo la OMPI.

Tenemos que conectar estas cámaras para poder validar la pregunta a través del mecanismo, hacer la pregunta y esta pregunta llega a las partes contratadas. Lo que hicimos fue reunir todo esto. Nuestra intención es volver a las autoridades de protección de datos para hacer una simple pregunta. ¿Esto reduce la responsabilidad de las partes contratadas? Si la respuesta es sí, aquí utilizamos la palabra: "Guía". La guía en la perspectiva europea es vinculante desde el punto de vista legal. Cuando la DPA da una respuesta por escrito a la pregunta, eso forma parte del proceso de toma de decisiones. Por lo tanto, esa es la palabra que prevalece. No pueden decir algo que no esté dentro del contexto legal.

La idea es que de hecho esto da a la comunidad de la ICANN, si ocurriera esto, la oportunidad de crear políticas para el modelo de acceso unificado. Quién debe acceder, qué pensamos nosotros con respecto a la privacidad y el acceso a la información. La intención no es asumir el control. El trabajo de políticas dentro de la ICANN apunta a informar a la comunidad de la ICANN acerca de las posibilidades legales para el modelo de acceso unificado o lo llamemos como lo llamemos.

Quiero advertirles que si ustedes hablan con las autoridades de protección de datos, van a decir que cada uno tiene que hacer su propio trabajo pero recibir guía legal de alguna autoridad de

protección de datos es algo con lo que tenemos que trabajar muy estrechamente, especialmente dentro de la Comisión Europea. Nosotros somos uno de los pocos que recibieron guía durante la última parte del proceso. Para que quede registrado, yo ya no puedo nombrar ningún otro proyecto dentro de la ICANN.

Esta es una de las problemáticas. Cuando comenzamos, recibimos guías de las DPA. Recuerden lo que decía la guía de la DPA. Podríamos recolectar datos. No especificaba cuáles pero podíamos recopilar datos. También decían que aceptaban que teníamos una especie de modelo con cierta información que era pública y otra información que no era pública. Esto fue una guía muy sólida y muy importante para nosotros. Sin eso, creo que nuestro trabajo habría sido mucho más difícil. Ahora estamos en una situación en la que no tenemos ese asesoramiento legal para la fase dos. Eso es lo que estamos tratando de resolver. Voy a abrir ahora el espacio para recibir preguntas.

ORADOR DESCONOCIDO: ¿No hay preguntas?

GÖRAN MARBY: Me siento muy solo.

ORADOR DESCONOCIDO: Yo tengo una pregunta. ¿Alcanza con reducir la responsabilidad? Hay muchas empresas que van a invertir miles de millones. ¿Alcanza con decir que existe la posibilidad de que se reduzca la responsabilidad? ¿No podemos tener una respuesta más precisa con respecto a qué es lo que las DPA no van a aceptar categóricamente?

GÖRAN MARBY: Eso depende de las DPA. El GDPR es interesante. Yo fui regulador y GDPR es interesante desde el punto de vista técnico. Tengo un mal sentido del humor. En algún momento lo llamé la suegra porque cuando yo era adolescente, mi mamá decía que yo podía salir si me portaba bien. Yo salía y me portaba bien, pero ella tenía otra perspectiva de lo que significaba portarse bien. Cuando alguien le dijo que me estaba portando mal, ahí es cuando yo tenía problemas. Esto pasa con la ley. La ley dice que uno tiene que hacer lo que le parece que es correcto. Siempre y cuando lo pueda explicar está bien. Pero si no está bien, lo vamos a castigar. Hay una interpretación bastante amplia. Eso es lo que crea uno de los problemas de esta ley porque las partes contratadas individuales tienen que tomar esa decisión por su cuenta. La ICANN, como entidad legal a través de nuestros contratos, tiene un gran problema en cuanto a hacer cumplir esto con las partes contratadas.

RUBENS KUHL: Tengo un comentario y una sugerencia. El comentario es que si bien una de las motivaciones es reducir la responsabilidad, existe el potencial de que este modelo reduzca los costos operativos en relación con el modelo de acceso unificado. Por lo tanto, hay incentivos positivos y negativos que también podrían tener un papel aquí. Mi sugerencia es que la ICANN no trate de hacer que este modelo sea obligatorio. Todo lo que es obligatorio en general recibe reclamos. Por qué se hace así, por qué se hace de otra forma. Quizá puede ser algo que sea opcional pero que tenga una sólida cobertura dentro del espacio de gTLD. Quizá esto sea más sólido que algo que sea obligatorio o algo que se impone. Es una idea.

GÖRAN MARBY: Con respecto al segundo punto, nosotros en la ICANN, en nuestros contratos ya tenemos lo que llamamos exenciones. La ley local o el derecho local va por encima de nuestros contratos y obligaciones. Ustedes podrán decir que esta es una exención muy importante. De hecho, comenzó en 28 países miembros. La ICANN no es y no debería estar en esta situación. Nosotros ya no podemos hacer cumplirlo si la ley local está en contra. Escuché ayer que alguien dijo que esto es un sueño. Nosotros dijimos que vamos a tratar de hacer esto. ¿Si le doy un 100% de

probabilidades? No. Pero me pareció que era lo suficientemente importante investigar la posibilidad de reducir la responsabilidad de las partes contratadas. Por supuesto, si lo aceptan. Esto es algo que ellos deberán aceptar porque esto también tiene que ver con la ley.

El asesoramiento de la DPA tiene que ser muy sólido desde el punto de vista legal de forma tal que se sientan seguros cuando alguien toma decisiones en nombre de ellos. Es difícil pero, por otra parte, la ICANN como institución es un sistema de voluntarios. Los contratos que tenemos con nuestras partes contratadas están basados en políticas desarrolladas por la comunidad, nuestro proceso ascendente. En cierta forma, en este modelo de consenso se aceptan estas políticas pero entiendo lo que usted dice pero nosotros no somos un gobierno.

ORADOR DESCONOCIDO: Tengo algunas preguntas. Les pido disculpas. No soy parte del grupo… Me olvidé de la sigla… No sé si estos temas ya se trataron. Quisiera saber dos cosas. El GDPR les da a los usuarios más responsabilidad acerca de los datos. ¿Podría decirme por ejemplo si el dueño de un sitio web que quiere que la gente vea su información en ese nuevo modelo habría un casillero que diga: “Esta información es pública” o “Esta información debe ser confidencial”? Esta es la primera pregunta.

La segunda. Escuché que alguien de un registrador ayer le dijo a una señora que pedía acceso a los consumidores que querían verificar la autenticidad de un sitio web que lamentablemente, dado que los registradores no pueden diferenciar entre una persona y una empresa, no iban a hacer esa diferenciación directamente. ¿Es cierto eso? En primer lugar quisiera saber si es correcto que esta distinción entre personas individuales y empresas no va a existir en el nuevo sistema.

GÖRAN MARBY: Usted hace preguntas acerca de políticas que están en el PDP. Es un tema de políticas. Ni yo ni nadie de los que está aquí en esta mesa estamos involucrados en las políticas. Yo trazo una clara separación aquí porque creo que esa pregunta forma parte del grupo de trabajo sobre políticas. La solución técnica tiene un objetivo específico y es reducir la responsabilidad legal de las partes contratadas.

Yo acepto el hecho de que podría ocurrir que los legisladores o las DPA tengan opiniones acerca del PDP existente, lo cual podría tener un impacto pero todavía no tenemos una respuesta. Esto también es algo nuevo y hay muy pocos casos acerca de estos datos de privacidad. Con respecto a su primera pregunta acerca de si es posible hacer esta distinción, la verdad es que no sé la respuesta a su pregunta.

BENEDICT ADDIS: Soy Benedict Addis y trabajé también en el EPDP. Hablando desde el punto de vista del EPDP y no como miembro de este grupo técnico, puedo decirle que hablamos acerca de esta idea de que el titular de los datos de registro pueda publicar estos datos o no. La respuesta es que probablemente sea posible pero por el momento no lo es. Es lo que la gente está pensando mucho.

En cuanto a su segunda pregunta con respecto a esta distinción legal, hay varias razones por las cuales es difícil. Es una de esas cosas que a primera vez parece ser sencilla pero que en realidad tiene mucha complejidad. Hay organizaciones, por ejemplo, que tienen derecho a la privacidad en sus países en virtud del derecho local. Por ejemplo, una clínica de abortos. Por lo tanto, hay un nivel de complejidad con respecto a esa pregunta, lo cual significa que todavía no dijimos sí o no a esta pregunta en el EPDP sino que tenemos que pasar esa decisión a la fase dos. Gracias por sus muy buenas preguntas.

RAM MOHAN: Gracias, Benedict. Gracias, Göran. Gracias a los que hicieron preguntas desde el público. Con respecto a otras preguntas acerca de políticas y estas cuestiones, si tienen preguntas me las pueden enviar y nosotros actuaremos como canal y lo

enviaremos a los diversos grupos que podrían tener los abordajes pertinentes en relación con esas preguntas. Göran.

GÖRAN MARBY: Voy a ir a escuchar allí.

RAM MOHAN: Gracias. Gracias. Hablemos un poco acerca de lo que hicimos y cómo comenzamos. Göran ya les explicó cómo comenzamos. El propósito del TSG, el grupo de análisis técnico, es explorar soluciones técnicas para autenticar, autorizar y brindar acceso a datos de registración no públicos para terceros que tienen intereses legítimos sobre la base de RDAP. Ese es el propósito. Hay una carta orgánica que tiene el TSG. Todo esto está publicado en la carta orgánica. Si entran en la URL que ven en pantalla van a poder acceder a toda esta información.

Dejamos muy en claro, tal como dijo Göran y tratamos de adherirnos en la medida de lo posible a lo siguiente, que el TSG no va a tomar decisiones ni a hacer recomendaciones acerca de temas relacionados con políticas. Por ejemplo, preguntas acerca de quién tiene acceso. Incluso qué es el acceso. ¿Debería llamarse acceso? Qué campos de datos, bajo qué condiciones debería otorgarse el acceso, cuáles son los intereses legítimos. Hay toda una serie de cuestiones que existen y nos alegra que

exista pero no forma parte de nuestra competencia. Lo nuestro es la parte técnica.

¿Quiénes son los miembros del TSG? Como dijimos, Göran es el sponsor. Me pidió que armara el grupo en octubre del año pasado. Me llevó un tiempo tomar las decisiones. Aquí pueden ver algunas fotografías pero lo más importante es que pueden ver a casi todos los miembros del grupo de análisis técnico aquí, frente a nosotros. Creo que solo Murray, de Facebook, no está aquí, pero el resto de los miembros del grupo de análisis técnico están aquí frente a ustedes. Hemos tenido la suerte de que el trabajo de los voluntarios del TSG haya recibido el apoyo del equipo de primer nivel de ICANN org y aquí ven a varios: [Elisa, Diana], John Crain, Gustavo. También tenemos a Francisco Arias, que no está aquí con nosotros. También hemos tenido gran ayuda de Yvette y de Erika.

Cuando comenzamos, para mí era muy claro que la forma de obtener resultados reales era que el TSG trabajara sobre la base del consenso. Teníamos que tener un proceso iterativo. Nuestro foco tenía que ser técnico. Ese fue el modelo de participación inicial con el que comenzamos a trabajar. En realidad la forma de crear el proceso para llegar a un modelo, para llegar a una solución fue el siguiente. En primer lugar comenzamos definiendo preguntas y consideraciones clave. Luego

identificamos los supuestos principales. Posteriormente identificamos casos de uso así como el recorrido del usuario. Luego definimos los requerimientos del sistema: funcionales, operativos, de gestión. Creamos un mapeo con requerimientos funcionales. Creamos los modelos de actores. Determinamos consideraciones de implementación y después de haber hecho todo esto, que nos permitió en la reunión presencial que tuvo lugar el mes pasado llegar a una solución propuesta, lo logramos a través de un proceso muy iterativo. Tuvimos muchos modelos que analizamos para ver qué nos parecía que estaba bien o no. Finalmente, logramos llegar a una solución propuesta para este modelo técnico.

La parte siguiente de nuestro trabajo consistía en lo siguiente. Mientras trabajábamos, mientras llegábamos a un modelo técnico, mientras analizábamos el modelo de actor, la consideración de la implementación y los requerimientos, fueron surgiendo varias cosas que claramente eran consideraciones de todo este espacio pero también quedó claro que estas consideraciones y observaciones que estábamos haciendo no eran cosas para nosotros como grupo de análisis técnico. No eran cosas con respecto a las cuales nosotros teníamos que actuar. Por una cuestión de hacer un buen trabajo de custodios, nosotros tomamos nota de estas observaciones y consideraciones a medida que surgían. Todo esto formará parte

del documento final que publicaremos. El objetivo es que otras partes de la comunidad luego trabajen sobre esto y no que lo haga el grupo de análisis técnico propiamente dicho.

Después de hacer esto, la próxima fase es recibir los aportes de la comunidad. Esta es una de las sesiones en las que esperamos recibir sus aportes y más adelante en esta semana el grupo de análisis técnico se reunirá de manera presencial aquí en Kobe para analizar los aportes y comentarios que recibimos aquí para ver si tenemos que hacer algunos cambios u otras modificaciones en el modelo que creamos.

Luego dedicaremos las próximas semanas, tres o cuatro semanas más, a continuar con un proceso iterativo de trabajo. La intención es finalizar nuestro trabajo a mediados de abril y publicar lo que consideraríamos nuestro producto final, poder publicarlo a fines de abril para dárselo a ustedes, a la comunidad, a Göran, y finalmente esperamos llegar al punto 13 de nuestra carta orgánica.

Estaba hablando antes sobre el proceso. Si ustedes miran lo que hicimos, lo primero fue analizar cuáles son las preguntas clave y las consideraciones que deben estar presentes. Si van a icann.org/tsg, van a encontrar en esa página que está la carta. En esa carta van a ver que están las categorías indicadas y hay preguntas en cada categoría. Aproximadamente 17 o 18

preguntas que pertenecen a cada una de las categorías. Esto ayudó a organizar nuestro pensamiento en qué es lo que se debe estudiar, qué es lo que debemos hacer en cada una de estas áreas.

Una de las primeras cuestiones cuando empezamos a hacer este trabajo fue que teníamos que tener muy en claro cuáles iban a ser los supuestos que íbamos a hacer. Ciertamente, si no hubiéramos definido esos supuestos, la mayor parte de nuestro trabajo habría quedado de lado. No lo habríamos podido utilizar. Empezamos entonces después de este proceso. Una de las primeras cuestiones fue hacer una lista de las suposiciones clave. Refinamos estas suposiciones a medida que las repetíamos en el proceso. Empezamos en noviembre creo que con unos siete u ocho supuestos. Ahora tenemos muchos más a medida que fuimos avanzando en el proceso es un buen signo. Es un signo de que reconocemos otros asuntos.

Una de las cuestiones que quiero destacar es que cuando uno ve que nosotros hablamos de los supuestos, tanto en el documento como en estas diapositivas aquí, lo que se debe reconocer es que no estamos haciendo una afirmación sobre nosotros sino que estas son las cuestiones correctas que se deben hacer. Lo que ustedes ven es que simplemente estamos documentando que estos son supuestos que fueron hechos o que existen en este

espacio. Lo fundamental de nuestro trabajo está basado en supuestos que están presentes y que son ciertos. Claramente, si alguno de esos supuestos no son ciertos, o deben evolucionar o alguna otra cuestión, muy posiblemente esto va a tener algún efecto en el modelo en sí. Ciertamente yo quisiera estar en el espacio de ustedes, estando en la audiencia, escuchando el próximo grupo y viendo cómo evolucionamos hacia una solución técnica.

Una de las partes importantes de todo esto es también que la validez de las afirmaciones, en ellas nuestro alcance está en el componente técnico. Si ustedes ven los supuestos y ven partes de política o sienten que tienen que cuestionar si es que estos supuestos efectivamente se van a mantener, tenemos algunas declaraciones aquí. Traigan esas declaraciones pero reconozcan que nosotros no estamos en una posición de dar algún evento autoritativo sobre si estas suposiciones son correctas o no. Lo que sí queremos saber es si estos supuestos que estamos haciendo implican que hubo algunos que quedaron afuera y, en segundo lugar, si están completamente mal y podrían de algún modo socavar la validez del modelo técnico. En este marco quisiera ahora pasarle el micrófono a Steve y preguntarle si nos puede ir mostrando los supuestos.

STEVE CROCKER: Gracias, Ram. Aquí la imagen es una imagen conceptual básica donde las consultas de los datos no públicos de gTLD están mediados a través de un gateway de ICANN, lo cual da acceso a las credenciales que están implicadas en una consulta en particular en el proceso de autorización y de autenticación. Hay 12 supuestos. Me voy a referir a seis de ellos en los paréntesis en esta diapositiva y en la próxima están los 12. El modelo básico indica que RDAP es el mecanismo que se va a utilizar y luego el puerto 43 va a dejar de ser usado. El acceso a datos no públicos de gTLD va a ser acceso mediado. Las consultas de las fuentes no autenticadas van a ser hechas de acuerdo con la política y luego ICANN va a verificar la protección de credencial y la validez asociada.

Esta diapositiva indica los 12 supuestos. Los que están arriba son los mismos que acabo de cubrir. Los que están abajo son distintos supuestos que se ocupan de la evolución y las cuestiones vinculadas a medida que el modelo es puesto sobre la mesa. Hay un conjunto de reglas de RDAP existentes, prácticas existentes. Hay una experiencia piloto también, elecciones de política, utilidades de implementación. Estamos hablando de una presentación muy compacta. Por eso les pido que lean el informe para el resto de estas cuestiones. Le damos la palabra a Ram.

RAM MOHAN: Vamos a la próxima diapositiva. Habiendo hecho estos supuestos… Gracias, esto es autoservicio. Llegamos entonces a definir varios casos de uso. Antes yo les hablé sobre los procesos y los casos de uso son la parte siguiente del trabajo que hicimos y quisiera entonces que empecemos con esta parte con Andy.

ANDY NEWTON: Los casos de uso implicaron que tuvimos que ir refinándolos a medida que avanzábamos. Queríamos hablar sobre los usuarios autorizados, es decir, gente que tiene alguna necesidad de acceder a esta información como la aplicación de la ley, que creo que es un actor al que volvíamos varias veces por cuestiones de seguridad. También abogados de propiedad intelectual, este tipo de gente. Ellos requerían acceso a consultas múltiples o incluso a consultas de una sola vez. También hemos dicho que los usuarios que recibieron autorización online tenían que tener una autorización lo antes posible. Tuvimos también un tercer caso de uso donde dijimos que tiene que haber una capacidad para que algunos usuarios puedan tener acceso a los datos asociados e incluso tuvimos casos donde los usuarios autenticados no estaban autorizados a ver los datos. Finalmente hablamos de usuarios que son los sujetos de los datos y solicitaron esos datos.

Generamos entonces algunos requisitos de sistema que eran iterativos también. Empezamos primero analizando los distintos componentes del sistema y lo ampliamos un poco más después. En líneas generales, esto va a estar basado en estándares de Internet. Tiene soporte de IPv6. También de un modelo distribuido. Tuvimos que usar protocolos de seguridad como TLS y otros que eran aplicables a los sistemas que estábamos especificando.

Una de las cosas que aparecieron inmediatamente fue hablar sobre un portal web para gente que necesitaba solicitudes rápidas. Tuvimos también pedidos de portales web basados en navegadores. Hablamos también de determinación de autorizaciones. Queríamos que se delegasen, de ser posible, a los agentes calificados de acuerdo a la política de la ICANN. Quiero hablar también sobre cómo nosotros lo hacemos. Tuvimos este concepto de un gateway RDAP generado por ICANN que consulta las partes contratadas a través de sus servidores RDAP. Tiene que soportar solicitudes múltiples autenticadas y las políticas que van junto con eso y tiene que dar acceso granulado a los distintos elementos. Tiene atributos del solicitante a las partes contratadas. Cuando tenemos un pedido no autorizado tenemos que reiterarlo. Además, tenemos que poder soportar la automatización también. Luego están los

servidores de RDAP gestionados por las partes contratadas. Tenemos que responder a pedidos del gateway RDAP de ICANN.

Quiero darles algunos requisitos generales. Tenemos requisitos de login y de auditoría. También algún tipo de capacidad para retención de datos. También necesitamos reconciliar las consultas de todas estas partes. Por eso hablamos también del abuso del sistema. Otros aspectos fueron que analizamos el desempeño de los acuerdos de nivel de servicio. Tendría que haber estos acuerdos para todos los subsistemas porque sin ellos uno nunca sabe muy bien en qué parte del sistema deja de funcionar. Por eso es una especie de garantía sobre lo que va sucediendo.

Finalmente miramos los requisitos de seguridad e información que establecen que tiene que haber una evaluación de cuáles son los requisitos. Luego tiene que haber una manera de dar información de auditoría para cada una de estas solicitudes. Luego si hay incumplimientos hay que reportarlos.

Por último, miramos los controles organizacionales. Esto tiene que ser regido por un programa de continuidad y todas las técnicas de almacenamiento criptográfico que están dentro de las mejores prácticas deben ser las que se utilizan. Creo que eso es todo. Scott, si quiere hablar del modelo.

SCOTT HOLLENBECK: Muchas gracias, Andy. Como dice el título de esta diapositiva, el modelo es una propuesta y está basado en dos protocolos estándares: OAuth 2.0 y OpenID Connect. Antes de ir a esta parte técnica quiero mostrarles una imagen. Este diagrama de flujo de datos es una especie de evolución de lo que les mostró Steve pero con un poco más de detalle respecto de las interacciones entre los actores y los flujos en los distintos elementos. Si ustedes están familiarizados con los servicios de firma única, el tipo de cuestión que uno ve en los recursos web cuando uno ingresa con la dirección de email o con la credencial de Twitter o con la identificación de Facebook, ustedes conceptualmente entienden el modelo. Por supuesto que es mucho más detallado pero el flujo de datos es muy parecido. Vamos ahora a ver rápidamente la diapositiva anterior.

Hay algunos prerrequisitos antes de que este sistema de firma pueda funcionar. Hay proveedores de servicio anteriores que tienen que existir. Hay mucho desarrollo de software que tiene que estar allí para que sea operativo. Los solicitantes que son el término que nosotros tomamos del EPDP para identificar a las personas que están pidiendo datos deben tener credenciales que son emitidas por un proveedor de identidad. Estos proveedores de identidad van a ser nuevos actores y parte de su responsabilidad al emitir estas credenciales es asociar atributos de identidad a esas credenciales. Algo bueno de esta solución es

que funciona inmediatamente. Es decir, utilizando servicios provistos por empresas como Google, Microsoft y Yahoo, que soportan OpenID y OAuth. Estos proveedores no saben nada de RDAP. Por lo tanto, no tienen una asociación a estas credenciales. Esto es algo que está por venir de todos modos.

Una vez que los prerrequisitos están establecidos, todo el proceso se inicia cuando un solicitante envía un pedido RDAP a un servicio utilizando algún tipo de cliente. El acceso al servicio recibe este pedido y dado que este acceso de servicio no sabe quién lo está pidiendo, envía una redirección al cliente para que interactúe con un proveedor de identidad. Lo que ve el humano es alguna especie de forma web operada por un identificador donde a uno le piden que utilice credenciales. Puede ser un usuario y password o también los certificados de cliente. Eso es lo que el proveedor y el negociador establecieron.

Digamos que las credenciales se confirman y se validan y lo siguiente que ve el humano es un pedido para seleccionar distintos bits de identidad, estos atributos, y dan su consentimiento para que esa información sea compartida con la parte subyacente o la entidad, el acceso de servicio que proyecta la información.

El solicitante entonces presiona el botón de enviar y luego aparece algo que es un código de autorización al cliente que

envía otro redireccionamiento al servicio de acceso, lo cual inicia el proceso e inicia una consulta RDAP. El servicio de acceso toma este código de autorización y lo utiliza para extraer grandes cantidades de datos que se llaman tokens del proveedor de identidad. Estos tokens luego se envían al cliente. Son los tokens los que contienen la información sobre la identidad asociada con el solicitante y que incluyen información para determinar la autorización.

El cliente tiene los tokens y envían una consulta RDAP con la información de ese token al gateway de RDAP de ICANN. Cuando el gateway recibe la información, empieza a procesar la consulta RDAP. El gateway recibe la consulta, recibe los tokens y luego envía todos los bits de información a un tercero autorizador para que lo verifique. El autorizador procesa estos datos y asegurado que la información de los datos sea válida y que las consultas y los atributos estén listos y luego da el resultado al gateway esto típicamente dice que sí o que no, que esa persona no está autorizada para lo que está solicitando.

Asumiendo que estemos autorizados, el gateway luego envía consultas RDAP a la parte contratada de los servidores para poder tomar todos los datos no públicos. El gateway procesa y filtra estas respuestas para formar una respuesta completa a RDAP que luego es enviada al cliente y el cliente muestra el

resultado al solicitante. De nuevo, aquí está esta imagen en una forma de resumen. Es el mismo flujo de datos.

RAM MOHAN: Scott, si pudiera tomarse un momento y decirnos si del proveedor de autenticación al servicio de autorización, creo que sería útil porque tuvimos algunas preguntas ayer respecto de si la intención es que todo se modelo junto o si puede ser distribuido, este tipo de cosas. Creo que sería útil hablar sobre eso. Además, también tenemos ciertas discusiones en nuestras deliberaciones. Hay una idea de un proveedor de identidad y cuál es ese rol.

SCOTT HOLLENBECK: Sí, Ram, no hay problema. Aquellos que están familiarizados con cómo funciona el WHOIS y estoy seguro de que todos los que están en la sala lo reconocen, reconocen entonces dos actores en este modelo: el cliente y los servidores RDAP. El modelo no funciona tan bien cuando hay que tomar decisiones sobre identificación, autenticación y acceso. Ahí es donde aparecen estos servicios estándares. OpenID y OAuth 2.0 nos dan las facilidades que necesitamos para identificar a los clientes adecuadamente, autenticarlos y tomar decisiones de control de acceso en base a las identidades. Eso tiene que tener otros jugadores en este mix. El primero es este servicio de acceso

RDAP de ICANN. En este grupo nosotros lo llamamos un proxy. Si ustedes saben cómo funcionan los proxy, pueden pensarlo del mismo modo que un intermediario. Recibe las consultas y luego decide quién va a estar involucrado en ese vector.

Una de las primeras cosas que tiene que hacer el servicio es saber a quién le está hablando y lo hace a través de estos proveedores de autenticación y estos servicios de autenticación. El protocolo funciona así. Estos servicios pueden ser realizados por una entidad que a veces es descrita como un proveedor de identidad o esas funciones pueden estar divididas en distintos actores. El modelo que nosotros describimos soporta ambos métodos de operación y va a ser una cuestión de política la cual va a determinar cuál es el actor que desempeña cada función.

Como pueden ver, en las interacciones el proveedor de autenticación recibe la consulta del servicio RDAP, interactúa con el cliente. Esta es una interfaz web, la que describí antes, y allí es donde el cliente brinda sus credenciales. El proveedor de autenticación es el que las emite y el que puede realizar la función de autenticación y el servicio RDAP nunca tiene que ser expuesto, nunca tiene que exponer esta información. Es una afirmación del proveedor de autenticación respecto de si el cliente está identificado y autenticado completamente.

Luego vamos al servicio de autorización. Una vez que el RDAP identifica y autentica hay que determinar si ese solicitante tiene el nivel de acceso para lo que está solicitando. Tradicionalmente, esa es una función que se hace con un proveedor de identidad pero que nos permite dividir esa función en un servicio de tercero. Nosotros describimos esa posibilidad aquí en el modelo. Funciona así. Se envía la consulta, se hacen comparaciones, se habla de las políticas que hay que determinar y luego hay una respuesta de dedo arriba o dedo abajo que genera los servicios de RDAP para cada una de las consultas. ¿Eso fue suficiente, Ram?

RAM MOHAN: Sí, muy bien. Una cosa más. Hay una pregunta que surgió con respecto a si el servicio de acceso de RDAP de la ICANN funciona así, si la ICANN va a tener una copia de los datos en nuestro modelo o no. Sería bueno también responder esa pregunta.

SCOTT HOLLENBECK: Sí. Los datos en este modelo están con las fuentes autorizadas. Debo decir cuáles son estas fuentes porque la política del WHOIS extenso dice algo diferente. Nuestro punto de vista es que autorizado significa que la entidad que tiene la relación con el sujeto de los datos es una cuestión de prevalencia, dónde están los datos, dónde se recopilan los datos, dónde se producen los

datos. Esta es una razón por la cual vemos una superación entre las funciones de registros y registradores. Los registradores van a mantener los datos sobre los cuales tienen autorización. Los registros mantienen los suyos. El servicio RDAP de la ICANN no mantiene copia de los datos. Los datos pasan por el servicio para ser procesados pero no se conserva ningún registro más allá de registros de acceso. Los datos no se mantienen en memoria caché. Son transitorios y hasta ahí llegan.

RAM MOHAN: Muchas gracias. Sé que me siguen presionando. Quiero seguir hablando de este tema porque este es el núcleo de lo que nosotros vamos a hacer. Hay otra pregunta que surgió, Scott. Si el servicio de acceso de RDAP, sin nuestro modelo nosotros pensamos que esto va a estar centralizado. Pensamos que tendríamos un sitio web o algún otro mecanismo automatizado. Eso por un lado.

En segundo lugar, si no hay autenticación, si tenemos una solicitud no autenticada o no autorizada quizá para acceder a datos públicos o datos restringidos, si son datos que no son de un gTLD, ¿cuál es nuestro plan? ¿Qué pensamos nosotros al respecto? Quizá podría hablar sobre este tema.

SCOTT HOLLENBECK: El servicio de RDAP nosotros lo vemos como una interfaz web pero con dos fases. Como dijo Andy, necesitamos tener acceso automatizado online pero también necesitamos acceso asíncrono. Tenemos a alguien que no necesariamente tiene una credencial pero quizá tenga un propósito legítimo para solicitar información. Quizá tenga que haber soporte para el cliente que quizá deba completar un formulario web y ese formulario puede revisarse, procesarse y devolver una especie de respuesta. En cuanto a servicio web, este servicio de acceso RDAP puede implementarse así como se suelen implementar los servicios web. No necesariamente un servidor. Puede estar distribuido en varios lugares para ocuparse de cosas como balanceo de carga. Es una cuestión de cuáles son las mejores prácticas con el apoyo de los servicios de HTTP.

El proveedor de autenticación y las funciones de servicio de autenticación podrían centralizarse pero también podrían ser distribuidos. El modelo que estamos pensando es un modelo en el cual estas funciones no están centralizadas. El hecho de que estén distribuidas es lógico. Hay diferentes entidades que tienen relaciones con los solicitantes. Saben quiénes son los solicitantes, por ejemplo. Pueden emitir estas credenciales y tomar decisiones de autenticación y acreditación adecuadas sobre la base de las relaciones preexistentes.

Con respecto a los datos públicos, la expectativa es que las partes contratadas tengan interfaces públicas para datos públicos, para que los clientes puedan enviar consultas directamente a los registros y los registradores. Lo que van a recibir es lo que sea que la política determina que son datos públicos. ¿Respondí su pregunta?

ORADOR DESCONOCIDO: En nuestro documento cubrimos las diferentes combinaciones dividiendo o combinando proveedores de identidad. Lo llamamos el modelo de actores. Tenemos una serie de combinaciones definidas en el documento. Creo que hay cuatro. Por otra parte, volviendo a los usuarios no autenticados o no autorizados, en general lo que pedimos es que el gateway RDAP de la ICANN cuando recibe una solicitud de acceso pueda hacer un redireccionamiento a nivel de HTTP para que la fuente que figura en el bootstrap de la IANA encuentre esos archivos. Una de las razones por las cuales pedimos esto es no solo por una perspectiva de TLD sino porque RDAP también se utiliza en otro contexto como en los RIR y el espacio de ccTLD.

RAM MOHAN: Gracias. Gracias, Scott. Ahora voy a dejar que usted hable acerca de las consideraciones.

GAVIN BROWN: Voy a repetir lo que ya se dijo en realidad. Nosotros hablamos e identificamos algunas cosas que nos parecía que no se habían aclarado totalmente y que nos parecía que estaban un poco fuera de nuestra competencia porque nosotros nos centramos en las soluciones técnicas, si bien nos interesan mucho las políticas. Quiero subrayar algunos de los puntos que ustedes podrán ver en las siguientes diapositivas.

Ya hablamos un poco acerca de la retención de datos. Tal como se dijo, nosotros no estamos pensando en un gateway de acceso que almacene datos de registración. En la jerga se habla de un proxy reverso pero no un proxy reverso en caché. No almacena la información que recibe. Sí habrá determinados elementos de datos que sí se almacenan. Por ejemplo, los logs de la clave. Reconocemos que estos logs, estos registros podrían tener un cierto riesgo, un cierto valor asociado. Por lo tanto, corresponde que en el área de política se apliquen las reglas de retención de datos a estos registros. Esto es lo que debe hacerse. Obviamente hay diferentes cosas que tiene que tener el sistema para poder, por ejemplo, garantizar, y después vamos a hablar un poco más sobre este tema, que esto ocurre. Es importante auditar el sistema para asegurar que las cosas ocurran como deben ocurrir. Por eso el login está incluido aquí. También es necesario en

primer lugar reducir el riesgo de divulgación porque el hecho de que alguien haga una solicitud es que potencialmente esto mismo ya incluye información valiosa. Tenemos que tener una política para reducir el riesgo de divulgación de esa información. Nos parece que esto realmente corresponde.

Como dije antes, con respecto a los acuerdos de nivel de servicio, obviamente hay diferentes partes. El modelo que describimos tiene una serie de entidades independientes que dependen de los servicios que prestan todas para poder cumplir con su parte del sistema. En última instancia tenemos también los usuarios finales, los solicitantes que también dependen de que este sistema esté disponible. También necesitamos satisfacer sus necesidades. Quizá tengan un propósito legítimo para acceder a los datos. Identificamos una serie de acuerdos de nivel de servicio que debemos definir e instaurar para garantizar la disponibilidad y estabilidad del sistema.

También recomendamos que la ICANN org sea muy transparente con respecto al desempeño de estos acuerdos de nivel servicio y, por supuesto, que el solicitante pueda ver cuál es el estado del sistema. Nos parecía que era importante que la ICANN haga una revisión del impacto potencial que podría tener el hecho de asumir la responsabilidad de dirigir un sistema como este,

especialmente los ítems tres y cuatro de esta lista que podrían ser el mismo ítem.

Tenemos riesgos legales y también los riesgos operativos que podrían tener potencialmente una gran escala dependiendo de dónde esté la decisión de políticas con respecto a cómo se va a implementar el sistema. Hay muchos otros riesgos que deben considerarse. Obviamente, el riesgo de seguridad de la información. También está incluido. Para nosotros era importante advertir a la organización y a la comunidad de la ICANN cuáles son y el hecho de que es necesario hacer revisiones y evaluaciones para poder enfrentar estos riesgos.

Nos parecía que era necesario también señalar el tema de reducir la responsabilidad de las partes contratadas. Nosotros somos especialistas técnicos. No somos abogados. Por lo tanto, no sabemos si el sistema que proponemos de hecho reduce esa responsabilidad. Por eso nos parece que es necesario alentar a las partes contratadas a decirnos qué opinan. Seguramente lo harán.

Con respecto a la transparencia, nosotros pensamos definitivamente que una parte clave para garantizar la confianza en el sistema es que si la ICANN decide instaurar un sistema como este tiene que ser muy agresivo en cuanto a la transparencia con respecto al uso del sistema. No tenemos datos

con respecto a cuáles son las solicitudes que deben publicarse o divulgarse pero sí necesitamos información estadística con respecto a cómo se utiliza el sistema. Creemos que este va a ser un punto de datos clave para entender y garantizar que haya confianza en la integridad del sistema. Por eso proponemos que se produzca un informe de transparencia periódicamente para el beneficio de la comunidad.

Finalmente, también reconocemos que habrá resultados provenientes del proceso de autorización. El solicitante quizá no esté de acuerdo con ese resultado y debe haber un mecanismo para los reclamos, reclamos con respecto a los procesos, a problemas del sistema. Estos reclamos deben poder escalarse a través de un proceso. Probablemente esto también incluya una solicitud de eliminación de datos en virtud del artículo 17 del GDPR. Los sujetos podrían pedir a la ICANN que se eliminen datos de manera precisa o no precisa.

RAM MOHAN: Gracias. ¿Podemos pasar a la próxima diapositiva? Perfecto. De esta forma finalizamos con los comentarios que preparamos para esta sesión. Ya estamos trabajando. Recibimos aportes de la comunidad. Esperamos recibir aportes de ustedes hasta el miércoles. Incluso más allá del miércoles pero realmente nos gustaría recibir sus aportes, opiniones. Nuestra idea es pensar en

todo esto, analizarlo e incorporarlo al modelo técnico. Tenemos pensado organizar varias llamadas en conferencia así como reuniones presenciales a mediados de abril para finalizar nuestro trabajo y esperamos poder publicar el modelo técnico final el 23 de abril. Posteriormente, este grupo se va a desarmar y vamos a ver finalizado nuestro trabajo. Habiendo dicho esto, es hora de pasar a las preguntas del público. Veo que ya hay un señor allí parado. Hay otras preguntas. Por favor, quienes quieran hacer preguntas, vayan a los micrófonos. Yo haré todo lo posible por moderar esta sesión.

RUBENS KUHL: Soy Rubens, de .PR. Quisiera saber si el grupo consideró una situación en la que la ICANN solamente emita un token utilizando OAuth u OpenID. Luego contactar directamente a las partes contratadas porque esto evitaría el hecho de que los datos fluyan a través de los sistemas de ICANN. Esto evitaría la mayor parte de las cuestiones de SLA. Si bien no es un proxy de caching, este proxy igual llevaría a una divulgación o difusión de datos. ¿Por qué no se eligió este modelo más centralizado? ¿Hay un motivo?

ANDY NEWTON: Sí, hablamos de esto y la razón por la cual no elegimos esa solución es porque en ese caso tenemos que trabajar con

mecanismos para distribuir políticas entre las partes contratadas. Esto implica una mayor carga para las partes contratadas que deberían actualizar estas políticas continuamente. Nos pareció que era más sencillo que icann.org fuera el lugar donde se hiciera todo el filtrado de políticas. Esa es la razón por la cual elegimos ese camino. Es un modelo simplificado de tener un token de acceso que va directo a las partes contratadas. Con respecto a los SLA, yo no creo, y ninguno de los que estamos aquí me parece que tampoco, que cambie los SLA en absoluto.

RUBENS KUHL: Incluso con un motor de política centralizada en la ICANN, el flujo de datos podría no ser centralizado. No es necesario que una decisión afecte a la otra.

ANDY NEWTON: Entiendo lo que usted dice. En cuanto a los SLA, igual habrá un SLA sobre los servicios que presta la ICANN. Creo que hay algunas cuestiones de SLA que no cambian con ninguno de los sistemas.

GAVIN BROWN: Tener a la ICANN como único punto de acceso también permite resolver alguna de las cuestiones que plantearon los organismos

de aplicación de la ley en cuanto a que no haya demasiada información con respecto a sus propias solicitudes. Quizá Benedict pueda hablar más con respecto a ese punto en particular o Steve pero creo que cuando tuvo lugar este debate creo que esa fue la idea. Había muchos aportes u opiniones de las autoridades de aplicación de la ley en cuanto a que esto afectaba a la transparencia. La preocupación, el hecho de que una organización, un organismo de seguridad haga una solicitud y que esto lo sepa el registrador, eso es lo que les preocupaba.

BENEDICT ADDIS: Lo que voy a decir es que esto es algo que le estamos advirtiendo al EPDP fase dos porque hay una diferencia entre las solicitudes que llegan a la ICANN y la ICANN es responsable del login a diferencia de más divulgación, menos divulgación en las manos de las partes contratadas. Este es un debate que los organismos de aplicación de la ley tendrán que tener con las partes contratadas en cuanto a solicitudes anónimas o la posibilidad de las partes contratadas de saber quién está haciendo la solicitud pero esto realmente excede nuestra competencia. Hay otros beneficios. Pido disculpas por interrumpir. Hay otro beneficio y es que desde el punto de vista de transparencia, tener un servicio centralizado nos permite generar informes de

transparencia. Todos estamos de acuerdo en que esto es algo bueno.

RAM MOHAN: Gracias. El señor que está a la izquierda.

KLAUS STOL: Quiero agradecer a este grupo por su trabajo. Un comentario y una sugerencia. De acuerdo con las consideraciones, el punto número seis, transparencia, quizá deberían mencionar la investigación académica porque hay muchas personas que van a estar muy interesadas en esto. Esto va más allá de las estadísticas. Sería bueno que lo mencionaran. Gracias.

RAM MOHAN: Muchas gracias. Vamos a tomar nota y lo vamos a considerar en nuestras deliberaciones.

VITTORIO BERTOLA: Creo que mi pregunta es parecida a la que ya se hizo. Quería entender por qué buscamos un sistema centralizado, especialmente quiero saber si es una decisión técnica o si es una decisión relacionada con políticas porque desde el punto de vista técnico, si yo tengo que crear algo así, creo que algo descentralizado funcionaría mejor para trabajar con las partes

contratadas. Lo podemos debatir. Podría hacer distintas propuestas.

Por otra parte, cuando se hizo la pregunta, las dos razones que yo escuché fueron razones de políticas. Para poder hacer un seguimiento de todo a los fines de la transparencia, los organismos de seguridad quieren que utilicemos proxy para que las partes contratadas no vean quién lo solicita pero eso son decisiones políticas. En su presentación usted dijo que no podemos decir si esto es mejor en términos de políticas, posibilidades legales, etc. Ahora estoy un poco confundido. No sé si se está tratando de resolver un problema técnico con la mejor solución técnica o si tiene algunos requerimientos de políticas que hacen que sea necesario tener un modelo descentralizado. Quisiera saber si podemos hablar sobre esto.

GAVIN BROWN: Estoy de acuerdo en que podríamos decir en cierto sentido que hay un tema de política. También tenemos razones técnicas sólidas. Queremos reducir la complejidad técnica y operativa del sistema. Tener un sistema distribuido y que las partes contratadas tengan que actualizar continuamente las políticas y entender cuál es el texto de las políticas, sea como sea se haga esto es un proyecto técnico muy grande y una de las razones por las cuales hicimos lo que hicimos fue porque tratamos de reducir

la complejidad técnica del sistema. Lo que no mencioné antes, y esto lo incluimos en un documento, es que con la forma en que lo definimos, las partes contratadas solo tienen que utilizar TLS mutuos para saber en quién confiar mientras que si hiciéramos controles de acceso utilizando un token que el cliente recibe a través de las partes contratadas, esto eleva la carga de trabajo que tienen que hacer las partes contratadas.

ALEX DEACON: Tengo una pregunta que tiene que ver con la pregunta de Rubens que es específica sobre los requisitos sobre los atributos, identificadores, etc. Me parece a mí que está claro que esto es política. Hay una separación entre política y tecnología aquí pero me da curiosidad. Si la decisión que se tomó es que el modelo dos es el que vamos a adoptar, creo que es la decisión correcta y ese modelo describe la ICANN como el único autorizador y en ese caso no me queda claro que nosotros tengamos que mandar los datos a las partes contratadas. ¿Me pueden dar un poco de contexto respecto de por qué estos requisitos no se establece si son buenos o malos? No es que esté en desacuerdo con esto. Quiero conocer el proceso para la manera en que terminaron esos requisitos.

ANDY NEWTON: Buena pregunta. Los requisitos tienen que poder hacerlo. Es decir, tener estas identidades o pseudoidentidades o atributos al solicitante que tienen que poder soportarlo y pasar a las partes contratadas, si eso es lo que indica la política. No es que esa sea la política. Eso es lo que estamos tratando de expresar. Se trata de una característica del sistema donde se dice que la política debe ser aplicada y el sistema no puede soportarlo.

ALEX DEACON: Si la política decide que todo ocurre en este proxy de ICANN, estos atributos no se tienen que enviar.

ANDY NEWTON: Por eso tenemos cuatro modelos de actores. No sabemos cuál es el correcto o si va a haber muchos. Por eso los establecimos de esa manera.

NEAL MCPHERSON: Hola. Tengo una pregunta sobre los datos históricos. Creo que Steve mencionó que no todo el proceso tiene que ocurrir en tiempo real sino que va a haber casos de uso donde se puede tener información en un momento en el tiempo en particular. ¿Hay algún tiempo establecido donde uno tiene que mandar los datos, hoy o ayer o cuando ocurrió el reclamo? También en

cuanto a los pedidos, hay muchos pedidos que recibimos que están basados en quién es el dominio.

RAM MOHAN: ¿Le puedo pedir por favor que se acerque al micrófono? Escuché casos de uso, datos históricos y estoy llenando los espacios. Me gustaría no tener que hacerlo.

NEAL MCPHERSON: En cuanto a los sellos de tiempo, ¿cuál es el sello de tiempo de los datos de WHOIS que ustedes tienen que incluir en base a un proceso? También, nosotros recibimos muchos pedidos de datos históricos. ¿Cómo entra esto en el proceso? Si un solicitante dice que necesita los datos de hace seis meses.

ANDY NEWTON: Yo trabajo para ARIN y ahí tenemos el WHOWAS, que básicamente es: "Deme los datos de registración de hace seis meses". Nosotros discutimos los servicios de WHOIS, etc. Los ponemos fuera de nuestro alcance porque básicamente esto complica las cosas en una medida en la que no estamos seguros si está dentro de nuestro mandato. Nosotros discutimos esto y dijimos: "Lo vamos a dejar por fuera". Espero haber respondido su pregunta.

RAM MOHAN: Siguiente pregunta, por favor.

GREGORY MOUNIER: Hola. Soy Greg, de EUROPOL. Quiero hacer una pregunta vinculada a lo anterior, sobre otra característica que usan los investigadores penales en el 80% de su investigación. Se trata de hacer una referencia cruzada para identificar todos los dominios que se registraron con una información específica que podría ser una dirección de email o el nombre de un registratario. Leí informes donde se decía que esto se tenía que desarrollar. TSG no ha dicho que se tenga que desarrollar. Mi primera pregunta es cómo hacen ustedes para decidir si lo incluyen en su estudio y la razón por la cual no se incluyó.

ANDY NEWTON: La razón principal por la que no se incluyó es que esta investigación no es parte de RDAP. Hay una regla en el IETF que vamos a discutir en un par de semanas. Esto nunca fue parte del RDAP base. Más allá de lo que dice ese documento preliminar, hay cuestiones sobre cómo conseguimos los datos de todas las partes contratadas en este espacio, ¿Usted quería decir algo? Por eso no está cubierto.

GREGORY MOUNIER: Creo que sería una lástima si al final la política dice que sí se puede hacer y luego hay otros que dicen que no lo usamos por distintas razones. Sería bueno si al final del proceso se puede hacer técnicamente.

RAM MOHAN: Quédense en el micrófono, por favor. Son las 2:46.

El 11 de marzo de 2011 a las 2:46 PM un terremoto de magnitud 9.1 azotó el Océano Pacífico en cercanías de la costa noreste de la isla Honshu de Japón. El terremoto, conocido como el Gran Terremoto de Japón Oriental, desencadenó un gigantesco tsunami con olas que alcanzaron los 40 metros de altura y llegaron hasta 10 km tierra adentro. Fue el terremoto más potente que se haya registrado en Japón y el cuarto más potente en el mundo. Se estima que 20.000 personas fallecieron y cerca de 500.000 personas tuvieron que ser evacuadas. En conmemoración de las personas fallecidas y de quienes vieron sus vidas afectadas por el Gran Terremoto de Japón Oriental guardaremos ahora un momento de silencio.

Gracias, Andy. ¿Quiere responder?

ANDY NEWTON: Perdón, ¿cuál era la otra pregunta?

GREGORY MOUNIER: Era solo una declaración, un comentario. Dije que sería una lástima si técnicamente no fuese posible cuando la política dice que sí es posible.

ANDY NEWTON: Las características de RDAP están incluidas pero esto puede ser una cuestión de política, puede haber cuestiones técnicas, pero sería algo bueno apoyar en el futuro si la comunidad considera que lo necesita.

RAM MOHAN: Gracias.

SÉVERINE WATERBLEY: Hola. Buenas tardes. Soy de Bélgica. Soy miembro del GAC. Si entiendo bien, ICANN va a ser el que procese la DPA y los servicios de autorización van a ser el procesador del procesador. ¿La relación contractual está prevista entre los registros y los proveedores de autorización o identificación?

RAM MOHAN: Es una muy buena pregunta. No sé si tenemos la calificación para darle una respuesta. Lo que sí podemos hacer para que no

se pierda esto es que lo vamos a registrar, la vamos a pasar a las personas de ICANN org porque los aspectos legales no son cuestiones a las que hayamos dedicado nuestra energía ni nuestro tiempo.

BENEDICT ADDIS: De nuevo, estoy hablando desde mi lugar en EPDP, hay un acuerdo legal entre ICANN y las partes contratadas. Sé que el departamento de legales de la ICANN se ocupa del tema. En el EPDP, especialmente en la fase dos, habrá discusiones que ocurrirán en esta misma sala dentro de 40 minutos.

TIM CHEN: Primero les agradezco por el trabajo que hicieron aquí. Creo que es un buen servicio considerar la realidad técnica. Los aplaudo por su trabajo. Tengo dos preguntas técnicas rápidas. Una es sobre las consideraciones. Creo que mencionan las multiconsultas o consultas multiuso. Quisiera saber a qué se refiere. No sé si fue en la sección anterior o cuándo. Solicitudes multiuso. ¿Pueden decirme cuáles son?

RAM MOHAN: Esto ocurrió al principio de nuestro trabajo. Los pedidos de datos pueden tener distintas formas. Una forma es que se trata de una parte que está autorizada para acceder solamente a los datos

con un elemento, una sola vez. En otros casos podría ocurrir que la autorización es más persistente pero también es persistente para una sola clase de pedidos o para acceder únicamente a una cierta cantidad de elementos. No nos quedó claro a nosotros en esta parte de nuestras deliberaciones que teníamos que restringir el modelo y que solamente podíamos tratar una solicitud una vez por elemento de dato o una por objeto en una forma persistente o en una forma más efímera. De eso tratan esas preguntas.

TIM CHEN: Los servicios de bootstrap se mencionaron ayer con las partes contratadas. Quisiera hacer un intento técnico de hablar de la RFC. Esto no se trata de llegar a las partes contratadas. No es hacer un servicio inverso. Pareciera que un bootstrap service tiene que ver cuál es el servicio autoritativo. Quiero volver a los comentarios anteriores sobre bootstrap. Este servicio trata pedidos de información por fuera de los nombres de dominio de gTLD. Quisiera que me expliquen esto.

SCOTT HOLLENBECK: Sí. Es posible. Nosotros estamos hablando de si sería genial que internic.net nos dé servicios útiles. Cómo evolucione esto con el tiempo va a ser una cuestión de coordinación e implementación de política pero en teoría sí es completamente posible.

ANDY NEWTON: Quiero agregar a esto que hay una muy buena posibilidad de que existan personas que escriban clientes RDAP y que no quieren hacer el bootstrap por sí sino que quieren hacerlo con [inaudible] o Bash u otro. Sería bueno ver si una fuente de bootstraping fuese ICANN. En ese caso, sería muy bueno si ICANN pudiese actuar como un servidor bootstrap típico que utilice archivos de IANA.

RAM MOHAN: Adelante.

ORADOR DESCONOCIDO: Solo una observación. Creo que la única parte que quedó excluida de este modelo del EPDP fue el usuario final. Sé que ustedes tienen un caso de uso donde pueden verificar sus propios datos pero este modelo me parece a mí que el usuario final es el canario en la mina. Soy usuario final. No pertenezco a ningún grupo y es lamentable. Yo creo que esto es algo por lo cual tenemos que lugar pero siempre quedamos excluidos. Siempre tenemos las peores condiciones. Las partes van a encontrar mecanismos para conseguir los datos que quieren con restricciones, a través de medios legales u autorizaciones pero somos los únicos que hemos quedado excluidos. Es lamentable.

Creo que es algo por lo cual vamos a tener que pelear. Este es solo el comienzo. Gracias.

RAM MOHAN: Gracias. Es un tema peculiar para plantear ante nosotros porque en todas nuestras discusiones, y si usted va y escucha las grabaciones y mira las transcripciones, va a encontrar que hemos dedicado una gran cantidad de tiempo a analizarlo desde el punto de vista del usuario final que está haciendo un pedido. Si bien los casos de uso cuando los reducimos tenemos cinco de esos casos, hubo muchas discusiones sobre el usuario final. De hecho, hay un principio de que todo sea simple y que no existan múltiples servicios y que el usuario final tenga que ir a múltiples lugares a buscar la información. Esto fue justamente focalizarse en que la experiencia del usuario esté a la vanguardia. Desde mi punto de vista al menos pareciera que el usuario final ha sido una consideración para nosotros pero ciertamente en el proceso general yo estoy de acuerdo en que todos nosotros tenemos que ver cuáles son las necesidades y los requisitos de los usuarios. Steve tiene la mano levantada.

STEVE CROCKER: Quiero entrar en su pregunta un poco más. ¿Cuál es el tema aquí? Presumiblemente, un registrador puede entrar en la cuenta con el registrador y verificar toda la información. Tienen

acceso directo. Estoy un poco sorprendido genuinamente en cuanto a cuál es el tema del que estamos hablando, si se trata de algo que sea significativo en ayudar a apoyar al usuario final.

RAM MOHAN: Benedict está diciendo que quizá usted está hablando del sujeto, no del usuario final. En ese caso tenemos el caso de uso cinco.

ORADOR DESCONOCIDO: Quiero agregar que yo no sabía nada del WHOIS. Ahora que sé que existe el WHOIS, yo lo habría usado, habría querido utilizado. La señora francesa del GAC dijo que quería que los consumidores tengan acceso a la información para las empresas. Esta es una cuestión que es muy importante para nosotros. Creo que la solución habría sido para nosotros, si nosotros fuésemos el centro, sería entonces desarrollar el uso del WHOIS para nosotros como protección y no eliminarlo.

BENEDICT ADDIS: Después de la confusión inicial de los términos, y voy a hablar no como miembro de un grupo técnico sino como miembro del EPDP de nuevo, creo que usted está diciendo algo excelente. Yo lamentaría ver que un sistema sea un club para un pequeño número de personas. Creo que lo genial de este modelo es que tiene la flexibilidad. Voy a usar la palabra de nuevo. Si la

comunidad decide que se ha utilizado de ese modo para los usuarios ordinarios de Internet pero esa es una política, usted debería ir a la comunidad.

RAM MOHAN: Va a tener la última pregunta.

ORADOR DESCONOCIDO: Es un comentario que tenía sobre la experiencia del usuario en uno de los reportes. Describe la experiencia de usuario con la que no estoy familiarizado. Yo uso WHOIS y RDS desde hace mucho tiempo. Lo leí varias veces. Hay una especie de mejoras que se podrían hacer a esa experiencia de usuario para incluirlo en el contexto de un usuario de WHOIS o de RDS o como lo llamemos hacia delante. Quería que quede muy claro de qué usuario estamos hablado, qué experiencia están tomando y ponerse en los zapatos de la persona que va a usar el servicio para mirar a los datos de RDS.

RAM MOHAN: Es muy buen feedback ese. Lo agradecemos. Ya hemos llegado casi al final de esta sesión. Lo que quisiera hacer ahora es pasar el micrófono a los distintos miembros del grupo de estudio técnico para que agreguen alguna otra cosa que quieran agregar antes de cerrar.

SCOTT HOLLENBECK: Gracias. Esto es una consulta. Nosotros creemos que funciona pero ciertamente estamos buscando sus aportes. Envíennos un comentario. Queremos oír lo que tengan que decir.

RAM MOHAN: Andy.

ANDY NEWTON: Quiero hacerme eco de lo dijo Scott. Queremos recibir sus comentarios. Envíenlos, por favor. Los vamos a conversar.

BENEDICT ADDIS: Qué equipo. Gracias a todos. Gracias por venir a escucharnos.

RAM MOHAN: Jorge.

JORGE CANO: Quiero decir que apreciamos sus comentarios y se lo agradecemos.

JODY KOLKER: No tengo nada para decir.

GAVIN BROWN: Yo sí tengo algo que está basado en los comentarios previos sobre la protección de los consumidores. Una de las cuestiones sorprendentes de RDAP es cuántos datos de acceso de registro tienen en el WHOIS Puerto 43. Si ustedes están escribiendo algo en JavaScript o una app para un teléfono o una aplicación web, ustedes van a tener que usar algún servidor de proxy. RDAP funciona en la web y los datos son provistos por JSON. Cualquier programador sabe qué es JSON.

Creo que esto no se aleja de lo que hemos dicho antes. Creo que puede haber un potencial aquí de permitir muchos beneficios para los consumidores que quieran obtener confianza en los identificadores que utilizan porque va a permitir que la información clave de los nombres de dominio y otros recursos estén disponibles y que estén disponibles mucho más fácilmente para el usuario final como una extensión de un navegador, donde uno hace clic en la barra de direcciones y el navegador puede ver estos datos del registro o registrador en RDAP y muestra precisamente en el navegador sin tener que ir al puerto 43. Utiliza entonces los beneficios de la web en ese marco con cuestiones como el caché y la seguridad para darle mucha integridad al sistema.

TOMOFUMI OKUBO: Les agradezco por haberse quedado hasta el final de la sesión.

RAM MOHAN: Steve.

STEVE CROCKER: Adhiero a todo lo que se dijo. Gracias. Diana. [Eliza]. Gustavo. John.

JOHN CRAIN: Un comentario breve. Muchísimas gracias a este equipo. Como ingenieros siempre detestamos tener que crear sistemas sin requerimientos. Esto es exactamente lo que tuvo que hacer este equipo. Creo que hicieron un trabajo fantástico. Esta gente, como todos ustedes, son voluntarios y trabajan duramente para crear algo que esperamos sea agnóstico desde el punto de vista de las políticas, que sea lo suficientemente flexible como para sobrevivir a los golpes que va a recibir a lo largo de los próximos años. Mucho trabajo y muy poco tiempo. Un trabajo increíble. Gracias.

RAM MOHAN: Gracias. Damos por cerrada y finalizada esta sesión. Gracias a todos por haber venido.

[FIN DE LA TRANSCRIPCIÓN]