ICANN80 | Foro sobre políticas – Sesión conjunta: ALAC y SSAC
Martes, 11 de junio de 2024 – 15:30 a 17:00 KGL

YESIM SAGLAM: Hola y bienvenidos a la reunión conjunta entre ALAC y SSAC. Soy la coordinadora de participación remota de la sesión. Tengan en cuenta que esta sesión se está grabando y que se rige por los estándares de comportamiento esperado de la ICANN. Durante la sesión, las preguntas o comentarios solamente se leerán en voz alta si se presentan dentro de la ventana de preguntas. Si desean tomar la palabra durante la reunión, levanten la mano en Zoom y cuando se diga su nombre, por favor, abran el micrófono para hacerlo. Los participantes presenciales utilizarán un micrófono físico. Habrá interpretación en inglés, francés y español. Indiquen su nombre para los registros y el idioma en el que van a hablar si no fuera inglés. Recuerden hablar a una velocidad razonable. Y entonces ahora le paso la palabra a Jonathan Zuck, presidente de ALAC, y a Ram Moham, presidente de SSAC.

JONATHAN ZUCK: Creo que voy a hablar primero porque es nuestra sala. Bienvenidos todos. Esta es una reunión periódica entre la comunidad de At-Large y SSAC porque tenemos muchos intereses compartidos en cuanto al destino de los usuarios individuales y su interacción con el DNS en internet, verificando que las políticas que se desarrollan dentro de la ICANN tengan en consideración algunas de las consecuencias que se dan. Por ende, tuvimos una alianza productiva, ampliando algunos de los mensajes que surgen en SSAC. Y como hablaremos en un minuto,

SSAC es uno de nuestros clientes potenciales para nuestra campaña nueva que estamos encarando sobre la ciberseguridad. Bienvenidos a SSAC y le paso la palabra a Ram.

RAM MOHAN: Si nos pusiéramos símbolos distintivos diferentes, pareceríamos enemigos y no lo somos. Hay muchos amigos acá, así que la gente levante la mano, por favor, los que son de SSAC para que sepan…

JONATHAN ZUCK: Son demasiados.

BARRY LEIBA: Estamos en todos lados.

RAM MOHAN: Es un placer estar aquí. Tenemos temas muy interesantes para debatir. Hay algunos temas siempre vigentes que se dan entre nuestros dos grupos en las áreas de interés de ambos, así que estoy muy complacido de tener este tipo de reunión de manera periódica, porque hay mucho para hacer, hay mucho para ver, para crear un ambiente mejor para aquellos que utilizan esta herramienta. Así que le devuelvo la palabra. Lo que estamos pensando en hacer, Jonathan creo que va a comenzar estableciendo un marco de la cibercampaña que prevemos hacer y después algo de contenido específico que creo que va a ser muy útil para los miembros.

JONATHAN ZUCK: Excelente, muchas gracias. Muchas gracias. Quisiera recordar al personal que por favor me hagan co anfitrión. Tenemos distintos temas de debate. Están mis colegas de At-Large. Estamos tratando de organizarnos en esta idea de campañas porque hay cada vez más comunidades diversas en la comunidad de la ICANN que vienen a pedir ayuda a At-Large para amplificar el mensaje a la audiencia o para tener nuestra opinión sobre un tema que se está debatiendo. Y la tercera posibilidad es educar a los usuarios sobre un tema en particular. a los usuarios sobre un tema en particular. Entonces, la idea es tener una campaña de seguridad, ciberseguridad y dar un curso como un curso de UA para que la gente se proteja en línea.

Comenzamos la creación del curso y la idea es crear algo como hicimos con el Día de Aceptación Universal, que lo llamamos seminario en una caja. Les damos las presentaciones, las pueden personalizar para el orador. Tenemos un video de alguien que está dando su presentación, preguntas, unos dólares para tener algún alimento para convidar y para poder ofrecer a su grupo, a su unidad constitutiva. Vamos a trabajar en esto para ver cómo puede llegar a ser.

A ver si hay alguna otra persona que está compartiendo pantalla que no me permite compartir la mía. Esto es trabajo en desarrollo. Simplemente para tener una idea, queremos que esto sea claro. Algo que uno podría ver… Esto parece más de Apple que de ICANN, ¿no? Pero bueno, no dije nada, no dije nada. Estoy tratando de que sea amigable para el usuario a medida que vamos avanzando. Probablemente esto sea un curso de dos horas. Yo no voy a dedicarle dos horas ahora, pero simplemente le quiero mostrar un poco lo que estamos tratando de

hacer para elaborarlo. Hay animaciones integradas, hay datos. Son los costos del ciberdelito a nivel global. Debería decir 2023, creo. Hay muchos errores todavía. Es 6 trillones de dólares. Esto viene incrementándose año tras año. Son 10 y medio en 2024.

Tenemos que hablar de distintos tipos de ciberdelitos, hacking, fraude financiero, phishing, estafas en línea, ladrón de identidad. El phishing involucra mucho al usuario final, recibe un correo electrónico que dice, "llame a este número, seleccione este enlace, baje este adjunto", y ahí empiezan los problemas. Eso es lo que queremos concientizar al usuario. Hablemos de phishing, de qué se trata, identificarlo, cómo evitarlo, cómo informarlo. Tenemos algunas animaciones, algunas gráficas. Vamos a hablar de qué se trata phishing. Hay distintos tipos, el spear phishing, el smishing. A ver cómo identificamos el phishing; cuáles son algunas de las tácticas comunes, señales de advertencia, el remitente, si es una solicitud de información personal, una redacción que pide hacer algo urgente. Esos son signos. Y vamos a ver algunas muestras de correos y ver las distintas advertencias en acción de correos electrónicos reales. Estos son algunos que he visto, pero vamos a recopilar más para que la gente comprenda el tipo de redacción que se usa, la IA dificulta la identificación porque toma la información de uno de internet y la adapta al usuario.

Cuando le pide un correo electrónico que haga una cosa, que descargue un adjunto que vaya a un sitio de farming, o que vaya o que disque un número sin cargo. Hay distintos tipos de malware o software malicioso. Simplemente para tener una idea de qué aspecto tiene, evitar adjuntos, números que sean 0800, cómo tratan de hacerse pasar por atención al

cliente, lo que le pidan, cómo evitar los números de teléfono sin cargo. Sé que estoy yendo rápido, pero hay un link en el temario del día que puede llevarnos a ver todo esto con rapidez, pero es simplemente un primer borrador. Algunos tips, como el método de Haber. Cuando uno pasa por encima de un enlace, le dice a dónde va, y acá hay algunos ejemplos de homófonos que no funcionan. Y en ese método, porque utilizan IDN, por ejemplo, viendo algunos distintos ejemplos.

Después hay una encuesta que encontró Eduardo en un punto que armó Google en varios idiomas para identificar correos de phishing y demás. Entonces hacemos que la gente lo use, hablamos de distintos tipos de phishing y después algunas gráficas adicionales. Y finalmente hablamos de las mejores prácticas. Vamos a hablar luego de cómo informarlo, cómo denunciarlo. Primero hay que reconocerlo, hay que evitarlo y cuál es la higiene que uno tiene que tener. Y algo que comentaba Eduardo son las herramientas creadas dentro de la comunidad para facilitar la denuncia; por ejemplo, el asset tool, y vamos a mostrar cómo utilizar estas herramientas. Si quieren ingresar como usuario, dar un paso más y denunciarlo y ayudar al resto de la comunidad una vez que ya lo han evitado.

Esa es la estructura básicamente del curso. Estamos en comunicación con SESAC para mejorarlo, para agregar cosas, pero les quería contar un poquito lo que estamos tratando de armar y lo vamos a traducir a los distintos idiomas y vamos a tratar de armar un paquete tal como se hizo con el Día de Aceptación Universal. ¿Preguntas sobre este tema antes de seguir?

EDUARDO DIAZ: Disculpas que vine tarde, no vi el principio. Yo vengo dando cursos de este tipo. La primera parte de lo que hacemos es explicar cómo leer los dominios de derecha a izquierda y después vemos el esquema, la URL, para saber las distintas partes. Cuando tienen este enlace gigantesco no saben qué quiere decir. Y también les explico cómo el DNS, lo que sucede cuando uno pulsa, selecciona ese URL para tener un contexto. Cosa de que uno muestra después un URL, les muestra el esquema y les muestra qué es lo que sucede al navegarlo.

JONATHAN ZUCK: No voy a absorber todo eso, Eduardo, así que tiene que ser parte del proceso de la mejora de la presentación. Parte de lo que comentó lo hemos tenido en cuenta, pero queremos incluir el resto. Hay preguntas a alto nivel que van surgiendo porque quiero ir absorbiendo y después agregaremos temas específicos.

WARREN KUMARI: Me parece que es una presentación muy linda, mucho mejor que las de anti-phishing que se suelen ver. Pero ¿cómo hacemos que la gente lo vea? ¿Cómo lo distribuimos? ¿Cómo logramos que la gente lo mire?

JONATHAN ZUCK: Todos son experimentos. Por ende, a veces el grupo de dirección de aceptación universal armó un lindo seminario de manera sencilla para dictarlo con una serie de aplicaciones para la gente que tiene audiencias a las cuales dictarles estos cursos. Hay gente que quiere ahorrarse 100 dólares para no dar algo de comer a la gente. Entonces nosotros

participamos en ese proceso y a veces dictan la mitad del contenido. En nuestra infraestructura tenemos organizaciones regionales, inclusive locales que son miembros de las regionales. Entonces, por ejemplo, una organización regional puede tener un subcapítulo localizado y dan presentaciones todos los meses buscando cosas que presentar a sus miembros. La idea es tomar algo de esto, que esté empaquetado, que se dicte fácilmente y solamente hay que llenar la sala y nosotros le pagamos el break y algo así.

WARREN KUMARI: Excelente respuesta. Va a ser muy fructífero esto porque Safer Cyber es muy bueno para la gente del mundo, para los usuarios de la internet y tenemos mucho contenido, mucha información que podemos embalar y podemos brindar o ustedes la embalan después de que nosotros la suministremos.

MATTHIAS HUDOBNIK: Pensando en voz alta, una opción podría ser grabar la sesión y subirla a la plataforma ICANN Learn para que la gente pueda acceder a la misma o presentarla a terceros.

JONATHAN ZUCK: Excelente sugerencia. Tratamos de utilizar nuestra infraestructura de At-Large para trabajar porque la organización quiere que utilicemos su infraestructura para evangelizar sobre el nuevo programa de gTLD. Otros quizás quieran que tengamos mensajes para DNSSEC como Steve o hasta que encuentren otra vía. Entonces, la idea es descalcificar a

nuestra propia vía de comunicaciones para que se puedan utilizar para múltiples campañas. Pero una vez que tenemos la herramienta creada, Matthias tiene razón, cualquiera la puede dictar. Yo puedo hablar en una conferencia, por ejemplo, y esto ya está listo, está en una caja, lo puedo dictar como contenido propio en la conferencia. Puede ser un video, no solo en ICANN Learn.

En el sitio de At-Large o de ICANN tenemos como el inicio de una alianza. No me acuerdo de quién era la idea ahora, uno de los canadienses, que tenemos que tener alianzas con bibliotecas, por ejemplo. Empecé una hermosa relación con la Asociación de la Biblioteca Nacional y las bibliotecas pasaron a ser centros comunitarios. Buscan contenido, cosas que enseñar a sus comunidades y están muy entusiasmados con tener un curso de phishing que puedan sacar de una caja y dictar. Todas estas cosas son excelentes ejemplos. Una vez que tengamos el paquete armado, pasa a ser un producto que se utiliza en diversos lugares.

WARREN KUMARI: Ah, perdón, me olvidé de bajar la mano. Pareciera que una de las cosas más grandes que he visto salir del ALAC que sea listo, útil y qué bueno que está. Quería decir eso.

JONATHAN ZUCK: Gracias. Dedicamos mucho de nuestro tiempo acá en las reuniones de la ICANN quejándonos de las partes contratadas. ¿Por qué no hacen más para proteger al usuario de las registraciones maliciosas y demás? Y no tenemos planes para gritar menos en cuanto a esto, pero tomar la otra parte de la ecuación y decir, bien cuando alguien lo llama y le pide la

contraseña, quizás no la da, y si podemos encarar el problema de ambos lados, estamos cumpliendo el propósito de ayudar al usuario final.

SIVASUBRAMANIAN MUTHUSAMY: A través de ICANN Learn y los seminarios apuntan a personas que ya tienen algo de conocimiento técnico. ¿No debería haber una versión light, liviana, para, no sé, medio millón de hits, medio millón de selecciones?

JONATHAN ZUCK: Lo que estamos tratando de hacer, y esa es una excelente sugerencia, creemos los miembros de las ALS. Esa es nuestra infraestructura, nuestros miembros. ¿Cuál es su audiencia? ¿Cómo llegamos a ellos? Y en eso nos centramos. A medida que tengamos algo de éxito y la comunidad lo vaya reconociendo, tendremos cosas muy creativas y podemos trabajar con bibliotecas, podemos tener una instancia inclusive más con chicos. Sería una excelente idea, gracias por traerlo a colación. No sé quién sigue. ¿Sébastien? Adelante, después volvemos a la cola. Me perdí en el orden.

SÉBASTIEN BACHOLLET: ¿Se va a traducir a los distintos idiomas? Me imagino que quizás queramos no pegarnos a los idiomas de la ICANN porque somos una comunidad mucho más grande. En los seis o siete idiomas, muy bien, pero para este tipo de documento sería útil tener muchos más idiomas. ¿Cómo podemos organizarlo, financiarlo? Sería un muy buen tema para nosotros a futuro, pero muchas gracias.

JONATHAN ZUCK: Excelente tema. Vengo hablando con diseñadores, que es muy divertido, sobre las diapositivas para que no parezcan viñetas nada más y parte de lo que estamos tratando de hacer es que sea gráfico en su naturaleza y agregarle algo de script que es mucho más fácil de volcar que un montón de cosas desparramadas en la diapositiva. Es más fácil traducirlo, pegarlo, organizarlo para que esté en más idiomas. Lo bueno con respecto a este ejercicio de Google es que ya están 20 idiomas aproximadamente.

BUKOLA ORONTI: Durante la presentación observé que dijeron que otra forma de detectar el phishing es utilizando inteligencia artificial. Hay algunos vocabularios que en algunos países africanos no les resulta fácil. En algunos casos quizás no alcance con detectar este phishing. Sobre la base de nuestra experiencia, lo que se suele utilizar, los términos que se utilizan en inglés, son términos comunes en nuestro vocabulario, al menos hablo de la perspectiva de Nigeria, porque hablaron de AI-ish. Son términos o uso incorrecto de términos en inglés. Y a veces esto lo utilizamos para detectar spam.

JONATHAN ZUCK: Les diría que no seamos demasiado específicos ahora, porque no vamos a hablar del proceso, pero en términos breves, lo que se estaba diciendo es que la inteligencia artificial hizo que fuera más fácil para los delincuentes porque cometen menos errores con lo que escriben y hace que estén haciendo más investigación acerca de cada uno de nosotros,

acerca de lo que hay en las redes sociales. Entonces, lo que están diciendo es que la inteligencia artificial funciona en contra de nosotros. Nosotros tenemos que depender de nosotros mismos para detectar si un email es malicioso o no. Ese es el objetivo del curso.

ABDELDJALIL BACHAR: Buenas tardes, voy a hablar en inglés. Soy secretario de AFRALO y creo que es una muy buena presentación. Los usuarios finales necesitan este tipo de presentaciones y será ideal para las ALS. Podemos usar estas presentaciones para los ALS. En las escuelas de gobernanza de internet locales y en los foros de DNS también puede ser muy útil este documento para nuestros usuarios y observamos que en chat, en las redes sociales tenemos muchos problemas como phishing. Usted habló acerca de ciertas cifras acerca de ciertas cifras de 10 mil millones de dólares en 2024. No sé de dónde proviene ese número, en 2024 me refiero.

JONATHAN ZUCK: De un estudio. Yo tampoco recuerdo, sin embargo, está documentado en la presentación. Quiero dejar espacio para nuevos temas que surjan de SSAC. Bueno, una más. Tendrá la última palabra.

PARI ESFANDIARI: Creo que quizás sea necesario ajustarlo en función de las distintas regiones en largo plazo. Al mismo tiempo, pienso que esta es una muy buena herramienta que se puede utilizar para darle más energía a las ALS. Esto los va a ayudar porque les va a dar contenido, les va a permitir

comunicar el mensaje y activarlos también. Creo que podría funcionar en forma bidireccional.

JONATHAN ZUCK: Muchas gracias. Creo que es una muy buena observación. Nosotros tenemos que desarrollar nuestros propios procesos, pero yo creo que uno de los pasos del proceso consistirá en que las RALO miren la presentación y digan si les parece que es necesario cambiarlos para sus regiones, porque quizás podemos traer distintas muestras, ejemplos de emails. La personalización es una buena idea y debería ser uno de los pasos antes de que se lo pase a las ALS, hacer una especie de verificación regional del material. Vamos a ver cuál es el proceso que utilizaremos. Habiendo dicho esto, le doy la palabra nuevamente a Ram.

RAM MOHAN: En el temario teníamos la sección de SAC074. Ustedes verán material que se presenta, que incluye detalles técnicos, pero el objetivo es tomar este tipo de materiales y convertirlo en algo que esté preparado para ser usado en una campaña que sea fácilmente comprensible. Así que lo podemos tachar del temario. Pasemos ahora a Marike. Hace un rato, hace poco tiempo, ese SAC publicó SAC 74 y queríamos presentarles esto y hablar un hablar sobre este tema porque nos parece que es especialmente importante para usuarios finales y para los registratarios. Y pensamos que la mejor persona para presentar este tema es Merike, así que vamos a poner las siguientes diapositivas. Merika está conectada en forma remota y va a hablar sobre este tema.

MERIKE KAEO: Muchas gracias, Ram. Saludos desde Japón. Estoy en otra conferencia, pero pude conectarme, lo cual es fantástico. ¿Por qué asesoramiento sobre gestión de credenciales? Empezamos a trabajar en el 2003 y terminamos en 2015. Hubo dos asesoramientos del SAC 40 y 44 que son recomendaciones con respecto a la buena identificación de la autenticación, pero no eran muy específicos en cuanto a los métodos y la metodología. En la reunión de Durbin en 2013, el Día de la Tecnología, Maarten Van Horenbeeck dio una presentación sobre el secuestro del DNS. Él estaba trabajando en Google en ese momento y a lo largo de cuatro años había identificado 40 países en los cuales Google había tenido problemas con nombres de dominios comprometidos. Y los tres temas principales que él incluyó en su lista, uno tenía que ver con la gestión de credenciales. Y dijo que el atacante intenta autenticar utilizando una lista de contraseñas frecuentes o utilizando una contraseña robada de otra base de datos de autenticación de registros.

Entonces, luego de la reunión de Durbin, una serie de miembros de SSAC que hablaron acerca de este tema y nos preguntamos si había que hacer algo. Y hubo tanto interés que creamos este grupo de trabajo. Las siguientes dos diapositivas son nuestros gráficos, son tablas tomadas directamente de SAC074. Y la razón por la cual lo muestro es que empezamos a hacer una lista con las distintas clases de credenciales que se estaban utilizando en el ecosistema de DNS, identificamos para qué se las usaba y también cuál era la entidad que se estaba autenticando. O sea, cuál era la entidad que usaba la credencial y también cuál era la entidad que validaba la credencial, que podía ser el registratario, el registro, el registrador, privacidad y representación, etc.

Y si pasamos a la siguiente diapositiva, también incluye una lista adicional de estas credenciales. Bueno, era la anterior, pero no importa. Acá lo que mostramos son las credenciales importantes desde la perspectiva de un registratario. Entonces, la relación que tienen con un proveedor del distribuidor o registrador. Entonces, nos centramos en este trabajo desde el punto de vista del ALAC. Tenemos que ver si ALAC quiere tomar parte de este trabajo y comunicar y difundir las prácticas, las buenas prácticas para la gestión de credenciales. Ese es un foco específico de esta diapositiva. Pasamos a la siguiente, por favor. La anterior, por favor.

Una de las cosas que también señalamos es que hay distintas formas en las que se comprometen las credenciales. Esto en general es interesante para algunos usuarios finales porque hay diferentes formas, y cuando vemos todo esto, a veces nos preguntamos, nos decimos que no es sorprendente que haya tantos sistemas afectados. No voy a entrar en detalle porque no quiero excederme del tiempo asignado, pero ustedes luego pueden acceder a estas diapositivas. SAC074, además, analiza todas las etapas e introduce el marco del ciclo de vida de gestión de credenciales. Básicamente, si uno crea una credencial, la cambia o la renueva, tiene que pensar en todos estos diferentes pasos: la distribución, el almacenamiento, encriptación si es necesario, recuperación de una credencial perdida, delegación. Digamos que un registratario quiere cambiar de registrador, básicamente delega algunos aspectos de autenticación, la revocación de las credenciales o la destrucción entonces SAC074 entra en detalle en cada una de estas etapas explica qué significan establece el contexto y también se refiere a las mejores prácticas.

SSAC no creo nuevas prácticas, menciona las normas existentes utilizadas en la industria, como los criterios comunes, el ISO 27000, los requerimientos relacionados con la certificación y también las mejores prácticas en caso de que se utilicen tarjetas de crédito o TCIP. Utilizamos algunas recomendaciones, damos algunas recomendaciones, pero nos referimos a las mejores prácticas de la industria. Creo que todos sabemos ya a esta altura la importancia de la autenticación de múltiples factores. El documento también habla de algunos métodos más sólidos de autenticación, cuáles son los débiles que se pueden explotar más fácilmente, y también hay un aspecto que yo siempre escucho mencionar y que escuché mencionar a lo largo de 15 años. Yo también doy charlas sobre seguridad a nivel global y la gente dice los expertos siempre nos dicen qué hacer pero no cómo hacerlo. El cómo es lo que suele faltar.

Este vínculo proviene de una presentación dada por un registro en Brasil o en la reunión de LACTLD. Estamos haciendo investigación sobre autenticación de doble factor, también consideramos diferentes regiones geográficas. Ellos tenían una diapositiva excelente acerca de cómo trabajar con claves de acceso de una única vez basadas en el tiempo o basadas en HMAC. Lo bueno y lo malo de cada cosa para que otros puedan aprender y obtener información y también aprender a resolver las cosas. Entonces, a modo de resumen con respecto a SAC074, básicamente el objetivo era ofrecer orientación sobre mejores prácticas para registros, registradores y registratarios respecto de la protección de las credenciales. Acá nos estamos focalizando en los registratarios, pero como mencioné en las diapositivas anteriores, mostraron un conjunto de credenciales que administran los

registradores y los registros, pero acá queremos centrarnos en los registratarios.

Y también muestra el marco de ciclo de vida de la gestión de las credenciales y luego el marco se puede aplicar para proteger las credenciales de los registradores y distintas recomendaciones. Y también van a escuchar hablar de esto a OCTO, y la recomendación es que la junta directiva en la ICANN debería indicarle al personal de la ICANN que facilite programas de capacitación prácticos a nivel global para los registradores y registros, en este caso, en función de las mejores prácticas descritas en el documento. El objetivo es que las partes puedan aprender acerca de prácticas operativas y para preservar la seguridad y la estabilidad del ciclo de vida de la gestión de credenciales. En pocas palabras, SAC074.

RAM MOHAN: Muchas gracias, Merike. ¿Alguna pregunta?

SATISH BABU: En primer lugar, gracias por un excelente documento que es SAC074. Los documentos de SAC siempre han sido una fuente de información autorizada para ALAC. En segundo lugar, el material de capacitación del que hablaba Jonathan apunta al usuario final. Nosotros hablamos de usuarios finales que quizás no tiene formación técnica y por eso el material lo simplificamos un poco. Pero hay algunos ALS que sí son organizaciones técnicas. Hay documentos que son para personas técnicas y desarrolladores. Este material también resulta muy útil para abordar parte de ese tema por parte de las estructuras At-Large.

MERIKE KAEO: Gracias.

RAM MOHAN: No veo que nadie más quiera hablar. Jonathan.

JONATHAN ZUCK: Quería agregar algo con respecto a lo que dice Satish. El aspecto que más nos importa acá son los registratarios, a diferencia de los registradores y los registros. Para nosotros, los registratarios son los usuarios y representan una especie de minoría dentro de la comunidad usuarios finales, pero, sin duda, hay muchos que son titulares de nombres de dominio, entonces comunicar esta información a través de nuestra red creo que sería una muy buena idea, especialmente el elemento de cómo hacerlo. Porque tal como dijo Merike, muchas veces nos dicen qué hacer, pero no cómo hacerlo.

RAM MOHAN: Muchas gracias. Pasemos ahora a Yazid.

YAZID AKANHO: Hola a todos. Soy del equipo de participación técnica dentro de la oficina del director de tecnología de la ICANN. Jonathan y Merike ya establecieron el contexto y, por lo tanto, puedo ir directamente al grano. El grupo de participación técnica tiene por misión llevar a cabo actividades de creación de capacidades, desarrollo de capacidades en todo el ecosistema para las diferentes partes interesadas de la

comunidad. Y por supuesto, desarrollamos distintos materiales, distintos cursos. Actualmente, ofrecemos cursos en tres idiomas: inglés, francés y español. Por supuesto, tenemos un equipo regional. Cada uno de nosotros se centra principalmente en sus regiones correspondientes. Llevamos a cabo mucha capacitación. Esta es nuestra actividad central. Desarrollamos material de capacitación, presentaciones, organizamos talleres y también, por supuesto, actividades prácticas para los registros, los registradores, los proveedores de servicios de DNS en general. Pero también llevamos a cabo actividades de desarrollo de capacidades con partes interesadas tales como agencias de aplicación de la ley, universidades, incluso entes reguladores, funcionarios del gobierno. Pasemos a la siguiente diapositiva, por favor.

En relación con la gestión de credenciales de la que estábamos hablando, tenemos un curso totalmente dedicado a este tema. Pueden entrar en nuestro catálogo de cursos, en el sitio web de la ICANN. El curso número 15 se ocupa de este tema. Recientemente comenzamos a revisar todos nuestros cursos, porque estos cursos existen ya desde hace unos cuatro años, e introdujimos el curso sobre el ciclo de vida de la gestión de los credenciales en seis de los otros cursos que identificamos como pertinentes.

Entonces, básicamente, cuando uno toma el curso de operaciones de registro para los operadores de registro con código de país. Cuando hablamos de uso indebido del DNS, es obvio que hablar de gestión de credenciales es crítico en relación con este tema. Entonces, el curso sobre el ciclo de vida y la gestión de credenciales introduce el concepto de las credenciales, qué son, cuáles son las diferentes versiones por así

llamarlo de credenciales donde se las utiliza dentro del ecosistema del Dans. Todos sabemos que el DNS está muy distribuido. Hay múltiples sistemas que interactúan y que son gestionados por diferentes entidades, organizaciones. La audiencia incluye principalmente a ingenieros, que son quienes supervisan las operaciones de los sistemas del DNS en la infraestructura, pero también incluimos a personal de políticas, como dije antes.

Aquellos que redactan las políticas, y también los administradores porque en general son quienes están a cargo de desarrollar los procedimientos, las políticas y de asegurarse de que los ingenieros y el equipo que opera los diferentes sistemas cumpla con estas prácticas y políticas. Entonces, acá en este curso también se genera conciencia en el grupo de los administradores. La duración depende del tipo de actividad, pero básicamente, si es un curso en línea, dura entre una hora y media y dos horas con todo tipo de interacción, preguntas, etc. Y también llevamos a cabo cursos prácticos. A veces, cuando hacemos creación o desarrollo de capacidades prácticas con las partes interesadas, hacemos que estas partes descubran cómo, por ejemplo, crear una autenticación de múltiples factores. A veces la gente piensa que para eso tiene que comprar algún sistema muy costoso, pero, básicamente, se puede utilizar el sistema nativo para implementar esto.

Estos son casos prácticos que implementamos durante nuestros cursos. Por supuesto, el DNS 101 es el curso que hay que tomar como prerequisito para tomar el curso de ciclo de vida de la gestión de las credenciales y cubre distintos aspectos que Merike ya explicó en su presentación anterior. Pasamos a la siguiente, por favor. En breve, esto

es una reseña del material para laboratorio en línea. Es un ambiente virtual que proveemos a cada participante que tiene una serie de máquinas virtuales que corren en Linux Ubuntu, y así llevamos a cabo la capacitación. Es algo práctico. Recientemente, la semana pasada estuve en Camerún con ccTLD, registradores, ministerios, administradores de sistemas que a menudo trabajan con los servidores e infraestructura del Dans. Hablamos del curso de gestión de credenciales y lo mismo se llama a cabo en Latinoamérica, en Asia-Pacífico y en Europa con las distintas partes interesadas de cada lugar.

Estamos brindando el recurso correcto a la gente correcta. La gente que puede ayudar a divulgar el ciclo de vida de gestión de credenciales, los principios, las mejores prácticas dentro del ecosistema. Y estaríamos dispuestos, como dijo Satish, a participar. Tenemos un curso de desarrollo de capacidades para instructores. Hay diversas avenidas que pueden ayudarnos a todos a divulgar mucho más todo esto en la comunidad. Le paso la palabra a Jonathan. Muchas gracias.

RAM MOHAN: Creo, Jonathan, que ya hemos hecho una visión preliminar. Comentaba también Satish, un agregado útil puede llegar a haber dos caminos; el del usuario técnico y el usuario final. Con distintos niveles de materiales para cada uno y creo que esto es una buena lección para llevarnos. Sébastien, creo que es una mano anterior, ¿no? Usted tiene la mano levantada, Claire.

CLAIRE CRAIG: Quería decir que miré esta presentación y me pareció que era muy informativa. Particularmente, aunque hablamos en ALAC a nivel de usuario final, interactuamos con parte de la comunidad técnica en distintas áreas. Desde donde yo estoy, les cuento que hacemos mucho trabajo a través de la oficina de CTO. La gente viene a algunas reuniones, pero no era consciente de que tenían como un catálogo de cursos de los cuales podemos seleccionar lo que nos interese. Esto es muy informativo y nos puede ayudar en alguna de las sesiones que prevemos tener más adelante. Así que muchas gracias por la presentación.

RAM MOHAN: Muchas gracias. Muchas gracias a Merika por presentar todo esto desde Japón. Antes de pasar al punto siguiente, que es sobre colisión de nombres, algo que quería compartir con ustedes es, dentro de SSAC ahora tenemos un cierto nivel de consenso de que tenemos algunos temas sobre los cuales hay un nivel persistente de interés e información que esperamos que siga habiendo participación. No están en un orden en particular, uso indebido del DNS, nuevos gTLD, pero SSR, el aspecto de seguridad y estabilidad de los nuevos gTLD, problemas de protocolo de DNS, DNSSEC, esa área, espacios de nombres alternativos y finalmente SSAR. Los aspectos de la gobernanza de Internet de SSAR. Son seis áreas que esperamos desarrollar, tanto material, contenido, recopilar, curar la información de lo que ya hemos hecho, lo que planificamos a futuro. Personalmente creo que tenemos esas áreas unidas, lo que pueden constituir un terreno muy fértil para elegir. Hay interés en esta área, hagamos, consigamos contenido de aquí y

construyamos algo para las comunidades a las que queremos atender. Adelante.

YAZID AKANHO: Me olvidé de hablar de que la comunidad puede pedir capacitación, así que envíennos un correo a OCTO en ICANN.org y vamos a comunicarnos y planificar la interacción. Les decía que tenemos personal en todas las regiones. Yo personalmente y Simon Mayoye en África y Medio Oriente, Champika para Asia-Pacífico, Nicholas para Latinoamérica, David Huberman para Norteamérica, y Ulrich para Europa.

RAM MOHAN: Muchas gracias.

JONATHAN ZUCK: A veces nos olvidamos que lo que hace OCTO y es muy bueno que se nos recuerde hablar nuevamente.

RAM MOHAN: Muchas gracias. Creo que tenemos que pasar al tema que sigue, que son colisiones de nombres. Hemos elaborado algo de asesoramiento sobre posibles colisiones de nombres. Es un punto muy importante. ¿Matt está en línea?

MATT THOMAS: Sí, Ram, ¿me escucha?

RAM MOHAN: Lo escucho un poco bajo.

MATT THOMAS: ¿Me escucha bien?

RAM MOHAN: Sí, así es mejor. Le paso la palabra a Matt para que comience con el tema.

MATT THOMAS: Gracias, Ram. Voy a ser breve y pido disculpas. Vengo batallando con un resfrío desde hace semanas, así que mi voz no es de las mejores, pero hablaremos un poco de posibles colisiones de nombres y el trabajo que realizamos, que nos llevó varios años. En general, son un problema que continúa las posibles colisiones de nombres de 2012 cuando SSAC comenzó a publicar su asesoramiento. Estas pueden traer interrupciones de la red, exponer datos delicados o sensibles, exponer datos delicados o sensibles, crear etiquetas, crear ataques y están expuestas a distintos factores de ataque y explotar vulnerabilidades. En la última década hemos visto nuevas tecnologías que han evolucionado introduciendo también otros escenarios imprevistos de posibles colisiones de nombres. En la próxima ronda de gTLD delegados, la introducción de nuevos TLD directamente incrementa la probabilidad de potenciales colisiones.

Desde la última perspectiva de 2012 hasta el momento, hay diversos eventos notables de relevancia. Uno, el basarse en datos del servidor raíz solo, no tan eficiente como lo era en 2012. Hay numerosas

evoluciones del protocolo DNS, así como también nuevos cambios de tecnología que han afectado la telemetría que se observa en los datos del servidor raíz, que respecto a lo tradicional de 2012 que nos permitía evaluar los riesgos de colisiones de nombres que no es lo mismo que lo que tenemos hoy. A menudo uno puede mirar atrás y ver la consideración colectiva desde un repositorio central de los datos del Dans y los datos de internet, la vida útil de estos ya no era una opción factible lo que nos lleva solamente a evaluar una serie de datos de telemetría recopilados como Parcex en los servidores raíz en los cuales uno puede encontrar protecciones con falta de uniformidad o en el análisis de potenciales cadenas que pueden tener colisiones.

Esto nos lleva a una situación en la cual la falta de coherencia o consistencia, dado que no hay capacidad centralizada de observar toda la telemetría vinculada con una cadena de colisión específica, y esto nos lleva a la próxima ronda porque hay influencias en cómo las guías de colisión posible de nombres se deben llevar a cabo de manera repetible y sostenible. El estudio NCAP número 2, lo que quiere decir marco de evaluación de riesgo de colisión de nombres, trata de establecer un marco para crear un marco sostenible, repetible y determinístico que permita facilitar la evaluación de la colisión de nombres de manera continua, incluidas cuatro características principales, la primera de las cuales es la evaluación integral de riesgo.

Recordarán allá para el 2012, las colisiones de nombres era algo puntual dentro del proceso de colisión de nombres y del otorgamiento en ese momento. Acá tenemos colisión de nombres como parte del proceso de revisión general e incluidos en el proceso general para que la seguridad

no sea un botón al final de la lista. En segundo lugar, el establecimiento de un equipo TRT de revisión técnica que introduce un equipo dedicado para evaluar las nuevas cadenas propuestas de TLD que se basan en los datos de telemetría que se recopilan a partir de los distintos puntos de la jerarquía del DNS para su análisis empírico.

En tercer lugar, tenemos la introducción o la propuesta de recopilación de datos ampliados. Estos son nuevos mecanismos que permiten la recopilación de datos tanto cuantitativos como cualitativos de conjuntos de datos de disposición pública y de aquellos adaptados a las especificidades de las solicitudes de gTLD para ampliar la evaluación de colisión de nombres. En cuarto lugar, la prescripción que permita tener múltiples métodos de evaluación en cuanto a la recopilación de datos. El proyecto de colisión de nombres considera diversas metodologías que, en pos de la robustez de los datos que permitan evaluar las colisiones de nombres de diversas maneras.

En un proceso directo, el proceso de colisión de nombres tiene cuatro etapas. La cero comienza con los solicitantes que tratan de identificar potenciales inconvenientes antes de presentar su solicitud ante la ICANN buscando datos públicos, tales como de magnitud de ITH, u otros que sean indicadores fundamentales de riesgos en cuanto a las colisiones de nombres para las cadenas que puedan estar solicitando. Esto no es un indicador de aceptación o rechazo, pero, sin embargo, nos da un conocimiento a priori de que haya o no haya potencial de riesgo de colisión. Habiendo calificado esto como que la cadena de caracteres no aparece en la lista, esto no implica totalmente que ese nombre no sea nulo en cuanto al riesgo de colisión, pero es al menos un esfuerzo

para lograr información para darle al solicitante a priori. Una vez que el solicitante ha presentado su solicitud de cadena de caracteres, pasa a la etapa 1. El equipo TRT la evalúa y otros datos que tengan a disponibilidad, incluidos algunos públicos que estaban a disposición del solicitante pre-solicitud y que evalúan en la toma de decisión sobre si la cadena de caracteres es de alto riesgo o no.

Una vez que esto avanza, si no es de alto riesgo, pasa a la etapa 2, la evaluación de colisión de nombre. ICANN temporariamente delega el TLD a la zona raíz y el equipo de revisión técnica realiza uno o más de las siguientes evaluaciones, que no haya interrupción, interrupción controlada, interrupción visible y hay interrupción visible y notificación. Esas son algunas de las multitudes de las técnicas mencionadas que claramente se adaptarían a las cadenas solicitadas, vinculadas a la discreción del equipo de revisión técnica. Este es un método en el cual el equipo de revisión técnica tiene la posibilidad de recopilar el telemetría adicional de distintos puntos en el DNS para ampliar su evaluación del riesgo de colisión de nombres que se están dando.

Lo que finalmente nos lleva a la etapa 3. El equipo TRT presenta una recomendación a la junta. Se pueden brindar planes de mitigación si hay un alto riesgo de colisión de nombre. Se repite todo este proceso pero al fin y al cabo la Junta toma la decisión definitiva sobre la aprobación de la solicitud y potencialmente asignar la cadena de caracteres a una lista de cadena de caracteres en colisión si el riesgo es alto. En resumen, respecto de la recolección de datos, no estamos en el 2012. No podemos reutilizar los métodos de detección que utilizábamos en esa época.

La interrupción controlada en la última ronda fue efectiva en cierta medida, pero tenía sus limitaciones. Para IPv6 no funciona. También los datos de colisión de nombres estaban vinculados estrechamente a la recolección de datos de los servidores raíz y el Dans que, hoy por hoy, debido a la evolución de los protocolos del DNS y mecanismos de recolección de datos, esto se ve afectado en gran medida y es mucho más difícil hacer un análisis de posible colisión de nombres. Entonces, para hacer un análisis serio de posibles colisiones de nombres, uno tiene que recopilar los datos de manera diversa. Es imposible simplemente basarse en un caso generalizado en la raíz.

Esa evaluación solo en la raíz puede afectar la posibilidad u otro factor de riesgo de nombres específicos que se están evaluando. Creo que la organización ha expresado alguna inquietud respecto de los riesgos en cuanto a la privacidad y la confidencialidad. Creo que Ram va a hablar un poco de este tema luego. Y le paso la palabra, entonces.

RAM MOHAN: Vamos a solicitar que las preguntas queden para el final. En la próxima diapositiva vemos que lo que presentó Matt era… Ah, perdón, Matt, le quedó esta diapositiva y después me pasa a mí, me parece. ¿Sí?

MATT THOMAS: Ah, sí, gracias, Ram. Entonces, lo otro que quería comentar sobre todo esto es que claramente el equipo de revisión técnico TRT es un aspecto esencial sobre cómo manejar la colisión de nombres a futuro. Es una función muy técnica que hay que cumplir, una actividad que requiere grandes capacidades. No hay solución única. Una de las cosas que está

hablando el equipo y hace muchas veces es que cada cadena es una especie de copo de nieve especial. No hay un único caso, no hay una sola solución para las colisiones posibles de nombres. Para verificar que el TRT tenga éxito, tiene que tener personal con las capacidades correctas, que sean flexibles para entender los distintos aspectos de las metas, roles y responsabilidades. Y también tiene que ver los datos históricos, así como los datos a futuro, con el objeto de comprender efectos potenciales tales como gaming, manipulaciones, cambios de jerarquía del DNS, afectaciones a la telemetría del DNS, e incorporarlos en la evaluación del DNS en cuanto a colisiones de nombres.

Es una función muy especializada. Hay que lograr las personas adecuadas para ocuparse de esta actividad y ese es un paso crítico para hacer una evaluación de colisiones de nombres de aquí en adelante. Ram, le doy la palabra.

RAM MOHAN: Gracias. Matt y Susanne ayudaron a avanzar con el grupo de discusión que es un trabajo intercomunitario con el fin de preparar este documento que Matt acaba de resumir. Después lo que hizo SSAC fue tomar ese informe y lo consolidó en un asesoramiento específico que le dimos a la Junta Directiva de la ICANN. No voy a leer todo lo que figura acá, pero nuestros hallazgos fueron que hay dos clases de riesgos: el riesgo de delegar. Tenemos el riesgo alto de exponer datos personales. Y luego tenemos el riesgo de privacidad asociado con la evaluación de las colisiones de nombres. Son dos clases de riesgo, ¿no? Nuestra recomendación fue muy simple. Le dijimos a la Junta Directiva de la ICANN que adopten el marco de gestión de riesgos que está

proponiendo el grupo de colisión de nombres, porque no se trata de tecnología, no se trata de dinero, se trata de riesgos y de asegurarse de que a medida que surjan nuevos TLD, podamos primero medir y luego mitigar las posibilidades de que haya un problema de seguridad y estabilidad.

Y también sugerimos que, si están pensando en priorizar las cosas, la junta directiva de la ICANN debería priorizar la mitigación del riesgo de delegación a diferencia de la evaluación del riesgo de evaluación. Una de las cosas que surgieron en nuestro análisis y en nuestras conversaciones fue que la organización de la ICANN llegó con un diálogo muy útil y constructivo, y lo que dijeron fue: Si ustedes nos piden a nosotros, la ICANN, que vayamos a evaluar todos estos nombres que se están solicitando, inevitablemente van a surgir datos de privacidad y vamos a estar obligados a manejar, gestionar y evaluar todos esos riesgos, especialmente cuando el grupo de discusión dijo que el método de interrupción visual del que hablaba Matt y el método de interrupción visual con notificación, estos son métodos en los que existe la posibilidad y probabilidad de que la información de identificación personal aparezca.

Entonces ellos dijeron, quizás un modelo mejor podría ser que recibamos todas las solicitudes, luego pasan por un proceso de evaluación normal, pero cuando se trata de la evaluación de las colisiones propiamente dichas, solo vamos a hacer eso una vez que los nombres sean asignados a los solicitantes. Si alguien fuera el ganador, por así llamarlo, del TLD, vamos a decir, bueno, le otorgamos a usted el TLD, pero antes de permitir que pueda ser delegado en internet y que

pueda usarse en internet, necesitamos que lleve a cabo estas pruebas. Y luego, en función del resultado de estas pruebas, vamos a decidir si pueden utilizarlo o si hay que llevar a cabo medidas de mitigación, etc. Nosotros pensamos que, por supuesto, este es un método posible, factible, pero pensamos que lo único que logra es postergarlo un poco. Si tenemos información de identificación personal, ya sea que lo hagamos al principio o al final del proceso, tenemos que hacer este proceso. Entonces, no estamos reduciendo el riesgo de privacidad de esta forma. Uno podría argüir que se podría tercerizar ese trabajo a todas estas personas u organizaciones que van a solicitar TLDs.

Pero podría existir el potencial de que haya una implementación dispareja y, en cierta forma, si hay una violación de la privacidad, un problema con la privacidad, lo único que vamos a saber es que nos vamos a enterar después de hecho. Y después tenemos que ir a esa persona, organización, y exigirle que contractualmente haga algo. Digamos, parece más dificultoso. Entonces, estamos pensando en que sí implica más trabajo para la organización de la ICANN, sí existe la probabilidad y la preocupación, pero lo que realmente estamos diciendo es, escuchen, hagan el trabajo, hagan el trabajo de una vez, al principio, y también pensamos que esto implica lograr eficiencias, porque si ustedes lo están evaluando y se dan cuenta de que los datos muestran que es una cadena de caracteres de alto riesgo, no pasamos por todo ese proceso de conjuntos de controversias, ni subastas, etcétera.

Simplemente decimos, tenemos que dejarlo de lado. Entonces, hay una parte de sentido común y hay una parte de aspectos prácticos. Pero en

última instancia, la Junta Directiva de la ICANN debe decidirlo. Hemos tenido conversaciones muy productivas con algunos comités. Hemos tratado de informar al comité técnico y de riesgo acerca del equilibrio de riesgos, y hemos compartido con ellos el hecho de que uno no se aleja del riesgo de privacidad. Si pensamos que se puede elegir y que la opción de hacer la evaluación en el momento de la delegación es la mejor opción, entonces deberíamos ser muy cuidadosos al decidir esto. Bueno, esto es lo que dijimos. Pasamos ahora a la siguiente diapositiva. Y esta es la pregunta que nosotros tenemos: una de las cosas que viene diciendo la gente es, con el marco que propuso el grupo. Si se hace esto, entonces podemos manipular los datos. Si hay otra parte que quiere impedir que alguien acceda a un TLD, puede de una forma bastante directa pedirle a una máquina que cree toda una serie de colisiones que luego pueden generar un problema.

Entonces, pensamos que podría ser un problema, y no proponemos una solución, simplemente decimos que reconocemos que este podría ser un problema. Matt, ¿hay algo que usted quisiera agregar? ¿O los demás miembros de SSA que participaron en este trabajo quieren agregar algo antes de que pasemos al intercambio?

MATT THOMAS: Estoy dispuesto a responder cualquier pregunta o comentario.

JONATHAN ZUCK: Supongo que es todo un principio. Usted mencionó que una de las conversaciones que tenemos con el GAC y con la organización tiene que ver con la resolución de controversias y la idea es evitar todo ese circo

que tuvo lugar en la ronda del 2012 con subastas privadas, etc. Una de las recomendaciones que surgieron de nuestro grupo fue que las controversias por la subasta se resolvieran antes del proceso, del inicio del proceso. Y habiendo leído el informe de ustedes y hablando de este tema, parecería que tenemos que mitigar este tema, pero si no sabemos con quién tenemos una controversia, no vamos a poder tratar de evitar que otro acceda a un nombre. ¿Tiene sentido esto? ¿Es lógico?

RAM MOHAN: Le voy a explicar cómo lo veo yo. En general, la ICANN publica todos los TLD que se solicitaron. La revisión de controversias por subasta tiene lugar antes, pero en este punto la ICANN publicó una lista y el análisis de colisiones tiene lugar posteriormente. En ese caso sí existe ese potencial. Warren.

WARREN KUMARI: ¿Hablo yo? Hay algunas cosas que se pueden hacer por anticipado. Por ejemplo, la ICANN puede dejar de enviar consultas ahora a .coke. Entonces, cuando coke haga una solicitud, lo veremos. Entonces, aún si no sabemos quién utiliza o quién va a estar en un conjunto de controversias, hay algo que se puede hacer. Hay formas adicionales de hacerlo.

JONATHAN ZUCK: Nuestro deseo es tratar de abordar la resolución de controversias de una forma diferente.

WARREN KUMARI: Es cierto, pero si estamos en la industria, podemos hacer buenas suposiciones con respecto a quién puede solicitar qué cadena de caracteres. Esta suposición no va a ser perfecta. Por ejemplo, yo sabía que iba a haber un grupo de personas que iban a pedir .corp o .queen. Hay nombres que sabemos que la gente va a solicitar. Entonces, en ese caso, lo sabemos con seguridad. En otros casos, podemos hacer algunas deducciones o suposiciones. ¿Jim?

JIM GALVIN: Sí, gracias. Creo que lo importante en este caso es no unir dos temas separados. Tenemos el tema de los conjuntos de controversia, tenemos las subastas y colisiones de nombres. El informe sobre colisiones de nombres fue muy cuidadoso en cuanto a no decir en qué momento debe hacerse el proceso de diligencia debida, porque hay mucho más análisis que debe considerar la organización de la ICANN en términos generales. Lo único hacia lo que avanza el grupo de trabajo y que aprueba SSAC es que la diligencia debida debe hacerse antes de que se otorgue el TLD. Ahora, y esta es mi perspectiva personal con respecto a cuándo debe tener lugar una colisión de nombres, yo creo que debe ocurrir antes de que se resuelva el conjunto de controversias, ¿y por qué? Porque una parte del proceso de análisis de condiciones de nombres es que, si la cadena finalmente es una cadena de alto riesgo, esto podría ser información útil para aquellos que están en el conjunto de controversias porque quizás quieran decidir, “uy en realidad no quiero esta cadena”. O, lo que es más importante, es el solicitante, una vez que descubrimos que hay una cadena de caracteres que es de alto riesgo, el solicitante

tiene que tener la oportunidad de crear un plan de remediación o mitigación.

Esa información, entonces, es necesario tenerla en entrada. Yo, al menos, como solicitante, querría saber a qué me voy a enfrentar, y eso afectaría la forma en que yo me siento con respecto a mi lugar en este conjunto de controversias. Pero esa es la especie de impacto y consecuencia que la ICANN debe evaluar junto con todas las relaciones entre el conjunto de controversias y el resto de la diligencia de vida. Es interesante en ese sentido. Gracias.

RAM MOHAN: Gracias. Creo que Justine quiere tomar la palabra.

JUSTINE CHEW: Dos puntos. Por un lado, quería hablar acerca de lo que explicó Jim. El punto de vista de recomendaciones de políticas sobre procedimientos posteriores, Jim tiene razón: no hay una recomendación en términos de qué hay que usar. La recomendación básicamente dice que el marco de colisión de nombres existentes se aplica a menos que la Junta decida utilizar otra cosa. Entonces, no habla acerca de dónde está ese proceso en toda esa fase de delegación. Esa es la razón por la cual el estudio 2 de NCAP, si es aprobado por la junta directiva, bueno, luego la organización deberá determinar cómo hacerlo, pero el desafío de las subastas es que hay recomendaciones existentes ya aprobadas por la Junta, recomendaciones de políticas, que hablan de algunas acciones de último recurso.

Entonces, tenemos que invertir eso y avanzar hacia un conjunto de resolución de controversias por cadenas de caracteres diferentes. Pero el punto que quería señalar es que yo creo que NCAP estudio 2 es un trabajo sobresaliente y extremadamente útil en cuanto a qué guía el procedimiento para resolver el riesgo de colisiones de nombres en la próxima ronda. Y realmente valoro el hecho de que SSAC el grupo de debate de NCAP, que estaba abierto a otras personas que no eran miembros de SSAC, pudieran también trabajar en estos informes. Entonces, espero que haya oportunidades adicionales para que quienes no son miembros de SSAC puedan participar en el trabajo que hace SSAC.

RAM MOHAN: Gracias, Justine. Esa es nuestra intención, continuar invitando a miembros de la comunidad para hablar acerca de los temas pertinentes. Creo que está Hadia. Creo que Hadia quiere pedir la palabra. Nos quedan 10 minutos, creo. Así que si alguien más…

JONATHAN ZUCK: Hay preguntas en el chat.

RAM MOHAN: Sí, lo vi. Si alguien más quiere hacer una pregunta, levanten la mano ahora en el chat. Veo a Satish, Alan y Gopal. Si hay alguien más, levanten la mano. De lo contrario, vamos a cerrar la lista y a continuar.

HADIA ELMINIAWI: Gracias. Iba a decir que el momento en el que tiene lugar la evaluación de colisiones de nombres es muy importante. Por supuesto que esto es muy distinto de la resolución de controversias. Sin embargo, si lo hacemos posteriormente, después de la delegación y si pasamos por la resolución de controversias, etcétera, pasamos por todo esto y después se lo delega y después hacemos la evaluación, ¿qué pasa si es de alto riesgo? Si la cadena es de alto riesgo. Y, además, la manipulación de datos también podría ocurrir en ese momento. ¿Qué impediría que ocurriera después de la delegación cuando en realidad el solicitante necesita pasar por el proceso de evaluación? Esto podría pasar de todas formas. Además, según recuerdo, el estudio de NCAP dice que si se considera acepta esa cadena de caracteres de alto riesgo, entonces el solicitante puede proponer un marco de mitigación. Y ese marco de mitigación podría ser analizado y quizás luego se acepta esa cadena de caracteres. Entonces, hay un camino de allí en adelante, pero ese camino hay que analizarlo de forma anticipada.

RAM MOHAN: Estoy de acuerdo, Hadia. Matt, hay una pregunta en el chat. ¿Podría leer la pregunta y luego responderla?

MATT THOMAS: Sí, por supuesto. Creo que la pregunta es la interrupción controlada por una wildcard. ¿Aún se utiliza en ICANN? El operador registro implementará la interrupción controlada durante 90 días, insertando registros especiales en su archivo de zonas TLD. Se refiere a las recomendaciones que surgen de NCAP estudio 2. Nosotros

específicamente no tratamos de ser excesivamente específicos con el equipo de revisión técnica, sino más bien nos apoyamos en su asesoramiento respecto de la implementación sobre una base cadena por cadena.

El estudio 2 de NCAP consideró cuatro implementaciones o diferentes implementaciones técnicas dentro de la telemetría del DNS que pudiera reunirse con una perspectiva más holística o colectiva para contar con más material. Yo diría que específicamente no es algo que se esté utilizando, sino que el espíritu de la recomendación es que el equipo de revisión técnica implemente, según su criterio, los mecanismos adecuados para recopilar los datos que consideran necesarios para hacer una evaluación de colisiones de nombres, mientras que el informe, propiamente dicho, describe cuatro de las mejores técnicas que el grupo de discusión pudo enumerar en su momento y sobre el cual pudo ofrecer guías técnicas.

RAM MOHAN: Satish.

SATISH BABU: Muchas gracias. El SAC0124 me parece un trabajo muy valioso. Mi pregunta en realidad es una pregunta aclaratoria. En el marco propuesto, el marco propuesto parecería estar basado en la delegación temporaria durante la delegación inicial. ¿Qué ocurre después de la delegación inicial y después de la re-delegación? Continuamos teniendo este riesgo de colisiones de nombres.

JONATHAN ZUCK: Matt, ¿quiere responder?

MATT THOMAS: Es una pregunta complicada. Obviamente, siempre debe haber un equilibrio en cuanto a la cantidad de cambios que se aplican a la raíz al delegar un nuevo gTLD en el 2012. Esa delegación tenía lugar después del otorgamiento del TLD. Una vez más, no estamos siendo especialmente prescriptivos con respecto a las recomendaciones con respecto a cómo hay que implementarlo. Recibimos invitados de la IANA, quienes expresaron sus preocupaciones con respecto a cambios en la zona, la escalabilidad, y todo esto se incorporó a la raíz. Creo que será un trabajo que se hará caso por caso. Hay situaciones en las que los riesgos de colisiones de nombres son elevados y las situaciones a las que usted quizás se refiera están lejos de ser la norma. Por lo tanto, es probable que no estemos hablando de un evento repetible, sino de un caso poco frecuente.

RAM MOHAN: Gracias. Esto fue todo para Satish. Alan tiene la última palabra.

ALAN GREENBERG: Quisiera felicitarlo respecto de su explicación restringida del hecho de que se hiciera la prueba post facto y que lo hiciera otro. Me impresionó mucho como lo dijo. Pero el seguimiento de esto, el concepto de diferirlo hasta que esté prácticamente delegado y después pedirle al grupo al que se le delega que haga las pruebas de ellos, reduce la

responsabilidad civil y los riesgos de la ICANN. Por otro lado, asignar la responsabilidad de hacer las pruebas a un grupo que tiene muchos intereses en decir que no hay problema. Y respecto del riesgo de privacidad a un grupo que quizás no sea confiable y nosotros no lo podemos evaluar. Hay tantas razones para no hacer eso.

RAM MOHAN: Me estoy sonriendo. Pensamos lo mismo. Tenemos esperanza. Tengo un optimismo cuidadoso en el sentido de que la gente de la Junta leyeron el material, estuvieron preparados, hicieron buenas preguntas. Parecían comprender los matices subyacentes, no solamente en una reflexión primero protejamos a las cosas. Tengo esperanza. Jim dice que la pregunta va a estar frente a la Junta muy pronto y es parte de la razón por la cual estamos aquí compartiéndolo. Como una pregunta específica, creo que va a ser muy útil que ALAC hable también con el representante de la Junta, verificando que tengan todas las novedades sobre los matices de este tema.

JONATHAN ZUCK: Creo que terminamos. Siempre es muy bueno tener este todo esto previo para tener lógica puesta en común entre nosotros para que tenga sentido. Nuevamente, aprecio mucho que estén con nosotros, que compartan sus ideas, y como norma general, hemos hablado en privado sobre las recomendaciones realizadas que parecen no avanzar en la Junta y ese tipo de cosas. Especialmente cuando hay distintas implicancias de volver a traer a la superficie estos temas y volver a recordar a la Junta sobre estos temas cosas que deberían recordar. Es

un trabajo muy importante y nada debería terminar en el último cajón. Gracias a todos, gracias por venir.

RAM MOHAN: Gracias. Gracias por invitarnos y que podamos hacer nuevamente esto.

JONATHAN ZUCK: Se levanta la sesión.

[FIN DE LA TRANSCCRIPCIÓN]