TIJANI BEN JEMAA: Buenos días, buenas tardes, y buenas noches a todos. Este es nuestro sexto seminario web, dentro del marco de creación de capacidades de ALAC. Establecido para las ALSes y sus representantes. Y recurrir Y hoy tenemos a Julie Hammer, quien nos va a hablar de la seguridad y la estabilidad del DNS y ha compartido su presentación en el Adobe Connect.

En primer lugar, le voy a pasar la palabra a Terri, para que haga los anuncios habituales, y que mencione cuáles son las reglas. Terri, adelante.

TERRI AGNEW: Buenos días, buenas tardes, buenas noches a todos. Bienvenidos al seminario web previo a ATLAS II, de creación de capacidades, el día 15 de mayo de 2014 a las 13:00. No vamos a tomar asistencia porque es un seminario web y le pedimos a todos los participantes que silencien sus micrófonos y sus computadoras. Y al momento de hablar, que mencionen su nombre, no solamente para los intérpretes, sino también para la transcripción y para permitir a los intérpretes que los identifiquen en los canales correspondientes. Contamos con interpretación en español y francés. Le cedo la palabra a Tijani.

TIJANI BEN JEMAA: Muchas gracias, Terri. Ahora, Julie Hammer ya se encuentra lista para dar el seminario. Julie, buenos días para usted. Adelante por favor.

JULIE HAMMER: Buenas noches, aquí en Australia es de noche. Muchas gracias, Tijani. Me gustaría presentar algo de información sobre el rol de la ICANN en la seguridad y estabilidad del DNS. Y aquí tenemos las pautas generales del seminario web.

Uno es la definición de la seguridad y estabilidad. Dos es que tenemos el rol de la ICANN. Tres vamos a hablar de por qué es importante la seguridad y la estabilidad. Hablaremos sobre el Comité Asesor de Seguridad y Estabilidad, el SSAC. Y les daremos un ejemplo de un ataque de seguridad. Esto es el total del seminario. La idea de este seminario es tratar de cubrir todas las cuestiones o conceptos de seguridad. Y luego les voy a dar la palabra para que hagan preguntas.

En primer lugar, la ICANN tiene una misión técnica, que es limitada. Y está definida en una serie de documentos, relacionados con el marco de estabilidad, flexibilidad y seguridad. La misión técnica es preservar y mejorar la estabilidad, seguridad y flexibilidad de los sistemas y también mantener el sistema único de identificadores de Internet. Básicamente, hay tres misiones: una tiene que ver con la coordinación de la asignación del sistema de identificadores únicos de Internet. Luego mantener y operar el servidor de raíz L y sus instancias, y luego administrar los propios sistemas internos de la ICANN y proporcionar un portal de acceso para difundir y compartir información.

Nosotros nos vamos a focalizar en la segunda misión. Entonces, las definiciones de seguridad, estabilidad y flexibilidad son las siguientes.

La seguridad es la capacidad de proteger y prevenir el uso abusivo de los identificadores únicos de Internet. Y tenemos que tener en cuenta que estamos hablando de los números y de los nombres del DNS, es decir, números y nombres.

La definición de estabilidad es la siguiente: es la capacidad de asegurar que el sistema opera tal como se espera y que los usuarios de estos identificadores únicos tienen confianza en que el sistema opera tal como se espera.

La definición de flexibilidad es: la capacidad del sistema de identificadores únicos de tolerar, poder superar efectivamente, ataques maliciosos y otros eventos de interrupción, sin poner en peligro el funcionamiento.

En cuanto al rol de la ICANN, hay ciertas cosas que la ICANN no es. Y esto es importante de entender, cuando hablamos de la misión de la ICANN, entender qué es la ICANN en este contexto de la seguridad y la estabilidad.

Básicamente, la ICANN no es una agencia de cumplimiento de la ley, no es un tribunal, o ninguna otra agencia gubernamental en este proceso. El cumplimiento de la ley y los gobiernos participan como partes interesadas dentro de los procesos de la ICANN y el desarrollo de políticas, pero la ICANN en sí misma, no tiene ningún rol relacionado con este tipo de responsabilidad. La ICANN no es responsable por la vigilancia de la Internet, ni de combatir el abuso operativamente. No es responsable de determinar lo que constituye una conducta ilícita en Internet. No está involucrada en el uso de Internet, en relación al ciberespionaje o las ciberguerras o

ciberconflictos, y no está autorizada para, en forma unilateral, suspender, terminar o rescindir nombres de dominio. La ICANN puede hacer cumplir su contrato con terceros, por ejemplo los registros, incluyendo los proveedores de registración de nombres de dominio.

Ahora bien, ¿qué es lo que sí hace la ICANN? Tiene un rol en el apoyo del trabajo de las agencias de cumplimiento de la ley, o agencias gubernamentales, a llevar a cabo acciones legítimas, según sea necesario. Y, obviamente, el contexto legal varía de país en país, y el marco de trabajo también depende del contexto en particular. La ICANN sí participa con la comunidad de seguridad operativa en el estudio, análisis e identificación del uso abusivo o mal uso del DNS.

La ICANN sí tiene el mismo rol, como parte interesada, en relación a los protocolos de Internet. La evolución real de los protocolos de Internet y los estándares relacionados no están dentro del ámbito de la ICANN, sino que residen en una organización que es bastante más técnica, como por ejemplo lo es el Equipo de Tareas de Ingeniería de Internet y la Junta de Arquitectura de Internet.

En cuanto a la seguridad, estabilidad y flexibilidad, y cómo cabe esto dentro de la ICANN. Hay muchos puntos a tener en cuenta: hay que pensar en la seguridad como uno de los valores claves de la ICANN. Y esto está en concordancia con la afirmación de compromisos que tiene la ICANN con el Departamento de Comercio Estados Unidos. En segundo lugar, la seguridad es una de las cuatro áreas principales dentro del plan estratégico de la ICANN. La seguridad es un tema general que afecta a toda la organización de la ICANN. Por cierto,

desde el punto de vista organizacional, existe un departamento que se encarga de la seguridad, se encarga de observar las cuestiones de seguridad dentro de la ICANN en general.

La seguridad es un elemento esencial en todos los proyectos y actividades que lleva a cabo la ICANN. En cuanto a la seguridad, hay Grupos de Partes Interesadas Comerciales dentro de la comunidad de la ICANN, y está el SSAC, o el equipo de seguridad y transparencia.

Esto es parte de la introducción, pero también tenemos que tener en cuenta por qué son importantes la seguridad y la estabilidad. Esto es algo obvio para muchos, pero si lo consideramos de manera más específica, seguramente haya algunos puntos de tener en cuenta. En primer lugar, la seguridad y estabilidad del sistema de nombres de dominio dentro de la ICANN, en general, y la seguridad y estabilidad, contribuyen a la estabilidad de todo el ambiente económico mundial. Así que, para la prosperidad de las naciones en desarrollo y desarrolladas, ayuda a las naciones a llevar a cabo sus actividades y negocios. También brinda apoyo a las diferentes agencias para la preservación de la ley y el orden, y facilita el correcto funcionamiento de la infraestructura crítica en todo el mundo, mejora las oportunidades para llevar a cabo actividades comerciales en general, y permite el libre flujo de información. Y finalmente, la seguridad y la estabilidad protegen los intereses de los usuarios finales de Internet.

Básicamente, podemos decir que es importante, desde varios puntos de vista, pero también porque afecta a los individuos en forma global y particular, en todos sus aspectos.

Ahora les voy a contar un poco sobre el SSAC, que es el Comité Asesor de Seguridad y Estabilidad. Y su mandato es el siguiente: es asesorar a la comunidad de la ICANN y la Junta Directiva de la ICANN sobre cuestiones que tienen relación con la seguridad y la integridad de los sistemas de asignación de direcciones y nombres de Internet. El SSAC se inició en el 2001, hace ya doce años que comenzó sus operaciones, en realidad, empezó a operar en 2002, y le proporciona asesoramiento a la Junta Directiva de la ICANN y a las organizaciones de apoyo y comités asesores y también al personal de la comunidad en general. En marzo de 2014, el comité contaba con aproximadamente cuarenta miembros, designados durante un término de tres años por la Junta Directiva.

El SSAC tiene una serie de actividades, que lleva a cabo en forma interna. Hay un comité de membresía del SSAC que se encarga de entrevistar a los miembros del SSAC y analizar la membresía cada tres años. En cuanto a las reuniones de la ICANN, hay muchas actividades que se llevan a cabo para poder presentar el taller de DNSSEC y también se preparan para desarrollar reuniones de difusión externa, sobre el SSAC, con respecto a las agencias de cumplimiento de la ley. En donde hablan o discuten acerca de intereses en común.

El SSAC lleva a cabo también un taller anual, en donde se reúnen y hacen una revisión estratégica para todo el año acerca de las diferentes actividades. El SSAC también cuenta con socios de trabajo o partes que contribuyen con su trabajo. Y actualmente, hay varias líneas de trabajo. Una, que considera las métricas relacionadas con el uso abusivo de los identificadores. Otra que se encarga de una lista de sufijos públicos. Hay otro grupo que está trabajando sobre la

transición de la IANA, y está brindando aportes al respecto. Y otra parte se encarga de recibir y analizar los aportes del grupo JAS.

Previamente, esto es una idea acerca de los informes que emite el SSAC, al menos, de los que ha emitido los últimos años. Hay cinco informes realizados, que tienen que ver con la seguridad del DNS, que van desde, por ejemplo, los procesos de la implementación de la llave del DNSSEC, otros que tienen que ver con el asesoramiento en relación a la mitigación de los riesgos de colisión de nombres, también un informe que responde a una carta de la Junta Directiva de la ICANN, respecto del unos estudios interdisciplinarios, solicitados por la junta de la ICANN, y también otro informe que asesora sobre los certificados de nombres de Internet, especialmente sobre los TLD.

Dentro de la categoría del abuso o mal uso del DNS, tenemos un informe que asesora sobre los ataques de denegación de servicio, y cómo esto afecta a la estructura del DNS. También hay otro informe relacionado con los nombres internacionalizados de dominio, y otro que tiene que ver con los datos de registración, en relación al WHOIS.

Ahora, lo que me gustaría hacer es hablar de algún tipo de riesgos o ataques de seguridad. Esto es algo que evoluciona constantemente y me gustaría darles un ejemplo de un ataque de seguridad. En este caso en particular, me voy a focalizar en la denegación distribuida de servicio, el DDoS, que es un ataque que intenta hacer que una máquina o red no esté disponible para los usuarios.

Esto se detalla en el SAC065, por ejemplo, y como señalé anteriormente, es un ataque que tiene como objetivo hacer que una

máquina o red, o recurso de redes, no esté disponible para los usuarios. Esto es enviado por una persona o máquina, y luego es distribuido a diferentes partes por más de una máquina o persona que coordina este ataque. Los ataques contemporáneos que están relacionados con la denegación de distribución de servicios, son ataques importantes que, según se ha reportado, exceden los 300 gigabits por segundo, tal como se ilustra en la siguiente diapositiva.

El atacante, lo que trata de hacer, es disminuir la velocidad de la red con consultas y con otras cuestiones, para poder atacar y para que la red deje de funcionar. Y muchos de esos ataques también encubren otros delitos, que tienen que ver con la falsificación o el spoofing, y que, por supuesto, afectan a la víctima. El atacante genera y trasmite paquetes de datos que suponen provenir de la dirección de IP de la víctima o de la persona que está siendo atacada. Para esto, usa diferentes protocolos de respuesta para reflejar y amplificar las respuestas para poder lograr unas tasas de transferencia de datos que excedan la capacidad de la red de la víctima. Por lo general, también hay otras personas afectadas. El DNS, teniendo en cuenta que opera sobre una base de un protocolo de preguntas y respuestas, es especialmente vulnerable a este tipo de ataques.

Ahora bien, algunos términos explicativos que quiero mencionar. Hablamos de un servidor de nombre autoritativo, básicamente se trata de un servidor de nombres que brinda respuestas a preguntas realizadas sobre nombres en una determinada zona. Si tenemos un sitio web en particular, o un nombre de dominio en particular, se envía una consulta a un servidor de nombres autoritativo y este

servidor de nombres va a responder con la dirección del nombre de dominio.

Un servidor de nombres autoritativo es, por definición, un servidor que brinda respuestas. Un servidor de nombres recursivo, un servidor de nombre en caché, es aquel que almacena los resultados de las consultas del DNS durante un periodo de tiempo. No es un servidor autoritativo, sino que lo que hace es poner a disposición nombres de dominio. En este caso, si este servidor no tiene la respuesta sobre un determinado nombre de dominio, lo que hará es enviar la consulta al servidor de nombres de dominio autoritativo. En este caso, este servidor recursivo puede ser seguro porque sólo va a responder a consultas de fuentes autorizadas en las redes. Por lo tanto, es positivo desarrollar servidores de nombres recursivos. Por ejemplo, si una organización en particular tiene un servidor de nombres recursivo, va a estar asegurada, porque solamente va a responder a las consultas que provienen de fuentes en redes autorizadas. Los servidores, en general, responder a cualquier tipo de consulta, independientemente de su naturaleza.

Estas son las diferentes cuestiones a tener en cuenta cuando hablamos de la denegación de servicios o el ataque relacionado con la denegación de servicios. En esta diapositiva, vemos un diagrama, en donde encontramos al atacante y a la víctima. A la izquierda, vemos un ejemplo en donde un atacante utiliza un servidor de DNS abierto recursivo, y el atacante, lo que está tratando de hacer, es obtener las direcciones de IP de las víctimas, falsificando información y enviando consultas a los resolutores, los servidores. Y el resolutor envía esta consulta a servidores de nombre de dominio autoritativos,

y vuelve una respuesta. Y la respuesta no va a ser correcta porque el atacante, lo que está haciendo, es simular la dirección IP de la víctima. Va a obtener la respuesta como si fuera la víctima. La mayor parte de las consultas, cuanto más consultas envía el atacante más respuestas va a obtener la víctima, y por lo tanto, la red empieza a experimentar problemas.

El segundo caso, tenemos un caso en donde el atacante está lanzando o estableciendo un BotNet. Entonces, envía consultas, y las envía muchas veces a servidores de nombres de dominio autoritativos que responden a la víctima. La víctima, básicamente, termina teniendo problemas con su red porque excede la capacidad de la red en unos treinta minutos. Luego tenemos los factores que contribuyen a los ataques. Por lo tanto, es necesario mantener la estabilidad de la red. Básicamente, muchos de los servidores no son seguros y los recursivos muchas veces no están configurados para responder consultas de los servidores autoritativos. Y también hay conexiones de Internet que tiene muy alta velocidad y cada vez son más, y que se combinan con distintos dispositivos de los usuarios finales. Y esto da como resultado, una capacidad creciente para llevar a cabo ataques de este estilo a mayor escala, utilizando una infraestructura de DNS que no es segura. Cuanto más importante o mayor es la capacidad de la Internet, también crece la probabilidad de que los atacantes causen daño en las redes.

Las recomendaciones que el SSAC propone en su informe, después de haber mirado este tema, es que la ICANN debe ayudar a facilitar un comunidad en todo Internet, con un esfuerzo para reducir la cantidad de resolutorios abiertos y de redes abiertas, que permitan que se

ataque a la red, o que haya una imitación de los dispositivos que atacan a las víctimas. Y este esfuerzo debe intentar medir con qué frecuencia ocurren estos resolutores abiertos y poder llegar a estas organizaciones para tratar de asegurarlas.

En términos simples, se habla de identificar y publicar la escala del problema y tratar de ayudar a los operadores de la red a entender por qué tienen que asegurar sus servidores de nombres recursivos y tratar de que esto se pueda ir solucionando. En segundo lugar, todos los operadores de red deben tomar medidas inmediatas para evitar la alteración de datos o el spoofing, de las direcciones web, y así verificar de donde provienen las consultas que ellos están recibiendo, y solamente responder a aquellas que provienen de máquinas autorizadas.

Esto es lo que llamamos filtrado de de ingreso de la red. Estamos hablando de operadores de servidor de DNS recursivo, que debe tomar medidas inmediatas para que estos servidores sean seguros. De nuevo, garantizar que se responda solamente a las consultas que provienen de fuentes autorizadas. Los operadores de servidores de DNS autorizados, que tienen a un nombre de servidor que debe responder a todas las consultas, deben apoyar todos los esfuerzos para investigar la limitación a respuestas autorizadas. Y hay algunos proveedores de los equipos de servidores que tienen programas que permiten una cantidad de respuestas, que se pueden transmitir con un límite, dentro de un periodo de tiempo en particular, y lo que esto genera es que, si hay un ataque de DDoS, incluso si la cantidad de consultas excede una cierta cantidad, el servidor no va a responder a

las consultas por encima de una tasa en particular, y de ese modo la capacidad de la red no se excede.

Número Cinco, los operadores del servidor de DNS deben establecer procesos operativos para asegurar que el software se actualiza regularmente y comunicarse con sus proveedores de software, para estar al día con los desarrollos y los acontecimientos más recientes. Es decir, que siempre hay nuevas amenazas, que van surgiendo. Y si no se puede lograr que el software esté actualizado, tampoco se va a poder resolver una nueva amenaza. Y lo mismo va a ocurrir con el servicio del DNS, y salvo que el software pueda ser autorizado en campo, para prevenir alguna amenaza, el ataque DDoS va ser exitoso.

Finalmente, los fabricantes o las personas que configuran los equipos de redes, que están en el lugar del cliente, ésta es la terminología que utilizamos para referirnos a las máquinas que tienen las empresas dentro de las organizaciones para mantener su propia red, y sus propios sistemas de computadoras, esos fabricantes deben tomar medidas inmediatas para asegurar esos dispositivos y también garantizar que se puedan actualizar en el campo, cuando aparezca un nuevo software que esté disponible. Y reemplazar agresivamente los equipos que estén instalados y no se puedan actualizar. Es decir, en términos coloquiales, asegurarse de que los equipos de red de cliente no respondan a las consultas no autorizadas, garantizar también que todo el equipo tenga software que se pueda actualizar y reemplazar en campo y también reemplazar los equipos que no se puedan actualizar.

Éste es el tema específico de la seguridad, obviamente, hay una gran cantidad de asuntos de seguridad que, de vez en cuando, se van a manifestar. Yo diría, para reforzar el rol de ICANN el mantenimiento de la seguridad y estabilidad del sistema de nombres no identificados. Esto va a proteger a todos los que operan Internet, no solamente a los proveedores de servicios de Internet, sino a las empresas, los gobiernos, y a todos los que tienen que llegar al usuario final. Esto completa mi presentación. Ahora, le cedo la palabra a Tijani.

TIJANI BEN JEMAA: Muchas gracias, Julie, por esta presentación. Voy a iniciar ahora la sesión de preguntas. Quiero saber si todo está claro para ustedes. Tiene una pregunta el señor Alan Greenberg.

ALAN GREENBERG: Al principio, Julie, usted dio una lista de las cosas de las cuales ICANN no es responsable. Hay algunas cosas que quizás resultan obvias, pero tendríamos que quizás referirnos a aquellos procesos que pueden tener una cierta debilidad dentro del DNS, y nosotros sí tenemos un rol ahí. Espero que usted de acuerdo con eso.

INTÉRPRETE: Los intérpretes pedimos disculpas, el audio no es bueno.

JULIE HAMMER: Creo que usted tiene razón, Alan. En realidad, sí tenemos que referirnos, por otro lado, a lo que la ICANN hace. Tenemos que corregir eso.

ALAN GREENBERG: Usted habló de las ciberguerras y de las debilidades del DNS, y en ese sentido, nosotros sí tenemos que tratar de reducir esas debilidades, si bien no somos responsables de las acciones que se hacen, en realidad. Es una aclaración que quería hacer.

TIJANI BEN JEMAA: Tiene la palabra Olivier Crépin-Leblond.

OLIVIER CRÉPIN - LEBLOND: Muchas gracias, Tijani. Tengo una pregunta.

TIJANI BEN JEMAA: Olivier, no lo escuchamos.

OLIVIER CRÉPIN - LEBLOND: ¿Se escucha mejor ahora? La pregunta es, ¿cómo hace el SSAC para resolver el tema al que se va a referir, dado que ALAC, o At-Large en general, está preocupado por la seguridad del DNS? Y la pregunta es si podría dirigirse al SSAC para que lo asesore.

JULIE HAMMER: La respuesta es sí. El SSAC va a responder a cualquier organismo dentro de la ICANN, si tienen preguntas sobre la seguridad y estabilidad, que tengan que tener en cuenta, y el SSAC va a responder a los temas específicos, a los temas en particular. Muchas de las cosas que el SSAC hace tienen que ver con asuntos a los que

responden los miembros en sí, del SSAC, que le dan prioridades en la planificación anual. Si bien a veces surgen otras cosas durante el año, que pueden afectar la prioridad. Es una combinación de los distintos temas que van surgiendo.

TIJANI BEN JEMAA: Gracias, Julie. Ahora, Carlos Raúl tiene la palabra.

CARLOS RAÚL: Julie, es una excelente presentación para la gente que no es técnica, realmente me gustó mucho. Tengo una pregunta. ¿Puede usted hablarnos de la magnitud del problema con los servidores no seguros, donde están, cuál es un número, cuánto costaría reemplazarlos, quiénes son los propietarios de esos servidores, y a quién responden en el sistema? ¿Son los registros Regionales? ¿Quién los puede convencer de que hagan esta actualización de seguridad? Gracias.

JULIE HAMMER: Muchas gracias, Carlos. Parte del problema es que no tenemos una idea muy exacta de cuántos son los servidores no seguros y eso es lo que está por detrás de la tercera recomendación que el SSAC hizo en el informe SAC065, es decir, que se establecieron algunas métricas sobre cuándo están los resolutores abiertos, y no hay mucha información sobre eso. Cuánto costaría, es algo que depende mucho de cuál es la tecnología de la que estamos hablando en un servidor en particular. Eso es una pregunta que realmente no se puede responder. La dificultad más bien está en convencer a los operadores

de DNS de que es algo a lo que ellos tienen que dedicarle esfuerzo y dinero, cuando, en cierta medida, no hay un beneficio directo para ellos. Y ciertamente, no son vulnerables a los ataques del DDoS. Eso, no necesariamente hará que ellos gastan menos dinero, pero justamente parte del problema es convencer a la gente de qué es lo mejor para el usuario, cuando en realidad tiene que salir de su propio bolsillo.

TIJANI BEN JEMAA: Muchas gracias, Julie. Tiene ahora la palabra Otunte. Adelante Otunte.

Quizás tiene su micrófono silenciado, tiene que presionar asterisco siete para poder hablar. ¿Puede hablar, señor Otunte? Si no, hasta que podamos encontrar el problema, le voy a dar la palabra ahora Alberto Soto. Alberto, adelante por favor.

ALBERTO SOTO: Gracias, Tijani. Entiendo el tema técnico y creo que el convencimiento a quienes no tienen seguridad en su DNS, no tendría que venir de la ICANN, sino de otras múltiples partes interesadas, que son los gobiernos locales, que deberían generar las leyes correspondientes para la seguridad en todos los sistemas de información, dentro de su jurisdicción. Porque la totalidad de los ataques que se han hecho, las vulnerabilidades en los sistemas de información, no fueron en los DNS, no fueron en los sistemas WHOIS, pero la gente lo cree así. Nosotros representamos a los usuarios finales y hablamos, y la gente cree la vulnerabilidad viene por

problemas de falta de regulación por parte de ICANN. Y realmente no es así. Creo que el modelo de múltiples partes interesadas debería… … luego en las otras partes interesadas para que las cumplan. Gracias.

JULIE HAMMER: Muchas gracias, Alberto. Creo que sería muy bueno que algo así suceda, pero, lamentablemente, la infraestructura no está en el control de los gobiernos, necesariamente. Y no está dentro de la jurisdicción de los gobiernos tener un impacto en todo esto. Por eso, muchos de esos ataques, como sabemos, son globales. Y lo que los gobiernos puedan legislar, puede resolver alguno de los problemas, pero no lo van a resolver totalmente. Agradezco por su comentario.

TIJANI BEN JEMAA: Muchas gracias, Julie. Otunte, ¿puede hablar usted ahora? Si no, baje la mano en el chat, así podemos entender el problema. O escriba su pregunta. La otra pregunta que tengo es si él está en el puente o si está en el Adobe Connect.

JULIE HAMMER: Tijani, Maureen nos ha dicho recientemente que hay una pregunta en el chat sobre cómo uno puede convertirse en miembro del SSAC. Yo mencioné durante una entrevista que yo soy uno de los miembros SSAC menos técnicos. Yo fui propuesta al SSAC como enlace de ALAC. Y el SSAC tiene una política en la que hay que ser aceptado por el SSAC como miembro pleno, y participar como miembro pleno. Por eso, yo tuve que atravesar un proceso de entrevistas y sé que hay

muchos enlaces que, si quieren participar en las actividades del SSAC, también lo tuvieron que hacer. El SSAC evalúa otros mecanismos a través de los cuales la personas pueden convertirse en miembros del SSAC, y, de ese modo, se le puede sugerir a otro miembro del SSAC o alguien cuyas actividades le falte como nicho al SSAC, y ellos pueden indicar que puede estar interesados en que esta persona o personas participen. El SSAC tiene una política de no ser un organismo muy grande. En este momento, hay cuarenta miembros, y eso es ya bastante grande, para el tamaño que tiene el SSAC. De hecho, es un proceso bastante restrictivo, más que el proceso para convertirse en miembro del ALAC u otras unidades constitutivas.

TIJANI BEN JEMAA: Muchas gracias, Julie. Tengo a la pregunta de Otunte que dice: en mi región hay problemas con las tarjetas de crédito, que no se permite que se utilicen en la Internet. ¿Cuál puede ser la razón? Esa es la primera pregunta. La segunda es si hay equipos o fabricantes de equipos a los cuales se les exija que se implante un chip de vigilancia en el equipo y si es que el SSAC está preocupado por esto.

JULIE HAMMER: Hay un asunto de seguridad general, en el sentido de que las tarjetas de crédito no se permiten en Internet. No sé muy bien, no estoy muy segura si él está sugiriendo que a las empresas no se les permite, o a los bancos no se les permite, pero diría que la idea es que se proteja la información para que no se robe, o para que no se use incorrectamente y hay una cantidad de problemas que pueden ocurrir. Pero no estoy muy segura de cuál es realmente la pregunta.

En cuanto a la segunda parte, estoy tratando de ver si puedo encontrar cómo está redactada, en lo que se refiere a implantar un chip de vigilancia. Éste no es un tema de DNS. El SSAC está preocupado por los temas de seguridad asociados con los nombres y las direcciones del sistema de nombres y direcciones de Internet. Y un chip de vigilancia implantado en un sistema, yo creo que, si bien es un asunto que nos debe inquietar, no creo que tenga que ser un tema de DNS como tal, y el SSAC tiene que restringirse a los asuntos que están dentro del alcance de ICANN, y que están asociados con el DNS.

TIJANI BEN JEMAA: Muchas gracias. Yo entiendo lo que usted está diciendo. Yo confirmo que estos no son asuntos de la seguridad y estabilidad de Internet. Más bien, son temas de seguridad en general, pero no tienen mucho que ver con el DNS.

Tiene ahora la palabra Olivier Crépin-Leblond.

OLIVIER CRÉPIN - LEBLOND: Muchas gracias, Tijani. Quisiera agregar algo al debate sobre la seguridad de las tarjetas de crédito. Es cierto, por supuesto, por un lado, que la confiabilidad del sistema de dominio y la confiabilidad de que se utilicen correctamente los datos, es un tema muy grande, muy importante. Por supuesto, la implementación del DNSSEC, que requiere que se pueda evitar que los hacker le den a uno un sitio incorrecto del nombre de dominio, es algo que en lo que se está trabajando. El uso incorrecto del DNS, en este sentido, ya no puede

ocurrir y tiene que haber una resolución de las transacciones en Internet, porque puede haber incluso un software que diga si el nombre de dominio es correcto o no.

INTÉRPRETE: Los intérpretes pedimos disculpas, el audio no es bueno.

OLIVIER CRÉPIN - LEBLOND: Pero sí es cierto que el SSAC no aborda directamente los asuntos de tarjetas de crédito.

JULIE HAMMER: Yo debería haber mencionado esto. Lo que usted está diciendo es un gran punto.

TIJANI BEN JEMAA: Olivier, le pedimos que trate de acercarse al micrófono, porque usted está muy lejano y nosotros apenas podemos entender lo que está diciendo.

¿Hay alguna otra pregunta? Si no hay ninguna más, le agradezco muchísimo a Julie Hammer por su presentación, y por haber respondido nuestras preguntas. Les agradezco a todos ustedes por haber asistido este seminario web.

Por favor, no se olviden de llenar el formulario de evaluación que ofrecieron junto con la invitación. Y ese formulario de evaluación nos va a servir a nosotros para mejorar el proceso, el sistema, el

programa de generación de capacidades, para que lleguemos a un punto mejor.

Muchas gracias, y hasta luego. Les agradezco a los intérpretes, al personal, y a todos los que trabajan con nosotros en este programa.

Muchas gracias, hasta luego. Esta reunión finaliza ahora. Les agradecemos por haber participado en esta reunión y recuerden desconectar sus líneas en este momento.

[FIN DE LA TRANSCRIPCIÓN]