CLAUDIA RUIZ: Buenos días, buenas tardes y buenas noches a todos. Bienvenidos a la llamada mensual de LACRALO este 18 de abril de 2022 a las 23:00 UTC. En el canal de español hoy tenemos a Augusto Ho, Alfredo López, Carlos Aguirre, Gerardo Martínez, Gilberto Lara, Hannah Frank, Harold Arcos, Laura Margolis, Rodrigo Saucedo, Sergio Salinas Porto y Vrikson Acosta. Tenemos a Claire Craig en el canal de inglés y a Sindy Obed en el canal de francés. Tenemos disculpas por parte de Sylvia Herlein Leite y Dev Anand Teelucksingh.

Por parte del personal tenemos a Silvia Vivanco y a mi persona, Claudia Ruiz, administrando la llamada del día de hoy. Los intérpretes que nos acompañan son Marina y Paula en el canal de español, Esperanza y Bettina en el canal de portugués, y Jacques y Claire en el canal de francés. También tenemos a Alberto Soto, que acaba de entrar. Antes de empezar quisiera pedirles a todos que por favor digan su nombre al tomar la palabra para los propósitos de nuestros intérpretes. Muchas gracias. Con esto le paso la llamada a usted, Augusto Ho.

AUGUSTO HO: Buenas tardes, buenas noches a todos. Dándoles primero que todo agradecimiento a todos los que se han conectado en esta reunión mensual del mes de abril. Deseándoles lo mejor para esta reunión del día de hoy. Todos bienvenidos. Le voy a pasar la palabra a Claire para que dé lectura y aprobemos la agenda del día de hoy. Adelante, Claire.

CLAIRE CRAIG: Muchas gracias, Augusto. Bienvenidos a todos a nuestra llamada de LACRALO mensual en el día de hoy. En nuestra agenda tenemos el placer de escuchar una presentación de Nicolás Antoniello, quien nos va a hablar de cómo podemos hacer que el DNS sea más resiliente y seguro. Tengan en cuenta que esta es la primera parte de un seminario web de dos partes. Esperamos que todos vayan preparando sus preguntas para Nicolás.

Luego tendremos un informe de la junta directiva de la ICANN a cargo de León Felipe Sánchez. También tenemos otro informe de los representantes de ALAC, en este caso Carlos Aguirre, y otro proyecto muy interesante que nos va a comentar Sergio Salinas Porto. Nos va a dar información actualizada sobre todo el proceso de planificación para el proceso de LAC Digital que tendremos en mayo. También tendremos la actualización regional y allí esperamos tener un informe de los representantes regionales pero también vamos a hablar un poquito sobre las elecciones para el año 2022.

Ahora quisiera preguntarles a todos ustedes si hay algún otro tema que quieran agregar en el punto nueve de nuestra agenda. De ser así, por favor, les pido que levanten la mano y nos lo hagan saber. Muy bien. No veo ninguna mano levantada. Vamos a dar por sentado que estamos todos de acuerdo con la agenda que vamos a tratar en esta reunión. Bien. Muy bien. Le devuelvo la palabra a Augusto, muchas gracias.

AUGUSTO HO: Muchas gracias, Claire. Tal como se mencionó en la agenda, hoy tenemos una interesantísima intervención, inesperada, dicho sea de paso, de parte de Nicolás Antoniello. Va a contar con aproximadamente

45 minutos. Nos va a poner al tanto de este tema de cómo pueden ser los DNS más resilientes y seguros. Vamos a darle la bienvenida entonces a Nicolás Antoniello. A partir de este momento los micrófonos son de él. Adelante. Bienvenido, Nicolás.

NICOLÁS ANTONIELLO: Muchas gracias, Augusto. Muchas gracias a todos. Primero que nada, muchas gracias por la invitación a compartir este espacio con ustedes y la oportunidad de conversar un poco sobre estos temas. La idea de la charla de hoy… Bueno, para los que no me conocen, mi nombre es Nicolás Antoniello. Me desempeño en ICANN como gerente regional para la región de Latinoamérica y el Caribe de relacionamiento técnico. La idea de hoy era mantener una charla sobre DNS en general y las extensiones o protocolos estandarizados que se fueron agregando al protocolo básico de DNS para darle en algunos casos mayor seguridad, en otros mayor resiliencia al sistema global. Eso lo vamos a ir viendo en un momento y en algunos otros casos incluso agregarle privacidad, características de privacidad a la hora de intercambiar información. Privacidad me refiero a privacidad de los datos y de las consultas de DNS realizadas por los usuarios.

Voy a compartirles… No sé si podré compartir la presentación, Claudia, e irla haciendo desde aquí o si quieres que… Ahí está. Perfecto. Muchas gracias. Ahí está. Ustedes me indican si visualizan correctamente la presentación.

CLAUDIA RUIZ: Sí, se mira bien. Gracias.

NICOLÁS ANTONIELLO: Bien, bien. La idea es esto. Es hablar un poco de cómo hacer el DNS más resiliente y seguro. En cualquier momento de la presentación, cualquier pregunta que tengan, la pueden realizar. No necesitan esperar hasta el final de la presentación. De hecho, yo creo que las presentaciones son más entretenidas si las preguntas las vamos haciendo a medida que surjan. Yo no estoy visualizando correctamente el chat. Si alguien pone alguna pregunta en el chat, Claudia o alguno de ustedes, les pediría que si me pueden interrumpir y leerla en voz alta o si alguien quiere tomar el micrófono y hacer la pregunta, perfectamente. Adelante con las preguntas que tengan o comentarios durante la presentación o al final.

Bien. Empecemos entonces. Ahí está. Esta primera parece que fuera un slide mal hecho, que me faltó hacer algo aquí porque no hay nada. Básicamente hay una pantalla de un navegador en blanco. Lo que quería representar con esto es que hoy en día en Internet lo que sucede, como ustedes saben, cuando por ejemplo queremos navegar a un sitio, queremos acceder a un sitio web, es antes que el navegador pueda descargar de los diferentes lugares, todos los componentes de la página web o del sitio al que estamos accediendo, lo que necesito saber es si la dirección IP básicamente de esos servidores desde los cuales voy a bajar todos los pedazos de información que componen esa página web.

También sabrán que en general no es un único servidor. El servidor web es un único servidor web principal pero luego hoy en día los componentes de una página web en general pueden venir hasta de 10 o 20 sitios diferentes. Hay que hacer varias consultas a varios servidores

para traerse un gráfico, para traerse un componente de autenticación, para traer texto, etc.

El hecho de visualizar una página web, un sitio web, implica no una sino varias consultas al sistema de nombres de dominio para, teniendo el nombre, que es lo que normalmente tengo, el nombre de dominio, parte de esa URL, obtener la dirección IP y poder descargar esa página. Ahí es donde entra en acción el DNS.

Esa consulta de DNS en realidad a nivel de usuario es una consulta que en principio es a ciegas. El usuario no sabe qué es lo que está sucediendo ni ve qué es lo que sucede. El terminal del usuario, el teléfono, la computadora, lo que sea, envía al servidor de nombres recursivo, que va a ser el encargado de hacer la búsqueda de esa dirección IP correspondiente al nombre que le estoy dando, va a enviar la consulta al DNS entonces al servidor que tenga configurado. Ahí se va a suceder todo el mecanismo de búsqueda de esa dirección IP y luego el servidor DNS me va a responder a mi dispositivo con la dirección IP y a partir de ahí el navegador o la aplicación que sea podrá ejecutar el resto de las acciones.

En el caso de un acceso web se accederá a ese servidor web y se descargará el contenido web para mostrar el usuario. Decíamos que eso que sucede se oculta al usuario. El usuario no ve qué es lo que sucede. De hecho, a priori podríamos decir que el usuario tampoco puede estar seguro de que esa dirección IP que está obteniendo es la correcta. Si alguien hubiera ideado y perpetuada en forma satisfactoria algún tipo de ataque que pueda lograr modificar esa respuesta, modificar esa dirección IP que mi cliente recibe, mi cliente web va a acceder a ese sitio

pensando que es el sitio original al que yo quería acceder cuando en realidad puede ser un sitio falso armado por ese atacante que pudo efectivamente falsificar esa respuesta y hacerme llegar a mí una dirección IP incorrecta. Es la dirección IP de su servidor en lugar de la dirección IP del servidor real.

Algunos elementos a considerar hoy. En general, en los sistemas a los que estamos expuestos o acostumbrados a acceder, a utilizar en Internet hoy en día, cuando tenemos servicios de correo electrónico, de calendario, servicios de contactos. Hoy en día los contactos están casi todos en línea. La agenda de mi teléfono incluso no la manejo en mi teléfono porque yo hoy o mañana cambio de teléfono, se me rompe el teléfono o tengo más de un dispositivo y quiero compartir esa agenda, entonces normalmente la agenda también está en línea. Yo voy cargando los contactos. Eso se almacena en alguna nube, en algún sitio en línea y después mis dispositivos simplemente acceden a esa información.

Servicios de bases de datos, datos de negocio, datos de nuestros clientes en el caso de las organizaciones o las empresas en que trabajamos. Datos de los funcionarios, de los empleados de las empresas. Inventarios, etc. Servidores de archivos conteniendo información financiera, conteniendo documentación interna de la organización o de la empresa, conteniendo procesos, procedimientos de la organización, etc. Sistemas de control y operaciones, como sistemas de control de equipamiento, sistemas para monitorear el equipamiento en caso de que sea una empresa por ejemplo proveedora de servicio y algún tipo de servicio, cualquier tipo de servicio. No estamos hablando de servicios relacionados directamente con Internet. Puede ser un servicio de

energía, puede ser un servicio de agua, de cualquier otra cosa. Siempre hay sistemas de monitoreo y hoy en día todos los sistemas de monitoreo de alguna u otra manera, en algún punto tienen algún punto de contacto con Internet para poder accederlos desde fuera o para poder realizar el monitoreo remoto u otras tareas.

Sistemas de provisionamiento. Mecanismos de seguridad. Mecanismos de manejo de contraseñas. Controles de acceso, etc. Sistemas de registro y auditoría. Maneja información de auditoría de seguridad para la empresa. Después muchos otros sistemas. Yo por ahí puse sentido común y más sentido común. Esto es algo que lo vamos a ir viendo a lo largo de la presentación. En Uruguay tenemos un dicho que dice que a veces el sentido común es el menos común de los sentidos. Tenemos que entrenarlo. Lo que a algunos nos puede parecer sentido común, no necesariamente puede ser tan obvio para otros. Eso requiere capacitación o requiere por lo menos formación para saber a qué me puedo enfrentar y qué opciones tengo para resolverlo o para mitigarlo en caso de que no se pueda resolver por completo.

Todos estos elementos de los que hablamos en general, todos estos elementos que están en línea, a los que yo accedo en línea, en general antes de poder acceder a ellos empiezan con una consulta DNS o involucran en algún momento una consulta al sistema de nombres de dominio.

Repasando rápidamente, el sistema de nombres de dominio es un sistema distribuido. Está distribuido en lo que refiere a cómo se almacena la información. No está la información almacenada en un único servidor en el mundo sino que está distribuida en varios lugares,

en varios servidores. Además, la administración tampoco es concentrada. Esos servidores distribuidos, tampoco hay una única organización que los administre sino que, como ustedes saben, hay toda una administración distribuida y un protocolo diseñado para que esa administración distribuida funcione.

Esas divisiones administrativas del espacio de nombres de dominio son lo que denominamos zona. Cada administrador de una zona administra una parte de todo el sistema global de DNS. También sabemos que un administrador de cualquier zona puede delegar la administración de cualquier subárbol por debajo. La arquitectura DNS es una arquitectura de árbol invertido. A partir de la raíz se van generando ramas y sucesivos árboles. Un administrador de un punto en ese árbol, de una hoja en ese árbol, puede delegar cualquier árbol que esté por debajo creando una nueva zona. Ese acto de delegar crea zonas.

Después tenemos dos tipos de servidores. Servidores autoritativos y servidores recursivos. Ahí me quedó mal la traducción. Me quedó resolvedores. Donde dice resolvedores debería decir servidores recursivos o *resolvers* en inglés. Servidores autoritativos entonces, no autorizados, y servidores recursivos.

Servidores autoritativos son, para repasar un poco, los que almacenan la información. La información de cada zona, la información de cada dominio está almacenada en los servidores autoritativos. Los servidores recursivos son los que encargados de buscar esa información en el sistema de nombres de dominio en lugar o en representación del cliente, del dispositivo cliente. No es el dispositivo el que realiza la búsqueda sino que el dispositivo le entrega la pregunta, lo que quiere buscar al

servidor recursivo, el servidor recursivo es el que realiza la búsqueda y, una vez que tiene la respuesta, le responde al cliente final.

¿Por qué estamos repasando todo esto? Esto es un ejemplo rápido, un gráfico del mecanismo de resolución del DNS. Vamos a pasarlo rápidamente. Esto lo conocemos todos. Estamos repasando todo esto porque en adelante la presentación vamos a empezar a entrar en distintos puntos de todo ese mecanismo, de todo ese sistema de DNS y ver dónde actúa, cuáles son los tipos de amenaza más comunes, dónde actúan esas amenazas y si existe o no algún mecanismo para evitar esa amenaza por completo o, si no es posible porque hay algunos tipos de amenaza que no es posible eliminarlas, si es posible mitigarlas de alguna manera, algún protocolo, algún mecanismo disponible para mitigarla en caso de que no sea posible eliminar la amenaza.

Cuando hablamos de amenaza vamos a referirnos básicamente a estos tres tipos de [*threats*] que son los tipos más comunes de amenazas. No son los únicos. Sí son los más comunes. Lo que llamamos phishing, que es la práctica fraudulenta de enviar correos electrónicos que pretenden ser de empresas o servicios conocidos o de renombre, y tratar de inducir a los usuarios, a las personas… Aquí los usuarios son las personas y el phishing apunta de alguna manera a engañar al usuario de tal forma que el usuario crea que está accediendo a algún servicio conocido o a alguna información que desea buscar cuando en realidad el verdadero objetivo es inducir al usuario a revelar información personal como contraseñas, números de tarjeta de crédito, etc., con la finalidad de luego utilizar esa información del usuario para poder hacer una extracción de información o alguna inyección de información o algún acceso no autorizado a algún sistema en el caso de las contraseñas por ejemplo acceder a la cuenta

bancaria de un usuario para cometer un delito o algo, o un fraude. Eso es el phishing.

El malware. ¿Qué es el malware? El malware ya no está destinado al usuario. El malware está destinado a los dispositivos. El malware es software que está diseñado específicamente para o bien interrumpir una funcionalidad de algún dispositivo o bien dañar el dispositivo, no solo interrumpir la funcionalidad sino dañar provisoria o permanentemente el dispositivo o no interrumpir, no dañar sino que pasando totalmente desapercibido, obtener acceso no autorizado a un sistema informático, a un dispositivo para en general extraer información.

Es decir, si yo quiero extraer información de un sitio y soy un atacante, lo que voy a querer es pasar desapercibido, que nadie se entere de lo que yo estoy haciendo. Poder infectar uno de estos software, un tipo de malware que me dé ese acceso y me permita realizar las tareas sin que los usuarios siquiera se enteren de que yo estuve ahí y obtuve esa información. Por lo menos si se enteran, que ya sea tarde, que sea después de que obtuve la información. Por ejemplo, los conocidos con el nombre de ransomware, los conocidos como killover, rootkit, los virus, los famosos virus, etc.

Luego tenemos las botnets. Las botnets también son destinadas a dispositivos, no a usuarios. El objetivo de una botnet es… Básicamente qué es una botnet. Una botnet es una red de computadoras que yo como atacante yo me armo y esas van a ser mis armas. ¿Mis armas para qué? Para cometer un ataque a un tercero más adelante. ¿Cómo armo yo ese ejército de dispositivos? Inyecto este software, en general malware, software malicioso, etc. en esos dispositivos sin que los

usuarios se enteren y de alguna manera cuando decido en un futuro cometer algún tipo de ataque como típicamente por ejemplo un ataque distribuido, lo que hago es que de alguna manera le mando una orden a todos esos dispositivos que pueden ser miles de dispositivos que yo comprometí por ahí en Internet, les mando una orden, de alguna manera despierto ese software y hago que todos esos dispositivos hagan algo en forma simultánea contra un tercero.

Por ejemplo, mandarle datos sin importar el contenido de esos datos, mandarle muchos datos a un tercero. Si son uno o dos dispositivos que envían datos a un tercero no hay problema. Ahora, si son cientos de miles de dispositivos enviando datos a un tercero, lo que va a pasar seguramente es que entre otras cosas ese tercero se le va a saturar el ancho de banda y eso se conoce como ataque de denegación de servicio porque cualquiera que sea el servicio que estaba prestando ese tercero ya no va a poder prestarlo porque no va a disponer de ancho de banda por la cantidad de datos que están llegando, por ejemplo. Hay un momento de ataques muchísimo más elaborados que parten o se basan en este tipo de botnets.

Bien. ¿Por qué hablamos de amenazas al sistema de nombres de dominio o que utilizan al sistema de nombres de dominio como mecanismo para cometer otro tipo de ataque? Porque todos usamos el sistema de nombres de dominio. Es muy atractivo para los atacantes vulnerarlo o utilizarlo para vulnerar algún otro sistema. Si yo logro interrumpir el servicio de DNS, interrumpo todas las transacciones en Internet, básicamente, porque dijimos que todo en general comienza con una búsqueda de una dirección IP. Ninguno de nosotros nos acordamos en general de las direcciones IP de los sitios. Nos acordamos

de los nombres. Si no tengo la forma de traducirlo, si no funciona el DNS, estoy interrumpiendo transacciones comerciales, accesos web, correos electrónicos, toda la actividad en Internet o por lo menos de la región donde el DNS no sea accesible.

Servicios gubernamentales y no gubernamentales, redes sociales, educación. Hoy en día todo pasa o gran parte de nuestras vidas pasa en cierta forma por Internet. Una interrupción ahí puede ser más o menos problemática o hasta catastrófica en algunos casos. Si estamos hablando de sistemas de salud, etc. puede ser bastante catastrófico, o de energía o de agua potable o de algún otro sistema de soporte de vida.

También explotando el DNS se puede engañar y se pueden cometer fraudes contra los usuarios. Puedo robar credenciales para acceder a sitios bancarios, etc. Algunos de los vectores de ataque que podemos mencionar más utilizados o más conocidos o más vistos son registro de nombres de dominio en forma maliciosa. Por ejemplo, esto pasó mucho durante la pandemia. Se registraban en el sistema de nombres de dominio sitios pretendiendo tener información sobre las vacunas contra el COVID y la gente accedía ahí y en realidad la gente accedía realmente a información pero también estaba accediendo sin saberlo por ejemplo a una descarga. Yo descargo el archivo pero descargo el archivo ese y ese archivo además contiene un virus o un malware o algún software para una botnet. Yo sí accedo a la información pero sin darme cuenta también estoy inyectando o metiendo en mi dispositivo un software malicioso.

Secuestro de servicios de registro de resoluciones de nombres. Esto es un ataque a los registradores de nombres de dominio digamos.

Alteración de datos del DNS. Lograr acceso a servidores autoritativos y modificar la información. Recolectar datos mediante sitios comprometidos. Comprometer cualquier tipo de sitio con la finalidad de recolectar datos sobre usuarios y también extracción de datos. Es un ataque un poco más complejo. No vamos a entrar en detalle ahora. En próximas presentaciones entraremos en detalle sobre los ataques, cómo son y cómo funcionan.

Este es un tipo de ataque que aprovecha el hecho de que el DNS utilice un puerto conocido, que es el puerto 53 para transferir la información y utiliza ese mismo canal como mecanismo para extraer datos de las organizaciones, porque las organizaciones que tienen que dejar, que tienen que mantener en general ese canal, ese puerto abierto, porque es el puerto de acceso al DNS, entonces si lo cierran no pueden resolver el DNS y los atacantes pueden llegar a aprovecharse de esa funcionalidad de DNS para usar eso para extraer información y pasar los firewalls y las medidas de seguridad que las organizaciones tengan implementadas.

Este slide aquí lo que presenta es un pantallazo general de lo que sería todo el ecosistema de DNS global, incluyendo los registradores, los registros, los usuarios aquí donde dice stub. Este stub es el software de DNS que corre el cliente DNS de mi dispositivo. Digamos que le envía la consulta al servidor recursivo. Este servidor recursivo es el que busca la respuesta entre los servidores autoritativos y luego se la envía al cliente y luego tenemos los registros, los registradores y todo el resto del ecosistema de DNS.

Aquí las cruces rojas digamos muestran un montón de puntos donde es factible que un atacante cometa, valga la redundancia, algún tipo de

ataque. Estos son los puntos donde es posible que un atacante cometa sus ataques. Lo que vamos a ir viendo ahora son algunos mecanismos que se agregan, que se fueron agregando al DNS por medio de los protocolos estandarizados que lo que hacen es que funcionan en algunos de estos puntos y o bien evitan posibles ataques o bien mitigan posibles ataques en los casos en que esos ataques no se puedan resolver.

La realidad, la cruda realidad, como dice aquí, es que esto es una carrera que nunca termina. Los atacantes siempre están motivados para encontrar nuevas vulnerabilidades y siempre van a aparecer nuevas vulnerabilidades porque el software lo escriben las personas y las personas cometen errores. Cuanto más complejo es el software, más probable es que tenga errores y prácticamente no existe software más o menos complejo que no tenga absolutamente ningún error. Las vulnerabilidades aparecen, se corrigen, pero hay un tiempo entre cuando aparece la vulnerabilidad y se corrige la vulnerabilidad que queda una ventanita abierta para que los atacantes puedan aprovecharse de eso.

Los ataques son cada vez más creativos y en ocasiones muy, muy sofisticados. No existe eso del caballo del comisario en esto de la ciberseguridad. Los atacantes siempre van un paso adelante. En general, lo que podemos hacer son dos cosas. Una es prevenir y tener todos estos sistemas de los que vamos a hablar funcionando en la medida de lo posible y la otra es reaccionar. Frente al ataque, una vez que yo detecté una intrusión o un tipo de ataque, tratar de resolverlo o mitigarlo si no es posible. Debería aprender de eso e investigar si existe algún mecanismo que pueda poner en práctica que no lo haya tenido

implementado antes para prevenir que eso vuelva a suceder. Algún mecanismo de ataque siempre está a la vuelta de la esquina, algún mecanismo nuevo. Siempre van a aparecer nuevos vectores de ataque y nuevos tipos de ataque.

Algunos mecanismos entonces de resolución o mitigación a considerar, aplicar o desplegar. El primero del que vamos a hablar tiene que ver con el sistema global de nombres de dominio y es mantener múltiples servidores autoritativos. ¿Qué es esto? ¿Qué es mantener múltiples servidores autoritativos? Supónganse que yo tengo la autoridad para un determinado dominio. Tengo el dominio nicolas.com. No tengo el dominio de nicolas.com pero si lo tuviera, imaginemos que yo tengo el dominio nicolas.com e instalo un servidor DNS para mi dominio y tengo ahí el archivo de zona de nicolas.com con toda la información de mis subdominios por debajo de nicolas.com y creo dominios laboratorios.nicolas.com, documentos.nicolas.com. www.nicolas.com para poner mi página web, etc.

Yo mantengo la zona nicolas.com. Esa zona puede estar almacenada en un único servidor. Puedo tener toda la información en un servidor autoritativo. Listo. Sería lo más fácil. Lo más simple. El caso más simple. O lo que puedo hacer es lo que se está proponiendo aquí, que es, en vez de tener toda la información en un único servidor, tener varios servidores autoritativos, todos idénticos. Todos van a tener exactamente la misma información. Todos van a tener toda la información para la zona mía, para esa zona nicolas.com.

¿Cuál es la ventaja que tiene eso? A la hora de un servidor recursivo, cualquier servidor recursivo en el mundo tratando de resolver la

dirección IP de alguno de mis dominios dentro de alguno de los subdominios de nicolas.com van a poder preguntarle a cualquiera de esas copias que yo mantengo del servidor autoritativo. ¿Por qué le van a poder preguntar a cualquiera? Porque todos tienen la misma información.

Lo que yo tengo ahí es, en vez de tener toda la información en un único servidor, tengo varios servidores con la información replicada. Eso es lo que se llama replicación de una zona. Eso por suerte existe desde el principio prácticamente de la estandarización del DNS como un mecanismo que todos, cualquier servidor que elijan ustedes, cualquier aplicación que funcione como servidor de DNS, la aplicación que sea que utilicen PowerDNS, Bind, montón de esas aplicaciones para servidores autoritativos DNS, todos la implementan. Ya está implementado. Está prevista la replicación de zona y el protocolo DNS lo soporta. Eso es relativamente fácil crear varios servidores y después activar esta característica del protocolo para que se mantengan todos con la misma información. Yo ejecuto todos los cambios, todas las modificaciones en la zona en un solo servidor y el resto simplemente se van a mantener sincronizados y van a mantener una copia actualizada todos iguales al servidor que yo definí como el servidor principal.

¿Qué ventajas tiene mantener múltiples servidores autoritativos? Frente a un ataque a un servidor no me quedo… Mete un ataque en un servidor, no me quedo sin servicio porque tengo otros servidores que están prestando también el servicio. Tengo muchísimas consultas o alguien decide cometer un ataque que conste de enviar muchísimas consultas a mi servidor, como yo tengo varios servidores que pueden responder, yo lo que puedo hacer es repartir la carga entre todos esos

servidores. Ahora tengo más servidores capaces de responder. Tengo más capacidad de respuesta. Tengo más capacidad de mitigar por ejemplo una cantidad muy grande de consultas.

De alguna manera estoy haciendo el sistema más resiliente. Existe una técnica que se denomina técnica de Anycast que también se puede aplicar. Lo quiero mencionar justo enseguida después de esto de mantener múltiples servidores autoritativos. ¿Por qué? Porque para mantener múltiples servidores autoritativos básicamente puede haber alguna otra opción pero lo más común es implementarlo de una de estas dos formas que voy a mencionar.

La primera forma de tener varios servidores autoritativos con la misma información, respondiendo por la misma zona es… Ustedes saben que cuando se delega un dominio a un subdominio, cuando se delega un dominio lo que se hace es en el padre, para crear el dominio hijo, en el padre se ingresa un registro DNS, que básicamente dice cuál es el nombre de los servidores autoritativos para ese dominio que estoy delegando, que estoy creando.

Yo puedo poner varios nombres de servidores. Cuando un servidor recursivo está buscando esa información y me pregunte a mí cuál es el servidor autoritativo para esto yo le puedo dar un nombre solo, si tengo uno solo registrado, o le puedo dar una lista de nombres de n nombres, tantos como yo quiera definir. El servidor recursivo va a tratar de contactar a uno de esos. Todos van a tener la misma información porque todos van a ser autoritativos del mismo dominio, todos van a ser copias de lo mismo. Si el servidor recursivo le pregunta a uno y ese no responde, le va a tratar de preguntar al siguiente y así sucesivamente.

Puedo definir una lista con diferentes nombres, cada uno con una dirección IP distinta de servidores que son copias de un mismo servidor. Eso es una forma.

La otra forma es usar la técnica de Anycast. La diferencia es que la técnica de Anycast… ¿Qué es la técnica de Anycast? La técnica de Anycast se define como una combinación de direccionamiento IP y de enrutamiento donde la decisión de a qué destino llega el paquete la toma la red, la toman los mecanismos, los mecanismos de enrutamiento de una red.

Básicamente, Anycast no requiere ninguna configuración especial a nivel de aplicación y a nivel de cliente ni nada. Lo único que requiere Anycast es que yo le asigne la misma dirección IP a más de un servidor. Yo voy a tener dos dispositivos, en este caso dos servidores DNS, autoritativos, ya no con dos direcciones IP distintas, con nombres distintos. No, los dos van a tener exactamente la misma dirección IP. Y ustedes dirán: ¿Pero cómo? ¿Tengo la misma dirección IP en dos servidores? ¿Cuando quiero acceder cómo sé a cuál de los dos estoy accediendo? No importa a cuál de los dos estoy accediendo porque justamente todos son copias de lo mismo. Todos mantienen la misma información. No importa a cuál estoy accediendo, todos o cualquiera es capaz de responder la misma información. Es un caso en el que yo puedo asignarle la misma dirección IP a dos servidores distintos porque los dos servidores tienen la misma información. Si los dos servidores tienen distinta información y yo les asigno la misma dirección IP, ahí sí hay un problema pero en este caso no. Anycast se aprovecha de eso. Es justamente eso.

Yo agarro varios servidores autoritativos, todos con la misma dirección IP y cuando [inaudible] una consulta a un cliente a esa dirección IP, a ese servidor autoritativo, la red, Internet, y el enrutamiento se va a encargar de decidir a cuál de esos va a llegarle la consulta y ese va a responder. Estoy implementando el mismo mecanismo de dos formas diferentes.

¿Cuáles son las ventajas o los beneficios de Anycast? Proporciona redundancia y resiliencia a la infraestructura de DNS global. Distribuye la carga de consultas igual que lo veíamos para la otra forma de mantener varios servidores en copia. Distribuye la carga de las consultas y respuestas en muchos servidores. Reduce la latencia porque yo puedo ubicar esas copias más cerca de los clientes. Puedo distribuir las copias en todo el mundo. Todas con la misma dirección IP distribuidas en todo el mundo y poner las copias más cerca de los clientes. El tiempo de ida y vuelta de la consulta y la respuesta va a ser menor porque el servidor de DNS está más cerca del cliente. Reduzco la latencia y hago que la resolución de nombres sea más rápida.

En definitiva, estoy proporcionando más solidez al sistema de nombres de dominio. Lo hago más resiliente y colaboro o ayudo a mitigar eventos como ataques distribuidos o ataques de denegación de servicio a la infraestructura de DNS en este caso. Esta técnica de Anycast se puede aplicar tanto para servidores autoritativos como para servidores recursivos. Yo puedo tener varios servidores recursivos y utilizar la misma técnica de Anycast. No vamos a entrar en los detalles técnicos de la implementación. Sería toda una charla aparte. Implica conocimiento de enrutamiento, etc. Lo podríamos ver más adelante.

En caso de aplicarlo a servidores autoritativos siempre hay que tener en cuanto eso, que todos deben mantener la mismo información. Todos tienen que tener exactamente la misma información pero lo bueno es que el protocolo DNS ya lo prevé y ya hay un mecanismo para mantener una copia de una zona en un número indefinido o arbitrario de servidores. Eso es parte del protocolo DNS, ya está implementado.

Copia de servidores raíz. Esta es otra forma de dar resiliencia al sistema de nombres de dominio. Tiene que ver no con todo el sistema de nombres de dominio global sino con la raíz del sistema de nombres de dominio. Ustedes saben que la raíz del DNS es donde comienza todo el árbol de DNS. La raíz del DNS, si se quiere, haciendo una simplificación extrema, el dueño de la información, el que maneja o administra la información que está contenida en la raíz de DNS es ICANN, IANA, como oficina descentralizada de ICANN, pero no es ICANN el que lo sirve al público. No es ICANN el que mantiene los servidores autoritativos que contiene esa información. ICANN administra y gestiona esa información pero no la sirve.

¿Quién la sirve? La sirven las organizaciones que mantienen servidores autoritativos para la zona raíz. ¿Cuántas organizaciones [inaudible] hoy en día que mantienen servidores autoritativos para la zona raíz? 12 organizaciones que son estas que están listadas aquí. Aquí hay 13 pero fíjense que al que se le asignó a la letra A y al que se le asignó la letra J son la misma organización, que es VeriSign. Por eso, si bien aquí hay 13 letras, son 12 organizaciones. Estas 12 organizaciones cada una administra un servidor autoritativo para la zona raíz.

¿Qué quiere decir eso? ¿Eso quiere decir que hay solamente 12 servidores para la zona raíz? No. Para la zona raíz tenemos miles de servidores o cientos de servidores. ¿Por qué? Porque cada una de estas organizaciones utilizando la técnica de Anycast de la que habíamos hablado le asignan la misma dirección IP a muchos servidores y así crean muchas copias. Cada uno mantiene muchas copias de su servidor raíz. Este es un sitio al que pueden acceder, que es sitio: rootservers.org, que mantiene una especie de mapa y fotos actualizadas de la cantidad de copias de servidores raíz que hay en todo el mundo. Esta es más o menos la distribución actual. Esta foto la saqué hoy. Según este sitio que es correcto y acertado el valor, según este sitio hoy en día hay 1.533 instancias o copias de servidores autoritativos de la zona raíz. Estas 1.533 copias de la zona raíz que dice aquí son algunas administradas por algunos de esas 12 entidades y están más o menos distribuidas así. Por aquí aparecen en nuestra región. Hay 29 por aquí en la parte norte y esto abarca también parte del sur del Caribe. Unas 29 instancias, unas 29 copias de los servidores raíz. Como 110 copias en América más hacia el sur. De estas 266 que aparecen en Estados Unidos también hay unas cuantas que corresponden a la región norte del Caribe.

Como ven, hay varias decenas o cientos de copias en nuestra región de Latinoamérica y el Caribe de servidores raíz. ¿De qué servidores? De varios de estos servidores que mantienen estas organizaciones. De esta manera yo para la raíz de DNS que es donde empieza siempre la búsqueda en el árbol de DNS para la organización de DNS mantengo muchísimas copias del servidor autoritativo. Alguien, un servidor recursivo, cuando inicia su búsqueda y tiene que ir a preguntarle a la raíz

primero, puede acceder a cualquiera de estas copias y obtener la información.

Al tener muchas copias y tenerlas cerca de los clientes, lo que hago es de nuevo lo mismo. Más resiliencia, menos latencia, más tolerancia a errores, más capacidad de mitigar y de contener este ataque y, en definitiva, mejor esta calidad de servicio percibida por el usuario a la hora de resolver los nombres de dominio. Todos estos programas que existen a través de ICANN y de otras organizaciones que son los que gestionan, las que administran, mantienen los servidores para la zona raíz, uno puede aplicar a mantener o instalar una copia de alguno de esos servidores raíz cerca de sus usuarios, en su país o en su región, etc. Esa es una forma también de aumentar la resiliencia y la seguridad del sistema global de DNS aumentándola para la raíz en este caso. Seguridad. No sé si hay alguna pregunta hasta ahora. ¿Estoy yendo muy rápido? ¿Estamos bien? ¿Estamos bien con el tiempo?

SILVIA VIVANCO: Sí. Estamos bien. No veo ninguna pregunta. Solamente un comentario. Te lo puedo pasar por privado para lo que leas.

NICOLÁS ANTONIELLO: Perfecto, perfecto. Bien. Seguimos entonces. DNSSEC. Esta es otra de las características, de lo que se llaman extensiones de seguridad de DNS, diseñadas para eso, para, en este caso, incrementar la seguridad del sistema de nombres de dominio. Por eso puse aquí seguridad, DNSSEC.

Rápidamente, se acuerdan de ese pantallazo general de cómo era el ecosistema global de DNS. ¿Dónde actúa DNSSEC? En todo este

ecosistema, dónde actúa y qué aporta. ¿Dónde actúa? Entre el servidor recursivo y el servidor autoritativo. Recuerden, recordemos, este es el cliente, envía la consulta al servidor recursivo, el servidor recursivo busca la respuesta entre varios servidores autoritativos, preguntándoles a los servidores autoritativos empezando siempre por la raíz y una vez que obtiene la respuesta le manda la respuesta al cliente. Ese diálogo entre el servidor recursivo y el servidor autoritativo es el que se puede asegurar utilizando o desplegando el protocolo DNSSEC.

¿Quién tiene que desplegar el protocolo DNSSEC? ¿Quiénes son los participantes que tienen que aportar desplegando el protocolo DNSSEC? Son los que manejan servidores recursivos y los que administran servidores autoritativos. Aquí el cliente no juega. Es entre los servidores recursivos y autoritativos. DNSSEC les compete a los administradores de servidores recursivos y a los administradores de servidores autoritativos.

¿Qué hace DNSSEC? DNSSEC utiliza criptografía de clave pública, hablaremos en otra ocasión bien de qué es eso, pero es un tipo de criptografía, de mecanismo para encriptar datos y firmas digitales con la finalidad de proporcionar dos cosas, autenticación de origen. Esto es cuando yo hago una consulta, yo soy el recursivo y le hago una pregunta a un servidor autoritativo y obtengo una respuesta de ese servidor autoritativo, la autenticación de origen me permite estar seguro de que la respuesta que yo obtuve, que vino por Internet, digamos, hablando mal y rápido, vino realmente del servidor que tiene la autoridad para dar esa respuesta y no de un servidor de un DNS o de un atacante o de una procedencia fraudulenta. Me permite asegurarme de que la información procede de quien realmente tiene la autoridad para dar esa información y no de otro lado.

Lo otro que provee DNSSEC, además de autenticación de origen es integridad de los datos. Esto me asegura que los datos, mientras viajaban del servidor autoritativo al servidor recursivo no fueron modificados. ¿Impide que los datos sean modificados? No. Lo que permite es que si los datos fueron modificados y yo tengo implementado DNSSEC me voy a enterar. Recibo los datos y puedo verificar si esos datos fueron alterados o no. Tengo autenticación de origen, sé si los datos fueron alterados o no, puedo estar seguro. Si no fueron alterados y la autenticación de origen verifica, puedo estar seguro de que la información es la correcta y no es información falsa, que no es menor.

¿Por qué? Si estoy accediendo a mi banco y pongo www.mibanco.com, resuelvo el DNS, me llega la dirección IP de mi banco, no tiene implementado DNSSEC, acceso a mi banco y no sé si estoy accediendo al sitio correcto o a un sitio fraudulento y nunca lo voy a ser como cliente. No tengo forma de saberlo porque si lograron acceder y modificar la información de dirección IP en el servidor autoritativo no tengo forma de enterarme, entonces el atacante me arma una página que se ve idéntica a la de mi banco y listo. Cuando yo pongo el usuario y la contraseña, clic, chao. Obtienen mi usuario y la contraseña para la cuenta de mi banco.

Si tiene desplegado DNSSEC, cuando yo le envío la consulta al servidor recursivo y el servidor recursivo recibe las respuestas de los servidores autoritativos, si esa información fue falsificada, el servidor recursivo se va a poder dar cuenta de eso y no le va a dar la dirección IP al cliente. Le va a dar un mensaje de error y el cliente va a decir: “Okey, no puedo acceder a la página del banco. ¿Qué estará pasando? ¿Se habrá caído la página del banco?” No. Lo que está pasando es que el servidor recursivo

se dio cuenta de que alguien había manipulado esa información, que estaba [inaudible] información falsa y no me la da para que yo no acceda a un sitio fraudulento. El protocolo DNSSEC evita ese tipo de ataque. Ofrece protección contra la falsificación de datos de DNS y evita un tipo de ataque particular que es el ataque de envenenamiento de caché, del que hablaremos en alguna otra oportunidad.

¿Qué no hace DNSSEC? DNSSEC no provee confidencialidad en el intercambio de datos. Los datos viajan y no están encriptados los datos. Si alguien captura los datos puede ver la consulta que yo hago, puede ver la respuesta. No provee confidencialidad y tampoco evita ataques de denegación de servicio. Lo que provee es protección contra la falsificación de datos. Poder estar seguros de si los datos fueron manipulados o no. No encripta datos y tampoco provee defensa contra un ataque de denegación de servicio.

Beneficios técnicos de DNSSEC. Proporciona autenticación y validación de origen, que ya dijimos lo que era. Garantiza la integridad y no manipulación de los datos de DNS, y proporciona también un mecanismo, en el que no vamos a entrar en detalle ahora, pero también DNSSEC proporciona un mecanismo para indicarle al cliente qué pasa si yo hago una consulta [inaudible] dominio pero que en realidad ese dominio no existe. Supongamos que yo quiero entrar a la página www.nicolas.com pero esa página no existe porque no existe ese sitio en realidad. Yo tengo una respuesta. ¿Cómo puedo estar seguro de si esa respuesta que yo tengo es que en realidad el sitio no existe o es que alguien falsificó la información para hacerme creer a mí que no existe ese sitio y que yo no pueda acceder?

DNSSEC dispone de un mecanismo para que el servidor autoritativo de ese dominio que no existe le pueda decir al servidor recursivo: “Mira, ese dominio que estás consultando no existe. Yo te firmo que eso no existe”, entonces el cliente puede estar seguro de que si te digo que no existe, es que no existe. No es que esté a propósito siendo atacado o me estén haciendo creer que no existe. Me permite estar seguro de que un sitio no existe básicamente. Esos son los beneficios técnicos.

Los beneficios o el impacto en los diferentes miembros del ecosistema, en referencia al usuario final, agrega confianza de cara al usuario de llegar al sitio web deseado y correcto como complemento por ejemplo de HTTPS o de algunos otros protocolos. Desde el punto de vista del registrante, mitigación de fraude, mayor protección de marcas, reputación de código de país, los ccTLD, etc. Desde el punto de vista del registrador, cumple con los estándares de la industria y satisface las demandas de los registrantes para tener mayor seguridad y eso es parte de atraer y retener a los clientes, a los registrantes, concentrándome en seguridad y reputación, que es todo en esto del DNS. De cara a los registros que cumplen y aplican las mejores prácticas de la industria y las demandas de los registradores para mayor seguridad a la hora de registrar dominios.

SILVIA VIVANCO: Nicolás, me disculpas la interrupción. Ahora sí, ya estamos sobre el tiempo. Quisiera si me permites leer un par de preguntas que tienes de Alejandro Pisanty para ya ir terminando, porque queda solamente ahora sí solo queda media hora para la llamada y hay otros temas en la agenda.

NICOLÁS ANTONIELLO: Esto lo dejamos para la segunda parte de la presentación. El PowerPoint ahora es completo. Tienen toda la información pero lo que sigue de aquí en adelante que son otros mecanismos los vemos en esa segunda edición. Sí, adelante, Alejandro.

SILVIA VIVANCO: Fantástico, fantástico, Nicolás. Va a haber un seguimiento a tu presentación que es superinteresante y llena de contenido. Voy a leer las preguntas, que las ha puesto en el chat. La primera es DNSSEC tenía un efecto secundario no deseable. Facilitar la publicación de zonas enteras. ¿Cómo se está mitigando en la actualidad? Segunda pregunta. ¿De qué tamaño en adelante es costeable para un administrador implementar DNSSEC por sus costos y complejidad? Gracias. Nicolás, excelente presentación. De Alejandro Pisanty.

NICOLÁS ANTONIELLO: Muchas gracias, Silvia. Gracias, Alejandro, por la pregunta. Al respecto de la primera pregunta, déjame buscarlas aquí, así las tengo presentes, sobre el tema del efecto secundario no deseable de DNSSEC que facilitaría la publicación o recorrer completamente una zona. Si entiendo bien tu pregunta, Alejandro, y para explicar un poco al resto en qué consiste esto. Es cierto que con este mecanismo de que DNSSEC [inaudible] inicialmente a través del cual yo puedo estar seguro de que un sitio no existe. El último que les comentaba, que yo puedo estar seguro de que algo que yo consulté en realidad no existe y no es que alguien me esté haciendo creer que no existe. Las primeras

implementaciones, es un protocolo en particular, se llama NSEC, y ese protocolo o esa parte del protocolo, las primeras implementaciones es cierto que permitían que un atacante digamos, no era tan fácil pero con cierto grado de facilidad, haciendo consultas sistemáticamente podía hacer lo que se llama recorrer una zona y de alguna manera averiguar de una determinada zona cuáles existen y qué dominios no.

Por ejemplo, la más fácil sería hacer lo que llaman un ataque adicional. Empezar a generar palabras de diccionario. Son palabras que tengan sentido para los seres humanos en forma pseudoaleatoria y empezar a hacer consultas con esas palabras para ver si existen dominios asociados a esas palabras. Se empieza a preguntar a un servidor por un dominio, por otro, por otro, por otro, por otro. Cuando existe, voy a tener una respuesta positiva. Cuando no existe, voy a tener también una respuesta que me dice: “No existe”. Lo puedo ir recorriendo y así armarme una copia de la zona sin necesidad de ganar acceso al servidor para copiarme todo.

En realidad existe una siguiente versión de ese protocolo NSEC que se llama NSEC3 que justamente lo que hace es modificar la forma en que el DNS responde cuando no hay una zona y de alguna manera reduce enormemente, hace prácticamente imposible hacer ese recorrido de zona y obtener esa información. Eso también depende de si quien implementa DNSSEC implementa NSEC o implementa NSEC3, si está implementando la primera versión o la segunda versión de eso.

De nuevo, eso aplica solamente para obtener toda la información de una zona. Los autoritativos, por definición, las zonas son públicas. A veces nosotros somos extremadamente cuidadosos. Mejor dicho, los registros,

quienes administran servidores autoritativos son muy cuidadosos de no revelar todo su archivo de zona. Ahora, el archivo de zona es público. Por definición, porque si no es público, no sirve, no funciona, no cumple su propósito. Tiene que poder responderle a cualquiera que le haga la consulta, suponiendo que estemos hablando de un DNS público.

El hecho de obtener toda una zona tampoco implica si necesariamente sí o sí que eso sea un problema de seguridad. Puede ser un problema porque de alguna manera estoy obteniendo la lista de clientes de un determinado registro y eso es claramente un problema de seguridad para un registro pero no es un problema de seguridad a priori ni para el usuario ni para el sistema de nombres de dominio. Sí es una preocupación válida, totalmente válida, de los registros y de los registradores pero no es un problema de seguridad. De última no es un problema de seguridad tan grande y de hecho hay archivos de zona que son públicos. Por ejemplo, la zona raíz es pública. No necesito hacer un ataque porque la zona raíz la puede descargar cualquiera. Cualquiera puede descargar la zona entera. Hay algunos otros archivos de zona que también son públicos.

Ya yendo más abajo en la jerarquía, no necesariamente las zonas son públicas. Es parte del negocio de los registradores y de los registros. Mi respuesta es que sí, NSEC3 de alguna manera resuelve o busca resolver y mitigar ese problema al grado de que lo hace tan difícil que prácticamente lo estaría resolviendo.

La segunda pregunta. De qué tamaño es costeable para un administrador implementar DNSSEC por sus costos y complejidad. Ahí está. Esa es una excelente pregunta, Alejandro. Dijimos que DNSSEC hay

que aplicarlo en dos sitios. En los recursivos y en los autoritativos. Si solo lo implemento en el recursivo, no sirve. Es parcialmente útil. Si solo lo implemento en el autoritativo, tampoco, porque si el recursivo no tiene capacidad de validarlo, que yo le mande la firma de lo que digo no sirve para nada si no lo puedo verificar. Entonces hay que implementar desde los dos lados.

Implementar DNSSEC a nivel de un recursivo prácticamente no tiene sobrecarga técnica. Para los grupos de operaciones que operan servidores DNS recursivos hoy en día para empezar si instalo un servidor recursivo, cualquier software de servidor recursivo que yo instale de los 10 más conocidos, por decir algo, ya viene por defecto con DNSSEC habilitado. Tengo que a propósito tirar un comando para deshabilitarlo. Eso ya da una pauta de la complejidad que agrega. Por defecto viene activado. Ya viene con el paquete. Lo tengo que desactivar.

Para quienes hace años que mantienen un servidor DNS capaz que lo tienen desactivado. Activarlo no debería representarle ni carga operativa ni tampoco sobrecargar los servidores a nivel de que necesito aumentar la memoria o el procesador de los servidores. No. La sobrecarga de un servidor recursivo por implementar DNSSEC es despreciable frente a la sobrecarga que vas a tener si incrementas la cantidad de clientes, por ejemplo. En general, uno crece con los clientes y DNSSEC crece solo. No debería representar un problema. ¿Esto quiere decir que no hay que monitorearlo? No. Siempre hay que monitorearlo. Ningún protocolo es implementarlo y dejarlo andando solo y olvidarse. Sí hay que monitorearlo pero en general no tiene implicancias operativas.

Del lado del autoritativo, ahí sí tiene una complejidad un poco más grande porque hay que mantener firmas, hay que mantener claves privadas, hay que tener mecanismos de almacenamiento que pueden ser más o menos costosos, más o menos complejos dependiendo de lo que estoy asegurando, de la crediticidad que tenga mantener esa clave privada secreta, de qué tan a menudo tengo nuevos dominios en mi zona y los firmo.

Por ejemplo, si soy administrador de un ccTLD, de un código de país, todos los días puedo tener decenas o cientos de nuevos dominios y tengo que firmarlos en el momento en que se crean porque si no, no tienen DNSSEC habilitado. Tengo que tener un mecanismo online y automatizado de que cuando un cliente nuevo cree un nuevo dominio, automáticamente se genera la firma, etc.

Eso no es imposible, no es muy difícil. Hoy en día hay mucha ayuda para hacerlo. Hay mucha experiencia de otros que hacen lo mismo que nosotros, de otros ccTLD que hace años que lo implementan y hay mucha oferta de capacitación muy accesible para todos y de hecho aprovechando tu pregunta, Alejandro, nosotros en ICANN, una de las cosas que hacemos es invitar a cualquier operador a contactarnos y nos ofrecemos a acompañarlos en todo el proceso de despliegue de DNSSEC, ya sea a nivel de recursivo como de autoritativo. Hay operadores que, por ejemplo, prefieren hacerlo en forma privada. Los acompañamos en forma privada. No les vamos a decir ni lo que tienen que hacer ni qué tienen que comprar ni cómo lo tienen que hacer pero sí lo vamos a asesorar y capacitar para que puedan recorrer ese camino de una forma razonablemente eficiente.

Del lado de los autoritativos implica un poco más de costos. En general, de capacitación y operativos, no tanto de hardware. Yo creo que si tuviera que decir sobre DNSSEC, DNSSEC es algo que debería ser sí o sí implementado por todos. Es algo muy, muy necesario. El problema que resuelve es un problema muy grande y es un problema que si no se resuelve para un usuario es imperceptible.

SILVIA VIVANCO: Nicolás, me perdonan. Realmente excelente presentación. Sé que veo manos levantadas de Carlos y de Sergio pero revisando la agenda necesitamos avanzar. Te comprometemos, Nicolás, para que nos visites en una siguiente oportunidad, inclusive dos o tres oportunidades, para poder continuar con esta discusión. Me perdonan, Carlos y Sergio, que vamos a seguir con la agenda. Tal vez, Sergio, Carlos, si tienen una pregunta respecto a esta presentación, por favor, envíennos, me pueden enviar a mí, a At-Large staff, las preguntas por escrito y se las hacemos llegar a Nicolás.

NICOLÁS ANTONIELLO: Sin duda. Muchas gracias por la invitación. Yo respondo las preguntas si me las mandan y también me comprometo a anotarlas y comentarlas al principio de la próxima sesión. Muchas gracias a todos. Muchas gracias por la invitación.

SILVIA VIVANCO: Muy agradecidos, Nicolás. Perdónenme, todos los que levantaron la mano, por favor. Adelante entonces con la agenda, Augusto.

AUGUSTO HO: Muchas gracias, Silvia. Agradecer a Nicolás por su participación. Comprometido desde ya a darle continuidad al tema, que ha sido, por lo que he visto, muy cargado y con muchas preguntas que también se van a ir desarrollando. Siguiendo con la agenda de hoy nosotros tenemos aquí la participación de don León Felipe Sánchez para que nos dé un reporte del Board de ICANN. León, por favor, los micrófonos son tuyos.

LEÓN SÁNCHEZ: Muchas gracias, Augusto. Buenas tardes, buenas noches a todos y a todas. Ha habido bastante actividad por parte de la junta directiva en estos meses. Como saben, tuvimos obviamente nuestro taller de la junta directiva previo a la reunión de ICANN y también obviamente tuvimos diferentes interacciones con la comunidad durante la propia reunión de ICANN.

Comenzamos nuestro taller el día 3 de marzo y ahí revisamos algunas cuestiones que tienen que ver con el análisis de tendencias, el análisis estratégico de tendencias que nos permite ir tomando el pulso de cómo se va moviendo el ecosistema, cómo pueden ir surgiendo cuestiones que deban ser atendidas o simplemente observadas por ICANN como organización y determinando cuál es el grado de participación que debe tener ICANN en estos diferentes escenarios.

Obviamente analizamos tendencias desde aquellas que pueden parecer irrelevantes desde alguna perspectiva hasta cuestiones que pudieran representar tal vez un riesgo existencial para la organización. Un ejemplo de esto son los nuevos o alternativos sistemas de resolución de nombres

de dominio. Estos identificadores que están surgiendo a partir de la cadena de bloques y otros sistemas alternativos. Se analiza si tienen algún impacto sobre el sistema de nombres de dominio como lo conocemos actualmente, si se debe seguir la discusión, si se debe interactuar con quienes están impulsando este tipo de sistema alternativo de identificadores en Internet o en la red, como le quieran llamar. Eso es nada más un ejemplo de las diferentes tendencias que se van analizando.

También tuvimos una sesión en la que se analizaron también tendencias en cuanto a la actividad gubernamental e intergubernamental nuevamente dentro del ecosistema en el que se mueve ICANN, desde las iniciativas de ley que se están presentando en diferentes países, principalmente en la Unión Europea, y el posible impacto que esto puede tener para las actividades de ICANN.

En el segundo día tuvimos también algún ejercicio relacionado con el abuso del sistema de nombres de dominio del DNS y platicamos también sobre las recomendaciones que estaban pendientes respecto de la revisión de seguridad, estabilidad y resiliencia, la segunda revisión, y también platicamos sobre la propuesta para diferir esta revisión de seguridad, estabilidad y resiliencia en su tercera edición, por así llamarlo.

Finalmente hubo una resolución por parte de la mesa directiva. Justamente difiriendo esta revisión para estar alineados con las recomendaciones del ATRT3. Hubo una recomendación de este grupo de revisión del ATRT3. Recomendó que prácticamente se difiriera esta siguiente revisión o versión de la revisión de seguridad, estabilidad y resiliencia hasta en tanto no se completaran las recomendaciones

relativas al ATRT. Ahorita eso está puesto en pausa y obviamente seguirá su curso conforme vaya avanzando la siguiente versión del ATRT.

También tuvimos una sesión con Göran Marby justamente hablando sobre el sistema de mitigación de amenazas al sistema de nombres de dominio. Este programa que tiene para mitigar las amenazas. También nos presentó el reporte sobre abuso del DNS.

Continuamos también con este ejercicio. Un segundo esfuerzo de ver cómo podemos priorizar las diferentes actividades que están en el plato del Board, en la mesa del Board, y tratar de alinear esto obviamente con las prioridades que pueda tener la comunidad. Qué quiere decir esto. Hay evidentemente un cúmulo importante de actividades que tiene que llevar a cabo la mesa directiva y las tenemos que priorizar en cuestión de urgencia, de disponibilidad de recursos, de relevancia para la tarea que hacemos, etc.

Hacemos este ejercicio y lo que se trata de hacer es que no sea un establecimiento unilateral por parte de la mesa directiva de prioridades sino que con este ejercicio que nosotros hacemos como mesa directiva pueda tener también su participación la comunidad y decir, estamos de acuerdo o no estamos de acuerdo en el establecimiento de las prioridades conforme lo ve no solamente la mesa directiva sino los diferentes componentes que integran a ICANN como organización. El componente de la mesa directiva es uno más de los que se tienen que analizar dentro de este ejercicio de priorización.

Después, en el último día de nuestro taller vimos también los resultados del Operational Design Phase para la siguiente ronda. [inaudible] los resultados. Vimos cómo va evolucionando este Operational Design

Phase para la siguiente ronda de nuevos gTLD. Insisto, tuvimos nuestra reunión ordinaria, nuestra reunión ordinaria como mesa directiva y se aprobaron diferentes resoluciones. Una de ellas ya se la comenté. El diferimiento de la revisión del SSR en su tercera edición. También se adoptaron las recomendaciones de la segunda fase, de la fase 2A del EPDP que envió el consejo de la GNSO. También revisamos o consideramos o sometimos a consideración del Board la resolución que se dictó en un caso de revisión independiente, en un proceso de revisión independiente o IRP, por sus siglas en inglés, que involucra el gTLD .WEB en el que hay una controversia por ahí entre diferentes actores que han participado en la subasta para adjudicarse este nuevo gTLD.

Derivado de esta controversia o de esta confrontación de intereses hubo obviamente un proceso litigioso, no en el sentido de llevarlo ante una corte aún pero sí conforme a nuestras reglas de atención a este tipo de controversias y se inició por parte de uno de estos actores este proceso de revisión independiente. El panel que atendió este proceso emitió ya su resolución haciendo algunas recomendaciones y lo que se hizo fue someter ante la consideración de la mesa directiva esta resolución y se resolvió que el comité, el BAMC, que es el Comité de Mecanismos de Rendición de cuentas, debe revisar esta resolución en detalle y hacer diferentes recomendaciones a la mesa directiva. Esto obviamente todavía no termina. Seguirá su curso. Tendrá que ser analizado por este comité del que les hablo y obviamente habrá más historia que contar.

Otra resolución que seguramente ustedes ya deben de haber visto por ahí fue el destino o esta constitución de un fondo de emergencia para apoyar el acceso continuo a Internet. Obviamente esto se deriva de la crisis que se está viviendo en Ucrania con motivo del conflicto que hay

en la región y aquí se tomó la determinación de hacer un aprovisionamiento de un millón de dólares para que se pudiera trabajar con gente de la región para tratar de garantizar el acceso continuo a Internet en esta zona de conflicto. Obviamente también dentro de la misión que tiene ICANN y cuidando de que todo en momento haya perfecta transparencia y manejo de los fondos.

Esto a grandes rasgos, Augusto y toda la región, es lo que ha estado haciendo la mesa directiva. La próxima semana estaremos reuniéndonos en Los Ángeles por primera vez en mucho tiempo en una sesión presencial tanto con líderes de las diferentes organizaciones de soporte y comités consultivos como también como grupo, como mesa directiva. Va a ser nuestra primera reunión presencial en mucho tiempo. Con mucho gusto les estaré actualizando en su momento sobre las actividades que llevemos a cabo en este taller que llevaremos a cabo en Los Ángeles y de esta reunión que tendremos el presidente y su servidor como vicepresidente de la mesa directiva con el liderazgo de los diferentes SO y AC. Agradezco la oportunidad de estar con ustedes, Augusto. Permanezco obviamente por si hay alguna pregunta o algún comentario respecto de lo que acabo de platicar.

AUGUSTO HO: Muchísimas gracias, León. Le voy a dar el uso de la palabra rápidamente a Carlos Aguirre, por favor, para que nos dé su informe, tratando, Carlos, de compactar el tiempo lo más posible, que estamos por [inaudible].

CARLOS DIONISIO AGUIRRE: Muchas gracias, Augusto. Yo había levantado la mano para hacer una pregunta a León pero atento al tiempo que nos corre vamos a dejar la pregunta y se la haré de alguna otra manera. La idea de mi intervención en esta reunión es justamente también comentar lo que se ha estado tratando dentro del comité de ALAC en estos últimos tiempos. La verdad es que tiene mucho que ver con muchas de las cosas que ya ha mencionado León. Fundamentalmente todo esto se maneja dentro del grupo de políticas consolidadas de ALAC. Este grupo de políticas consolidadas se reúne todos los miércoles y yo le pediría al staff si puede poner a disposición de todos los participantes aquí el link para esa reunión porque esa reunión es absolutamente abierta y pueden participar todos y ponerse en autos sobre lo que allí está sucediendo.

De todas maneras les cuento rápidamente, y de vuelta atento al tiempo que nos está corriendo, que los temas que se han estado tratando en este grupo de políticas consolidadas tienen que ver con el uso indebido y el abuso del DNS. Fundamentalmente en la última reunión se habló sobre el tema del registro malicioso en bloques fundamentalmente que ha sucedido también durante la pandemia y cómo mitigar estos ataques, estas formas de entrometerse o de tratar de generar situaciones complicadas fundamentalmente para los usuarios. Estoy repitiendo mucho la palabra fundamentalmente. [inaudible].

Bien. Otro de los temas que se han tratado ha sido el proceso de políticas de la revisión justamente de la política de transferencia de dominios y aquí se ha planteado una cuestión endilgándole alguna complejidad que genera el GDPR. Se ha hablado también de los plazos para hacer estas transferencias teniendo en cuenta muchas veces el interés de los registros y aquí me parece que la región debería trabajar o

debería a lo mejor profundizar en esas cuestiones para llevar adelante el interés del usuario individual, del usuario final de Internet, porque muchas veces, y esta es una cuestión absolutamente mía y particular, que veo que muchas veces personas que son miembros del comité ALAC están por su antigüedad o por sus relaciones de mucho tiempo influenciadas por algunas otras posiciones como eventualmente la GNSO y del business constituency donde creo que hay mucho interés por custodiar los intereses fundamentalmente económicos de los registros y no particularmente de los usuarios individuales o usuarios finales de Internet. Esto creo que deberíamos trabajarlo en la región y plantear algunas cuestiones en el tema que [inaudible] recién del abuso de Internet, del uso indebido de Internet. Cómo hacer más fácil la denuncia por parte del usuario de Internet, cómo hacérsela más sencilla y cómo poder generar una solución o una satisfacción en ese usuario que vio vulnerados sus derechos a partir de estas cuestiones.

Otro de los temas que también se trataron en estos últimos tiempos en este grupo de políticas consolidadas es el procedimiento de desarrollo de políticas expedito sobre los dominios internacionalizados y que tienen que ver con la aceptación universal. Aquí hay varias cuestiones con relación a distintos lugares en el planeta donde se plantean algunos caracteres particulares, fundamentalmente uno que me acuerdo es en Myanmar.

Otro de los temas perdón que vaya muy rápido pero otro de los temas que es el sistema de acceso estandarizado o SSAD, que también se ha tratado dentro de este grupo de ALAC. Finalmente, lo que se está tratando ahora y que nos está corriendo el tiempo porque vencen los plazos para definir es la agenda para el ICANN74, que ya se nos viene

encima y qué es lo que se va a plantear en esta nueva reunión donde también hay otro problema que se suma, que es una reunión híbrida donde pocos van a poder participar de una reunión presencial y otros en otros lugares de manera remota, cómo hacer para congeniar este tipo de participación. Es cierto también que el staff lo está planteando como un desafío porque es algo nuevo que se está planteando para ellos, para nosotros los participantes y entonces veremos cómo resulta esto para próximas ediciones en otras reuniones de ICANN.

Otro tema, y que va a ser el primero de ICANN74, donde va a participar la comunidad At-Large y está planteado para el primer día en la primera hora, es algo que también proviene con intereses [inaudible] y esto permítanme que lo asuma como propio, con intereses de la GNSO, para hablar sobre los procedimientos subsecuentes, lo que viene para delante. Fundamentalmente lo que le interesa a la GNSO es ver qué pasa con la nueva ronda de gTLD. Yo no sé si esto es de interés para los usuarios. Sí es de interés para la industria y los [inaudible], para el business constituency, y están promocionándolo y lo están llevando adelante con mucho esfuerzo. Allí es donde nos involucran a nosotros porque nosotros, los miembros de ALAC, tenemos que dar asesoramiento sobre estas cuestiones. Esto es lo que yo puedo decir rápidamente, Augusto. Gracias por este tiempo y perdón por ser tan escueto a partir del tiempo que nos está corriendo.

AUGUSTO HO: Gracias, Carlos. Vamos rápidamente a escuchar la intervención de Sergio Salinas Porto, para que nos ponga al día en cuanto al progreso del

programa LAC Digital. Por favor, Sergio, adelante. Los micrófonos son tuyos.

SERGIO SALINAS PORTO: Muchas gracias, Augusto. Muy buenas tardes, noches para todos y todas. Voy a ser muy conciso, Augusto, así podemos seguir y llegar al punto final quizá en horario. Hemos avanzado. Tenemos aceptación de los tres temas. Aceptación universal creo que ya tenemos a todos los participantes. Estamos viendo que haya cuatro pero en principio ya hay tres garantizados. Eso nos pondría en una situación ventajosa por los otros dos, los otros dos objetivos que tenemos, tanto el de Internet como servicio público esencial como el otro que es el de infraestructura en zonas rurales, estaríamos también avanzados.

Yo creo que al finalizar esta semana tendríamos ya los 24 oradores. En realidad los 12 países intervinientes como para ponerlos y ya poder ponerlos en la web. La web ya está casi terminada. Faltarían las fotos y el currículum de quienes van a exponer, tanto sea por el gobierno como el de sociedad civil. Entiendo yo que estaríamos casi al filo de poder presentar un evento que llegue al 17 de mayo con volumen de comunicación para tener la sala llena. En unos días vamos a tener información más fuerte de esto y podemos seguramente avanzar. Igualmente, me comprometo como hice la otra vez, la semana pasada a demandar un informe por escrito a toda la región. Voy a volver a hacerlo y aprovecho esto para decirle a mi amigo Alejandro Pisanty que seguramente mañana vía mail y luego llamada por teléfono estaré hablando para que México te presente. Ya había hecho una pequeña

intervención con él pero me gustaría terminar de cerrarlo. Nada más. Muchas gracias, señor Presidente.

AUGUSTO HO: Gracias, Sergio, a ti, por ponernos al día en todo lo que está sucediendo con el programa. Por favor, en términos del tiempo, voy a solicitar a Claire que nos hable sobre elecciones 2022. Adelante, Claire, por favor.

CLAIRE CRAIG: Las elecciones para el 2022, hay dos posiciones disponibles en este momento para el año. Creo que deberían estar viéndolas en pantalla en este momento. Estas posiciones son: el representante del ALAC que corresponde a la región D, que es Argentina, Brasil, Paraguay y Uruguay, y luego la posición para el NomCom, que es la región de América Central, Belice, Costa Rica, el Salvador, Guatemala, Honduras, Nicaragua, México y Panamá.

Con respecto a estas elecciones, hoy… Disculpas, voy a comenzar otra vez. El 18 de abril, que es hoy, fue el anuncio de las nominaciones. Entre el 18 y el 29 de abril tenemos el periodo de nominaciones que son 10 días hábiles. El 26 de mayo es la fecha límite para la aceptación de las nominaciones. Del 9 al 12 de mayo son las convocatorias a los candidatos de ser así deseado por las RALO. Del 13 al 20 de mayo son las elecciones. De ser requerido, comenzarán no más de una semana después del plazo límite para las aceptaciones de las nominaciones y terminarán no después de dos semanas después de este plazo.

Por último, en la asamblea general, que es en la ICANN75, los miembros del ALAC y los líderes de las RALO asumirán sus cargos al final de la

asamblea general después del cierre de la reunión de la junta directiva el 22 de septiembre de 2022. Esta información está disponible en el sitio web. Disculpas por haber ido tan rápido. Les sugiero que consulten esta información y formulen sus nominaciones aquellos de los territorios específicos que corresponde. La región D para el ALAC y la región A, que es América Central y México, para el NomCom. Muchas gracias.

AUGUSTO HO: Muchas gracias, Claire. Estamos ya en el tiempo. Se nos han dado otros dos minutos de más. Vamos a tener que vernos en la necesidad de cerrar la reunión del día de hoy. Han quedado pequeños temas pendientes pero van a quedar para el próximo encuentro. No quiero cerrar sin antes recordarles por favor que al final de la reunión se va a enviar una encuesta para que la llenen por favor. Todavía tenemos dos minutos. Me avisan. Vamos a darle el uso de la palabra a Vanda, por favor, para que utilice esos dos minutos. Adelante, Vanda, por favor.

VANDA SCARTEZINI: Sí. Hola. Gracias. Simplemente para informarles a ustedes que salió todo muy bien con la reunión presencial en Washington, en Estados Unidos, de todo el NomCom. Estuvimos juntos como 14 personas y todo salió muy bien. Hicimos tests diarios a las 7 de la mañana, antes de entrar en la sala de reunión. Salimos todos con salud, sin problema. Me pareció que estuvo muy, muy, muy organizado, perfecto con las dificultades, claro, de transporte, de todo, pero sin problemas graves o problemas [inaudible]. Todo salió muy, muy bien con el staff en Los Ángeles y alrededor del mundo. Nos atendió perfectamente de forma híbrida así como los tres amigos que estaban, miembros de NomCom, que no

	lograron su pasaporte, su visa en tiempo para la reunión. Solo pudieron asistir como híbridos por teléfono. Estaba muy bien, muy organizado. Hablamos muy bien. Hablamos tranquilamente. Sacamos fotos incluso con los miembros que estaban fuera. Salió todo muy, muy bien. Para decirles que la experiencia piloto, como dijo Maarten, fue de éxito. Estamos más tranquilos para irnos, quien pueda, a La Haya. Salimos muy bien. Gracias.
AUGUSTO HO:	Gracias, Vanda. Ahora sí, Silvia, a menos que haya algo pendiente, creo que podemos cerrar, porque ya estamos en el tiempo.
SILVIA VIVANCO:	Sí. Entonces eso es todo. Les pido por favor que todos completen la encuesta de evaluación que aparecerá automáticamente al cerrar este Zoom. Les agradecemos por esta participación esta noche. Muchas gracias.
AUGUSTO HO:	Gracias a todos. Buenas noches.

[FIN DE LA TRANSCRIPCIÓN]