
CLAUDIA RUÍZ: Buenas tardes y buenas noches a todos, bienvenidos a la llamada mensual de LACRALO, este lunes 19 de abril de 2021 a las 23:00 horas UTC.

En la llamada del día de hoy en el canal en español tenemos a Augusto Ho, el Dr. Pablo Rodríguez, Harold Arcos, Vanda Scartezini, Adrián Carballo, Alberto Soto, Carlos Aguirre, Gerardo Martínez Hernández, Hannah Frank, José Arce y Lito Ibarra.

Tenemos disculpas por parte de Lilian Ivette De Luque, Dev Anand Teelucksingh y León Sánchez. Tenemos a Gilberto Lara que está entrando.

Y por parte del personal tenemos a Heidi Ullrich, Silvia Vivanco y mi persona, Claudia Ruíz, Administrando la llamada el día de hoy. Tenemos interpretación en español, portugués y francés, nuestros intérpretes que nos acompañan son Paula y Marina en español, Bettina y Esperanza en portugués, y Claire e Isabelle en francés.

Antes de empezar quisiera pedirles a todos que por favor digan su nombre al tomar la palabra y también que dejen sus micrófonos en mudo para prevenir el sonido. Muchas gracias y con esto le paso la llamada a usted, Augusto.

AUGUSTO HO: Muchísimas gracias. Muy buenas tardes a todos. En primera instancia, excusar la presencia de momento de Sergio, tuvo un imprevisto con una reunión que le colisionaba con esta, por ende, en mi condición de

Nota: El contenido de este documento es producto resultante de la transcripción de un archivo de audio a un archivo de texto. Si bien la transcripción es fiel al audio en su mayor proporción, en algunos casos puede hallarse incompleta o inexacta por falta de fidelidad del audio, como también puede haber sido corregida gramaticalmente para mejorar la calidad y comprensión del texto. Esta transcripción es proporcionada como material adicional al archivo, pero no debe ser considerada como registro autoritativo.

vicepresidente pues me corresponde hacer o llevar adelante la reunión de hoy, ¿verdad?

Dándole gracias, ante todo, a todos ustedes por haberse conectado en tiempo y aprovechar esta reunión mensual que está bien cargada de bastante información que necesitamos actualizar, ¿no? Así es la cosa, entonces voy a darle la palabra a Harold para efectos de que nos ponga al día con la agenda de hoy. Adelante, Harold.

HAROLD ARCOS:

Gracias, Augusto. Saludos a todos en la región, vamos a iniciar con la agenda del día de hoy, con el webinar del DNSSEC, que, con la amabilidad de Pablo Rodríguez, presidente de NIC, es quién lo va a facilitar, que en esta oportunidad nos acompaña nuevamente.

Posterior, vamos a tener los comentarios temáticos de los ALAC members, con la presencia de Sylvia Herlein, también en el punto número 6 de la agenda tenemos nuestros informes de los directores de los grupos de trabajo de LACRALO, comenzando con IDN y Aceptación Universal.

Luego el grupo de trabajo de capacitación, nuestro recién estrenado director de WHOIS y el informe del grupo de trabajo de comunicaciones a cargo de Marcelo Rodríguez. En nuestro punto número 7 tendremos el informe de Social Media, en este caso, excusamos a la colega Lilian De Luque, tuvo que ausentarse por razones familiares.

Y el punto número 8 es la actualización regional, donde estaremos viendo algunos temas relacionados con la región, la Asamblea General Virtual, el plan estratégico y elecciones LACRALO 2021.

En este punto si hubiese algún miembro que desee incorporar algún tema, puede hacerlo en este momento o esperar a que lleguemos a ese punto de la agenda. También queremos informarles que, en ese punto, pues también estaremos tomando aquellos temas que quisieran que fuesen abordados entre esta reunión y la siguiente o que quisieran abordarse en la siguiente agenda del próximo mes.

Esto porque hay varios temas en la agenda y que bueno, podemos empezar a moverlos a través de la lista de correo. Comentándoles esto y dando tiempo a ver si hay alguna mano levantada o alguna nota en nuestro chat que quisiera incorporar alguno, entonces damos por aprobada la agenda y avanzamos. Adelante, Augusto.

AUGUSTO HO:

Muchísimas gracias, Harold. Bueno, vamos a entrar de lleno hoy y tenemos el grato placer de contar con la participación del Dr. Pablo Rodríguez, vicepresidente de NIC Puerto Rico, yo voy a procurar por aquí ver el tema de su hoja de vida, la verdad que es muy extensa y, por ende, me puedo tomar algunos minutos.

Pero el tema que va a desarrollar hoy es, extensión de seguridad del Sistema de Nombres de Dominios, entiendo que, por sus siglas en inglés, es DNSSEC.

Así es que Don Pablo Rodríguez es altamente conocido por acá, los micrófonos son suyos, haciéndole la aclaración de que tiene suficiente tiempo para exponer y vamos a reservar algunos minutos al final, a efectos de preguntas y respuestas, unos 10 minutos por lo menos para

preguntas que puedan formularse de parte de la audiencia, ¿ok?
Adelante, Don Pablo.

CLAUDIA RUÍZ: Hola, Pablo. Disculpas, estás en mute de nuevo.

PABLO RODRIGUEZ: Buenas noches a todos y muchísimas gracias, Augusto, Adrián, Harold y todos los que están participando, un gran abrazo aquí desde Puerto Rico, espero que me estén escuchando bien.

El propósito de esta presentación es la de familiarizar a personas que no están involucradas en nuestra comunidad con el tema del DNSSEC, qué es y por qué es importante en tu vida. Y este es un gran mensaje que necesitamos llevar a todas las personas que forman parte de nuestra comunidad. Próximo slide, por favor.

Y así como dicen las escrituras, en el principio, un grupo de estudiantes graduados en la Universidad de California, Los Ángeles, o como se conoce UCLA, intentaban enviar un mensaje, un comando de login a Stanford Research Institute a unas cuantas millas de donde estaban ellos y comenzaron haciendo eso, conectados telefónicamente, les decía: “Enviamos la L, ¿ves la L de login?” “Sí la vemos” “Ok, ahora vamos a enviar la O”.

Y le daban a la letra o, “¿ves la O?” “Sí, la vemos”. Cuando le van a dar la letra G se cae el sistema y lo único con que quedan es con esta frase interrumpida que decía “LO”, que en inglés se usa como Lo. Comienza diciendo Lo and Behold “miren lo que tenemos aquí” ¿no?

Entonces fue así como algo profético, este es el comienzo de algo singular, este es el comienzo de una nueva era y comienza con esa frase tan humilde, con LO.

Aquí en la gráfica de la izquierda podemos ver cómo el campus de UCLA intentaba comunicarse con Stanford Research Institute, SRI, y pueden ver los otros dos nodos que habían ahí, que era UCSB que es la Universidad De California en Santa Bárbara y el otro era en Utah, ¿no?

Entonces ese es el gran comienzo humilde de lo que ahora nosotros conocemos como internet y que, parecería inimaginable para muchos de nuestros jóvenes, muchos de nuestros hijos, un mundo que no tuviera internet. Próximo slide, por favor.

Básicamente de la manera que ellos se estaban conectando era por un protocolo que había sido diseñado por el profesor, el Dr. Vinton Cerf y también por el Prof. Robert Kahn, ellos tuvieron la capacidad de crear... Llevaban mucho tiempo luchando con esto, con la creación de este protocolo, pero no es hasta que Vinton Cerf entra en la relación con Bob Kahn que pueden desarrollar un protocolo, que le llaman el protocolo de control de transmisión y el protocolo de internet.

Muchos de los que estamos en esta industria le llamamos TCP/IP, entonces en inglés lo mencionan como TCP/IP, ¿no? Y, finalmente, esa es la manera donde ellos comienzan a poder enviar paquetes del punto A al punto B y asegurarse de que esos paquetes de información llegaran allí.

Hoy día, nosotros usamos una asociación o una relación de un nombre de dominio. Si se dan cuenta en aquel tiempo cuando ellos comenzaron

a trabajar con esto, estos protocolos de IP era un número así muy similar a ese que estamos viendo ahí, 123.456.789.12, pero ¿quién pudiera acordarse de un número así?

¿No es mucho más fácil acordarse de LACRALO.ORG? Un nombre memorable, un nombre que nos permita acordarnos de nosotros, de manera que si yo puedo decirte, en vez de: “Conéctate a mí con un número de IP”. Es mucho más fácil que yo te diga: “Conéctate a ICANN.ORG, conéctate a DOMINIOS.PR, conéctate a NASA.ORG o .DOC mejor dicho”.

Entonces es mucho más fácil, son nombres memorables, nosotros nos acordamos de nombres, asociamos caras y nombres mucho más fácil que si nos dieran solamente una dirección numérica de esas personas. Entonces hoy día lo que hemos hecho es asociar, relacionar un nombre de dominio con un número de IP, que nos permite llegar y desde nuestras casas podemos acercarnos a una página web que existe en distintas partes del mundo.

Y eso lo hacemos de manera tan fácil que verdaderamente no pensamos mucho sobre el cómo, sencillamente escribo un nombre de dominio y mi expectativa es que voy a llegar ahí sin ningún problema. Próxima por favor.

Desafortunadamente en aquel momento que se estaba haciendo todo este asunto, la gran misión era llegar de UCLA, del campus de la Universidad de California en Los Ángeles, a conectarse al Instituto de investigaciones de Stanford, nada más. Solamente queremos un diseño, tenemos un diseño para conectarnos del punto A al punto B y ya, nada más.

Nadie en ese momento imaginó que pudiera existir la posibilidad de que alguien usara este diseño, esta arquitectura, para cometer fraudes, por lo tanto, como esa fue la situación nadie se dio a la tarea de pensar cómo nos podíamos conectar de una manera segura, no se incluyeron, no se diseñaron módulos que pudieran ayudar a prevenir fraude porque nadie lo pensaba, ya de por sí era un gran logro conectarse del nodo A al nodo B.

Pensar que alguien lo usaría para cometer fraude era impensable porque verdaderamente en ese momento quién hubiera imaginado que esa cosa que ellos estaban haciendo, ese ejercicio que estaban haciendo se iba a convertir en algo que iba a tener connotaciones comerciales, que iba a tener connotaciones de seguridad nacional para un país, para el usuario y así por el estilo.

Entonces había un elemento de ingenuidad, de que esto es algo que vamos a usar, nadie lo va a usar para cometer ningún tipo de fraude ni crimen, por lo tanto, no nos tenemos que preocupar con ellos. Gracias, por favor la próxima.

Entonces se acabó la inocencia, el fin de la inocencia comienza con el Prof. Bellovin, quien en aquel momento... El Prof. Steve Bellovin descubre; y esto es muy interesante porque el Prof. Bellovin trabajaba en los laboratorios de AT&T, y ya a partir de finales de la década de los 80', principio de los 90', ya él viene sospechando que la arquitectura del DNS tiene serias vulnerabilidades que podrían ser explotadas.

Sin embargo, esto se descubre muy cerquita del comienzo del nacimiento del internet y difícilmente muchas personas pudieran saber

cómo se podían explotar esas vulnerabilidades, así que él se quedó callado y no compartió esa información por prácticamente 5 años.

Y no es hasta que en una conferencia en 1995 en Utah, el Prof. Bellovin publica un artículo donde comienza hablando de las vulnerabilidades que tiene el DNS y de que pudiera ser posible raptar un website y redirigirlo a otro lugar, que pudiera ser posible que alguien se hiciera pasar por otro y que no tuviéramos la capacidad de darnos cuenta de que algo así pudiera estar sucediendo.

Así que, en ese momento comienza toda una discusión en el IETF, en el Internet Engineering Task Force, comienza todo un compartir de ideas y de los expertos en ese momento, comienzan a intercambiar información de cómo podemos resolver este problema.

“Ya que identificamos el problema, ahora vamos a ver cómo lo podemos resolver”. Y entran en todo este acuerdo. Es importante destacar que como en tantas otras cosas, en situaciones como estas una gran pregunta era: “¿Será verdad que es posible que alguien tenga la capacidad de raptar un website? ¿Será posible que alguien tenga la capacidad de hacerse pasar por otro?”

Y había muchas personas que dudaban de que esto fuera posible, pero no es hasta el año 2008 cuando Dan Kaminsky logra físicamente decir: “Ese ataque es posible y se hace de esta manera”. Logra el ataque y demuestra cómo se hace el ataque. Y aquí se le acabó el argumento a aquellos que dudaban y por primera vez se va este velo de los ojos, de que: “¡Wow! Es posible que algo así suceda”.

Y Dan Kaminsky comienza a trabajar con grandes empresas, como es Microsoft y tantos otros para buscar maneras de cómo se podía hacer esto. Es importante también destacar que ya para el 2004-2005 ya venía una versión de DNSSEC que se estaba desarrollando y se estaba comenzando a implementar, se comenzaba a tratar y esto le dio una velocidad increíble a ese descubrimiento.

Así que comenzaron a buscar maneras, lo que le llamamos en nuestra industria, los parches, ¿no? “Vamos a ver cómo vamos a parchar esto”. A manera de metáfora de que, hay un agujero en algún lugar por donde un malhechor pudiera aprovechar el agujero, siendo esa una vulnerabilidad, que un malhechor pudiera usar para hacerse pasar por otro y cometer un crimen.

Así pasa el tiempo, este protocolo nace y se adopta con mucha fuerza, entre una gran cantidad de pioneros que comenzaron a adoptarlo y como en tantas otras cosas, había muchas soluciones compitiendo.

Me voy a dar la libertad de cátedra de hacer referencia – y perdónenme aquellos de ustedes que son muy jóvenes para acordarse de esto –, pero hubo un momento donde antes de que saliera el VHS; que tenía un cassette muy grande para grabar películas, había otras soluciones que se llamaban betamax, por ejemplo, competían y hacían cosas muy similares, se parecían y eran bastante funcionales.

Excepto que en algún momento alguien comenzó a adoptar más VHS que betamax y el VHS se convirtió en un estándar, o sea que también había otras soluciones que competían con el DNSSEC y a través de los años el DNSSEC se convirtió en un estándar, aproximadamente para esa

misma época que Dan Kaminsky demuestra el ataque, aproximadamente en el 2008.

Como resultado de eso, nosotros comenzamos entonces a implementar y a fomentar el uso de esa tecnología. Por favor, próximo slide. Veamos, ¿qué es DNSSEC? Y DNSSEC es un protocolo que hace dos cosas, refuerza la autenticidad del DNS usando firmas digitales basadas en criptografía de clave pública o lo que conocemos como KPI.

Con DNSSEC no son las consultas y las respuestas las que en sí están firmadas criptográficamente, pero lo que está firmado criptográficamente son los datos que se están usando. Entonces aquí comenzamos a usar unas claves para asegurarnos de dos cosas. Próximo slide, por favor.

Y son dos características muy importantes. La primera, la autenticidad del origen de dónde vienen los datos, en otras palabras, cuando yo me comunique a través de un enlace para participar en esta reunión, mi expectativa es que yo me voy a conectar donde se va a celebrar la reunión de LACRALO. De la misma manera, cuando usted va a una página web, su expectativa es, ¿con quién se comunicó? Es la organización y/o persona con quien usted entiende que quiere comunicarse.

Así que, la autenticación del origen de los datos permite que un resolver o un resolutor verifique criptográficamente que los datos que ha recibido realmente provienen del lugar que usted espera que vengan. O sea, cuando yo busco información de LACRALO, yo me estoy comunicando con LACRALO y no es un tercero que ha interceptado esta conexión y me está pasando información falsa.

Cuando yo me comunico con mi banco, yo quiero asegurarme de que estoy hablando con mi banco. La segunda característica importantísima que ofrece DNSSEC es que, protege la integridad de que los datos que yo estoy recibiendo no han sido modificados, en otras palabras, no hay un tercero que haya interceptado esta comunicación y la información que me esté enviando sea información falsa.

O sea, la protección de la integridad de los datos permite al resolver o al que está recibiendo los datos, saber que los datos no se han modificado, y que desde el momento que salieron de su origen no han sido interceptados y mucho menos modificados. Esto da una gran seguridad, el saber que me conecté con quien yo quiero conectarme y que la información que estoy recibiendo es información apropiada y que no estoy viendo información falsa.

Porque, ¿de qué otra manera pudiéramos asegurarnos nosotros de que estoy hablando con quien yo quiero hablar? De que me estoy conectando con quien yo quiero conectarme y no que hay un tercero que esté manipulando todo esto, y me está llevando a un lugar donde puedo ser víctima de robo de identidad y tantos otros crímenes. Próximo slide, por favor. Gracias.

Entonces el DNSSEC reduce vulnerabilidades a los ataques, ¿cómo? Pues como ya mencionamos en el slide previo, lo hace usando estas claves públicas que, cuando el resolver se conecta puede ver si es o no la organización, institución o persona con quien me quiero conectar.

Miren en el diagrama, sin DNSSEC. Una persona intenta comunicarse con su banco, ese banco que no tiene DNSSEC puede ser víctima de que un malhechor logre falsamente enviar una respuesta falsa a un resolver y

hacer que el resolver tome esa respuesta como buena, y la convierta en la respuesta de ese dominio.

En otras palabras, yo voy a MIBANCO.PR, MIBANCO.PR no tienen DNSSEC, cuando alguien trata de comunicarse, el usuario A intenta comunicarse con su banco para acceder a su cuenta de banco y lo que ha sucedido es que, un malhechor ha tomado el resolver y le ha enviado una respuesta falsa y dice: "MIBANCO.PR ahora se encuentra en este otro IP". Y eso se llama envenenar el caché.

¿Por qué? Porque la arquitectura del DNS está hecha para ser eficiente, ¿y cómo podemos ser eficientes? Bueno, teniendo una arquitectura que se acuerde, ¿que se acuerde de qué? De la primera respuesta que le dieron.

Así que, si un malhechor le envía una respuesta falsa al resolver, él la graba y a todos los que vayan a ese lugar, los envía a este otro lugar que posiblemente puede ser idéntico al de su banco, al de MIBANCO.PR, excepto que ahí están capturando credenciales de nombre de usuario, de contraseña y que luego, de una manera muy sutil regresarán a MIBANCO.PR y puedan sacar dinero mío.

Puedan no solamente robarme dinero, pero también si fuera... Vamos a suponer en Hacienda o en el departamento demográfico, pudieran capturar datos personales míos que pudieran ser usados para cometer fraudes o algún otro tipo de crimen.

Entonces es importantísimo que las instituciones con que nosotros hacemos negocio o con las instituciones, por ejemplo, gubernamentales con quienes tenemos interacciones, ya sea el Ministerio Demográfico, ya

sea Hacienda, mi banco, mi hospital que hayan implementado este tipo de tecnología, que permita protegerme por lo menos de ese tipo de ataque del envenenamiento del caché que da paso a muchos otros ataques.

Por ejemplo, el ataque de robo de identidad no sucede con el envenenamiento del caché, pero comienza con el envenenamiento del caché, ¿por qué? Porque me redirige a un lugar falso donde están capturando información, donde están capturando mis credenciales para cometer algún tipo de crimen.

Y ahí comienza entonces el phishing, ahí comienza el robo de identidad, ahí comienza actividades fraudulentas, así que es importantísimo, la gran puerta para muchos otros ataques comienza con un envenenamiento de caché y el DNSSEC precisamente detiene ese tipo de actividad.

Cuando tenemos DNSSEC el resolver envía también la clave pública, de tal manera que se puede comparar con la clave pública que se está usando en esa zona, si no son iguales el resolver lo que hace es que devuelve un error diciendo: "403" "la página no existe". Pero no lo envía a ningún otro lugar, a diferencia de cuando uno no tiene DNSSEC y sí lo hace llegar a otro lugar.

Entonces aquí podemos ver de una manera a nivel muy alto, ¿no? De cómo la vulnerabilidad funciona con y sin DNSSEC, pero, por supuesto, esto es mucho más complicado y mucho más profundo de lo que estoy explicando.

Volvemos, el propósito de esta presentación es que podamos entender qué es DNSSEC, cómo nos protege y cómo usted puede ser partícipe de ayudar a nuestra comunidad, a esta comunidad, a ser más robusta, resiliente y segura. Próximo slide, por favor.

El DNSSEC también tiene algo que promueve la innovación y promueve la innovación porque actualmente se han desarrollado nuevos protocolos teniendo a DNSSEC en cuenta y aprovechando las características importantes que ya hemos visto y discutido del DNSSEC, su autenticación y la capacidad que tiene de asegurarme la validación de que la información no ha sido esparcificada.

Hay otras tecnologías, otros protocolos como es el protocolo DANE, el protocolo DANE es un ejemplo que permite que la publicación de claves de seguridad a nivel del TLS, el Transport Layer Security, y a nivel de transporte de seguridad pueda proteger los correos, proporcione y nos provea una forma de verificar esa autenticidad de esas claves.

Es importantísimo porque tenemos que destacar que el DNSSEC no es la única solución, no es lo que le llaman una bala de plata, no es un silver bullet que resuelve todos los problemas o todas las vulnerabilidades que potencialmente pueden ser explotadas por malhechores.

Y, por lo tanto, tenemos que tener muchas soluciones para muchas cosas que en subconjunto nos ayudan a asegurar una y otra vez que nuestra seguridad del usuario y de las distintas organizaciones se pueda mejorar.

Entonces aquí lo que estamos buscando es un ejemplo de un protocolo como es DANE, que funciona solamente en zonas que ya están firmadas con DNSSEC.

No es posible poner DANE y otros protocolos en zonas que no están firmadas, así que aquí vemos un beneficio de firmar la zona con DNSSEC porque entonces les permite a aquellos que han implementado DNSSEC, poder implementar otras tecnologías que siguen sumando a la seguridad de ese ecosistema. Próxima por favor.

Y en este momento haciendo eco de esas palabras que ya mencioné, el DNSSEC no es una bala de plata, no resuelve todos los problemas, por ejemplo, un problema que no resuelve es el DDoS.

El DDoS, en inglés, es un ataque que usa muchos terminales que han sido convertidos en zombies para atacar con preguntas desde muchos lugares a la misma vez y tomando un servidor que es incapaz de poder contestar a todos esas preguntas, a todos esos request no les puede contestar de manera efectiva y lo que hace es que los saca del aire, lo saca de función. Y entonces se llama un Distributed Denial Of Service, en otras palabras, es una denegación de servicios distribuida, ¿por qué? Porque está distribuida a través de muchos terminales que están atacando desde distintas partes.

Y volvemos. Es importante asegurar que nuestras infraestructuras están tomando en cuenta todas las posibles soluciones de seguridad, para asegurar que no haya estas vulnerabilidades que pueden ser explotadas.

También es importante destacar que con cada solución que nosotros traemos también traemos un problema y eso es característico de los

problemas complejos, los problemas complejos son diferentes a los problemas complicados. Complejo y complicado no es lo mismo.

Un problema complicado es aquel que requiere de personas expertas y de recursos para solucionarlo, ¿qué pudiera ser un problema complejo? Queremos enviar una nave al planeta Marte, ¿qué hace falta para eso? Pues bueno, hacen falta, como se sabe, muchos ingenieros eléctricos, electrónicos, de computación, ingenieros químicos para hablar del combustible, ingenieros astrónomos porque necesitamos astronautas, gente de medicina que investigue cómo el cuerpo funciona en cero gravedad.

Hay una cantidad de cosas que son necesarias porque ya están definidas o, por ejemplo, ¿cómo podemos crear una computadora? Cada uno de los componentes de una computadora están definidos, son muchos, son complicados, pero están definidos y no cambia su definición.

Sin embargo, los problemas complejos no son fáciles de definir porque no sabemos necesariamente cómo funciona cada vez que implementamos una solución para eso.

Aprovecho en hacer una salvedad, un ejemplo que me gusta dar de la diferencia de las características de un problema complejo, fue en un año en el que hubo un invierno muy crudo en los Estados Unidos y los guardabosques decidieron que era buena idea darle comida a los ciervos que apenas podían llegar tan profundo en la nieve para comer el poquito de hierbas que había.

Entonces empezaron a darle de comer a los ciervos y los ciervos comenzaron a comer la corteza de un árbol, creció la población de

ciervos, se comieron la corteza de los árboles. Y en esa corteza había precisamente los árboles que a los castores les gusta usar para crear sus piscinas, sus pequeñas reservas de agua, donde ellos hacen sus casitas y puedan tener a sus crías ahí.

Así que los castores de esa área se fueron y se fueron muy lejos, ¿y qué sucede? Que cuando vienen los salmones empiezan a buscar donde viven los castores, porque en esas piscinas que se forman como resultado de las represas; que hacen los castores, pueden desovar ahí y la corriente no se lleva los huevos.

Por falta de esas casitas que hacían los castores los salmones desovaron, como siempre lo han hecho y se fueron, excepto que pasó un año y al próximo año la población de salmones bajó, bajó de una manera tan grande que se perdieron millones de dólares en negocios de enlatados y capturado de salmones en la industria de los salmones.

Quién hubiera tenido la visión, la capacidad de decir dos años atrás que darles comida a los ciervos nos iba a causar un problema de quedarnos sin salmón en dos años. La distinción, la característica clásica de un problema complejo es que, son incapaces de poder ver a largo plazo en muchos años, como esta solución que estamos implementando hoy, puede ser un problema en el futuro.

Tanto así que los problemas organizacionales como personales que tenemos, y que solucionamos hoy día, son el resultado en muchos casos de soluciones que damos, de decisiones que tomamos y aceptamos pensando que era la mejor solución en ese momento.

Así que eso es parte de lo que es un problema complejo y ves cómo contrasta con un problema complicado. DNSSEC es un problema complejo, a cada solución que damos a DNSSEC ha causado un nuevo problema.

Entonces ustedes habrán visto que existe un paso donde, primero, hubo DNSSEC, ahora tenemos DNSSEC 3 y así por el estilo, seguimos haciendo investigaciones muy profundas para asegurarnos de que cuando venga el próximo problema, estemos listos para poder mitigar ese problema, mitigar esos riesgos.

Volviendo a este slide, otra cosa que DNSSEC no hace es mantener la confidencialidad de los datos que nosotros enviamos, entonces lo que me dice es: "Estos datos vienen de tal lugar. Estos datos no han sido falsificados". Pero están libremente abiertos, cualquiera los puede ver.

Entonces necesitamos buscar maneras de cómo podemos garantizar la privacidad de esos datos y ahí tenemos una cantidad de resoluciones que están en desarrollo, que se están usando, como es el DoT o DNS/TLS y el DoH o DNS/HTTPS, pero esas soluciones aquí no las vamos a discutir en este momento.

Otra cosa que tampoco hace el DNSSEC es proteger al servidor, o sea que el servidor está vulnerable a otra cantidad de ataques que también tenemos que estar preparados para asegurarnos de que el servidor se le haya tomado en cuenta todas las posibles vulnerabilidades que puede tener y también hayan sido tomado en cuenta, y se haya actuado sobre la misma para evitar que una cosa así suceda, para que un ataque suceda.

Un momentito... Próximo slide, por favor, próximo slide. A través de los años, en 1995 ya se venía hablando de DNSSEC, ya para los años entre 2005 y 2010 se convierte en estándar, comienza a ser adoptados por muchos TLD por muchas instituciones, pero, aun así, DNSSEC sigue teniendo retos, grandes retos. Por ejemplo, la adopción e implementación de DNSSEC por ccTLD, por ISP y otras instituciones, es muy lenta en Latinoamérica y en África, por ejemplo.

Estudios identifican retos financieros asociados a la implementación de DNSSEC. Y, volvemos, estos retos financieros han sido para yo implementar DNSSEC, requiere que contrate personal nuevo. Si la respuesta es sí porque usted quiere hacer esto en casa (inhouse), ¿no? Quiere hacerlo en su organización, no quiere contratar estos servicios; es muy posible que tenga que contratar nuevo personal.

El DNSSEC no es algo que... Y se están haciendo grandes esfuerzos para proveer webinars, proveer talleres y demás, diseminar la información de cómo implementar DNSSEC, pero, aun así, sigue siendo complicado y tiende a ser un poco costoso porque si requiere que yo contrate a alguien nuevo, mi nómina está aumentando. Si mi nómina está aumentando pues tengo ahora retos de cómo producir más.

Además, es muy posible que la persona que contrate, aunque tenga un perfil técnico suficientemente bueno, es muy posible que necesite adiestramiento especial sobre DNSSEC y sobre otras soluciones relacionadas al DNSSEC para asegurar de que pueda, no solamente implementar el DNSSEC en esa organización, pero que también lo pueda mantener.

Y eso requiere adiestramiento, el adiestramiento usualmente requiere desplazarse a algún país aun cuando es dentro del mismo Suramérica o del mismo Latinoamérica hay un costo que está involucrado en ese desplace y entonces puede también ir buscando hotel, el desplace y todo ese tipo de cosas que les puede costar muchísimo.

Entonces esos pueden ser algunos de esos retos y eso ha fomentado un poco esa resistencia. Próximo slide, por favor. Para aquellos de ustedes que se pregunten: “Pero bueno, mi banco tiene DNSSEC, ¿cómo pudiera saber yo si mi banco tiene DNSSEC o no? Pues pueden tomar una foto de esto o pueden... Estoy seguro que esta presentación estará disponible y puede ir aquí y escribir el nombre del dominio del cual quieren asegurarse si tiene el DNSSEC o no, y con estas herramientas lo van a poder saber. Traten con el mío rodriguez.pr y ahí van a ver cómo se ve un dominio que tiene DNSSEC y luego comparen con otros a ver si se ve igual.

Finalmente, protéjase adoptando buenas medidas de seguridad, no use computadoras públicas o no seguras, identifique quién le está hablando o quién le está escribiendo antes de responder, instalen software que tengan antivirus que lo protejan del spyware y... Próximo slide, por favor.

Parte de eso... Próximo slide, por favor. ¿Cómo yo pudiera saber quién me está escribiendo y quién no? Aquí les doy un ejemplo, un banco muy famoso en Puerto Rico es popular.com, pero noten que le pongo un, no es igual a, y pareciera que dice pOpular.com, pero eso es un cero, no es una “O”. Entonces “ojo” cero y la “O” son usados a veces para cometer

fraudes, hacerse pasar a simple vista así cuando uno mira apurado parece que es la misma cosa, pero no lo es.

El uno (1) y la ele (l) minúscula parecieran ser lo mismo, entonces asegúrense de que quién le está hablando, quién le esté enviando un correo... Y estas son algunas maneras de cómo usted puede ayudar a protegerse a usted mismo, a diseminar esta información de cómo otros pueden protegerse y, a la misma vez, de convertirse en embajadores, de hablar con sus instituciones para que, si no tienen DNSSEC implementen DNSSEC se protejan a sí mismos y a sus usuarios.

Muchísimas gracias por esta oportunidad, ha sido un gran honor y un gran placer poder compartir o de compartir con todos ustedes en esta noche, muchas gracias.

AUGUSTO HO:

Muchísimas gracias, Dr. Pablo Rodríguez, que reiteramos vicepresidente del NIC PR y por su didáctica conferencia impregnada de academia y de sapiencia, ¿no? Todos hemos estado muy atentos a esta conferencia, y muchísimas gracias por su tiempo Dr. Voy a solicitarle a Harold por favor que si hay preguntas en el chat las formule, adelante, Harold.

HAROLD ARCOS:

Estamos revisando Augusto, por ahora no tenemos preguntas, pero sí tenemos algunas manos levantadas, la primera de ellas es de Alejandro Pisanty, entonces les iremos informando cuando vayan levantando las manos o alguna otra pregunta. Adelante.

ALEJANDRO PISANTY:

Gracias y muchas gracias por esta estupenda presentación, dos puntos. Uno, es cierto que no se previeron todos los ataques posibles en el diseño del DNS, en el Sistema de Nombres de Dominios. Repito, felicitaciones y gracias por esta estupenda presentación.

Pero quizás sea un poco excesivo hablar de inocencia en los diseños y daños originales de internet, debemos recordar que se estaban conectando computadoras que tenían los mayores secretos de Estados, los mayores secretos científicos-tecnológicos y los mayores secretos comerciales, desde la nómina de pago de la General Motors o de [Inaudible] hasta investigaciones básicas en las universidades.

Y los diseñadores, los autores de los protocolos iniciales pidieron concentrar la seguridad en la orilla, la criptografía, por ejemplo, estaba avanzando a una velocidad extraordinaria hace unos años cuando se creó precisamente el KPI o criptografía simétrica y la llave pública que fue descrita en la presentación.

Y tanto las matemáticas como la computación, la diversidad de las computadoras haciendo imposible mantener los protocolos en la COR de la red, de manera que eso dio lugar al principio de inteligencia en la orilla, el principio de Postel, el mismo que diseñó junto con Mocafo el DNS. Entonces hay una decisión deliberada no de ignorar la seguridad, sino de remitirla a la orilla y solo años más tarde empieza a haber ataques contra la seguridad también en el COR de la red como el Sistema de Nombres de Dominios.

Hay que recordar que el DNS está en la capa de aplicación como a los sistemas operativos y a los protocolos mismos de los equipos que están en el intermedio estarán, nota uno. Y la nota dos, que no le quita merito

a las aplicaciones lo sigo aplaudiendo, pero es importante mantenernos visitando esta construcción errónea.

Y segundo, es muy importante para las organizaciones de LACRALO mantener a nuestro alrededor una cultura en la cual se hagan preguntas acerca de la seguridad en general, en la que seamos capaces de llevar a la gente más técnica de la organización, cuando hablamos de nuestra propia organización, pues a alguien como nuestro exponente de hoy para discutir con los ccTLD y con los principales puntos de contacto para nosotros, con instituciones como universidades, banca, los ISP y los proveedores, o sea para mí serían ONG de la Sociedad Civil.

Es muy importante proteger nuestros propios servicios web a través de quienes nos proveen ese alojamiento o servicio. Gracias.

AUGUSTO HO: Adelante, Harold. ¿Va a leer una pregunta o alguien que esté...?

HAROLD ARCOS: Vamos a proceder a leer la pregunta que colocó Gerardo, disculpa que no le había visto a usted. Gerardo pregunta: “De acuerdo con el ejemplo del invierno, las posibles soluciones de un problema complejo con respecto al DNSSEC, ¿lo mejor sería entonces trabajar de forma indisciplinaria?” Esta es la pregunta para el Dr. Pablo.

PABLO RODRÍGUEZ: Harold, déjame repetir para ver si escuché apropiadamente porque había un poquito de ruido. Creo que me preguntaste o la pregunta es, si

dada la naturaleza compleja del DNSSEC, ¿es mejor trabajar eso desde una perspectiva multidisciplinaria? ¿Esa es la pregunta?

HAROLD ARCOS: Sí, de acuerdo con el ejemplo del invierno, las posibles soluciones sería afrontarlo de forma interdisciplinaria, sí, básicamente es eso.

PABLO RODRÍGUEZ: Existen muchos problemas complejos en distintas situaciones, en distintas industrias y en distintas disciplinas, el DNSSEC es una que, por su naturaleza, una y otra vez necesita de... Y nuestra industria lo hace, es la de aportar una cantidad de soluciones. En los problemas complejos hay un dicho que dice: "No existe una bala de plata que lo resuelva todo".

Entonces no puedes controlar 100% a la bestia, solamente puedes bailar con ella, entonces tienes que adaptarte según va evolucionando esto. Una respuesta es que, según van los distintos académicos, investigadores y desarrolladores, buscando soluciones a otras vulnerabilidades dado el camino que ya DNSSEC aplanó para que otros puedan construir encima de ese y puedan crear otros protocolos que puedan ayudar a fomentar una solución más amplia.

Así que, siempre el trabajo multidisciplinario es importante y nos ayuda muchísimo, así que la respuesta corta es sí, siempre los equipo multidisciplinarios los van a ayudar. Pero, en este caso, también tenemos que tener en cuenta que una y otra vez van a suceder elementos que hemos provisto y por eso causa el que años más tarde

tengamos que buscar soluciones a una o varias de esas soluciones que en su momento era lo mejor que teníamos.

AUGUSTO HO: Harold, ¿tenemos algo más?

HAROLD ARCOS: Augusto, estoy viendo por acá por el chat y no tenemos nada, estoy verificando que no se me haya pasado alguna otra como la de Gerardo al inicio. No, no tenemos ninguna y tampoco tenemos manos levantadas, Adelante, entonces Augusto.

AUGUSTO HO: Ok. Siguiendo con la agenda el día de hoy, entonces tenemos para efectos de comentarios de los ALAC member a Sylvia Herlein, por favor Sylvia va a contar con 5 minutos, ¿sí?

SYLVIA HERLEIN-LEITE: Hola, ¿me escuchan?

AUGUSTO HO: Adelante, Sylvia, te escuchamos.

SYLVIA HERLEIN-LEITE: Hola, buenas noches. Bueno, brevemente les quería hacer un comentario de lo que se estuvo trabajando este último mes con la gente de ALAC, pero antes de empezar quiero realmente comentarles como siempre, como ustedes ya saben, que las reuniones son abiertas a toda

la comunidad, no solamente a los ALAC members, entonces siempre es bueno recordarles que pueden participar y es bueno que participen porque siempre estamos abiertos a todos los comentarios.

En el mes de marzo hemos tenido que votar en varias recomendaciones que hizo el ALAC, una de ellas es la que tiene que ver con la IANA, que fue la recomendación para una enmienda del contrato de función de nombres de la IANA y voté que sí, ¿no? Todas las votaciones que hice en realidad voté que sí porque uno va acompañando todo el proceso y, en realidad, cuando uno vota es solamente definir y apoyar todo el gran trabajo que vienen haciendo los que trabajan en estos grupos.

Entonces, en realidad, es cuando uno tiene alguna inquietud o alguna duda lo bueno es hacerlo antes, entonces es por eso que incluso también les comento sobre la participación de todos. Después hicimos una declaración, es sobre la directiva de la unidad económica europea sobre la seguridad de las redes y los sistemas de información que se llama por la sigla NIS2, creo que Harold iba a poner el link de esto que les estoy comentando a ustedes, por si alguien le interesa el tema y quiere saber más.

También hicimos la ratificación del informe del grupo de trabajo sobre la movilización de personas no aplicadas, o sea de los participantes individuales. Se hizo también la revisión del informe final del SSR2, que como ustedes saben las siglas ya se hicieron famosas, sobre seguridad, estabilidad y resiliencia.

Y lo último que fue votado en ALAC fue el asesoramiento de ALAC a la Junta sobre los requerimientos superiores o subsecuentes, eso es lo que fue votado en sí entre marzo y abril, y hay varios temas que están

abiertos que aún hay tiempo de participar, yo lo estoy consiguiendo visualizar, pero no sé si Harold puso en el link para que ustedes vean todo lo que está siendo tratado en ALAC. Muchísimas gracias.

AUGUSTO HO:

Muchísimas gracias, Sylvia, por la presentación. Vamos ahora a pasar a los informes de directores y, no sin antes darle la bienvenida a Sergio que ya está por acá acompañándonos, gracias, Sergio. Continúa acá entonces para el informe de directores, cada uno de ellos va a tener un máximo o un promedio entre 3 a 4 minutos para exponer, el primer grupo va a ser el de IDN, Aceptación Universal, va a estar Sylvia Herlein nuevamente conversándonos sobre este tema o dándonos el informe respectivo. Adelante, Sylvia, ¿creo que es así?

SYLVIA HERLEIN-LEITE:

Ok, gracias. Bueno, con respecto a mi grupo de trabajo ustedes saben que tenemos dos subgrupos, el de IDN propiamente dicho, que el año pasado hemos hecho un trabajo muy interesante y diferente a todo lo que ya se había hecho, y que este año lo vamos a retomar de forma particular. Mañana incluso tenemos reunión del grupo de trabajo y nuestra idea es entrar en contacto con todos los .NIC de Latinoamérica y El Caribe para presentarles el informe, el resumen, que habíamos hecho y que nosotros intentamos transmitírselos a través de LACTLD y no fue posible.

Entonces eso es lo que vamos a organizar mañana para trabajar eso de forma firme y no desaprovechar todos los esfuerzos que tuvimos el año pasado porque realmente el informe fue muy buen preparado por

Gabriela [Sisgon], entonces queremos seguir trabajando en pos del IDN, estamos en la etapa de entender cómo funciona, queremos hablar con los ccTLD para que nos cuenten cómo es todo el proceso, cómo funciona, por qué algunos ccTLD admiten caracteres, por ejemplo, como la “Ñ” y otros no.

Entonces queremos entender eso para incluso pasárselo a nuestros representados. Y, por el otro lado, con el tema de Aceptación Universal estamos muy contentos, felices porque desde julio del año pasado venimos trabajando realmente muy arduamente y ahora estamos viendo nuestro trabajo florecer. Está confirmado el curso para técnicos, programadores, estudiantes de TI, creo que iban a poner en el chat los flyers, tenemos flyers en inglés, en portugués y en español.

Tenemos cinco profesores muy respetados en el tema que van a participar, el curso va a empezar el 04 de mayo, ahí veo que están poniendo nuestra página Wiki para que vean los detalles, para que puedan saber quiénes son los profesores. Van a ser cuatro sesiones de una hora y media, se va a dar en español oficialmente y con traducción simultánea al inglés.

Y ya tenemos como 60 inscritos porque estamos haciendo realmente junto con Marcelo Rodríguez del grupo de comunicación y Adrián Carballo de capacidades, una cosa inédita, no me canso de repetirlo. Entre muchos conseguimos hacer algo fantástico y eso nos va a llevar a poner como un ejemplo y es una modalidad diferente de trabajo y también podemos llamar o invitar de lo que estamos haciendo a todas las otras RALO para que participen en este primer curso de Aceptación Universal.

Estamos trabajando arduamente para fomentar esto, hemos recibido comentarios de estudiantes de la UBA, de la Universidad de Buenos Aires, que les interesaba el tema, pero que no sabían de qué se trataba, ni para qué servía. Y también hemos recibido inscripciones de personas que son programadores de Java o de otras cosas.

Pero a lo que me refiero es que, estamos realmente haciendo una cosa importante en el fomento de la educación y en saber qué es esto de la Aceptación Universal, y entonces por más que las personas no sepan de qué se trata, si tienen algún conocimiento mínimo de programación van a poder participar en este curso.

Y que quede claro que en julio vamos a tener un curso para usuarios finales en donde todos los miembros de nuestras ALS serán realmente invitados a participar, lo que sí estamos pidiéndoles ahora a nuestras ALS es que, por favor nos ayuden a divulgar esto porque va a ser único y la idea es repetirlo obviamente, pero no sabemos cuándo, entonces estamos a mitad de abril y tenemos hasta el 03 o 04 de mayo para que se inscriban.

Entonces les voy a pedir por favor que copien la información que están viendo en el chat y que nos ayuden a difundir esto, que realmente creo que va a valer la pena y va a ser una cosa icónica para nuestra región, para LACRALO. Así que estoy a disposición si tienen alguna pregunta, alguna duda, pero termino por aquí que sé que estamos cortos de tiempo. Muchísimas gracias.

AUGUSTO HO: Muchísimas gracias, Sylvia. Vamos a darle la palabra a Adrián Carballo del grupo de capacitación, Adrián estamos bien apretaditos de tiempo, así que vamos directo al informe, ¿sí? Gracias.

ADRIÁN CARBALLO: Te agradezco muchísimo las palabras. En primer lugar, quisiera decirle al Dr. Pablo Rodríguez por su excelente presentación, totalmente creo que nos ha dado a todos mucho más allá de lo que uno esperaba de estos temas, que siempre, digamos, es muchísimo pretender y me consta de todo el trabajo que ha llevado él personalmente adelante para poder tener este conocimiento y poder hacer esta transferencia de conocimientos justamente, así que gracias, Pablo.

Respecto del grupo, les quiero comentar que seguimos avanzando con lo que es ICANN Academy en español, no hay mucho tiempo, pero sí quisiera comentarles brevemente, digamos, el contenido del programa inicial del desarrollo de esta capacitación que va a constar de cuatro módulos. Solamente voy a enumerar los cuatro títulos que, en este caso, serían ecosistema de internet e ICANN, el número dos, el Sistema de Nombres de Dominios y su estructura, el módulo tres, seguridad, resiliencia y privacidad.

El módulo cuatro, internet y su impacto en la sociedad y en la economía. Los avances que tenemos del proyecto en este momento, luego pasarlo a Heidi también del staff, cosa que lo puedan tener también en la Wiki y lo puedan ver en detalle.

No quisiera dejar de lado también, como recién nombraba Sylvia Herlein, el avance que hemos tenido con el curso de Aceptación

Universal. Realmente hemos trabajado los tres grupos como equipo muy bien y estamos con una gran expectativa con este curso que se va a dar en principio para los técnicos y luego que será para los usuarios finales.

También quisiera pedirles de manera especial que nos puedan ayudar con el tema de la difusión de este curso, que pueden encontrarlo tanto en Facebook como en Twitter como para poder capitalizar la mayor cantidad de gente que esté interesada y que pueda sumarse. Y, por otro lado, que al igual que hoy estamos armando un cronograma de actividades junto con el grupo del GSE de distintos webinars, que se irán sumando en la continuidad de las reuniones mensuales de las RALO.

Así que por el momento este sería mi informe y cualquier consulta estoy a disposición, muchas gracias.

AUGUSTO HO:

Muchísimas gracias, Adrián. Vamos a darle la palabra rápidamente para que dé su informe a Carlos Aguirre, ¿sí? Para el grupo de GDPR, tiene unos 3 minutos Carlos, adelante.

CARLOS AGUIRRE:

Gracias, Augusto. No quiero dejar pasar la oportunidad para felicitar, también como lo hizo Adrián y como lo hizo Sylvia, la presentación de Pablo fue decididamente espectacular con una focalidad y una capacidad increíble, así que te felicito Pablo. Se entiende muy bien cada cosa que explicas.

Pasando directamente a lo que es este grupo WHOIS & GDPR debo decir que bueno, nosotros hemos hecho un llamado a este grupo hace poco

tiempo, estaba conformado ya desde hace algún tiempo atrás y hoy estamos pidiendo la participación, sumando participación. Nos ofrecieron desde la presidencia de LACRALO colaborarnos con este tema, estamos generando los contactos para ver la incorporación de miembros a este grupo.

Y, por otro lado, estamos trabajando también, ya hemos pedido colaboración al director del grupo de capacitación a los fines que nos provean algún referente en la materia de poder generar un webinar y ojalá sea tan claro como lo hizo Pablo en su exposición recién, porque la idea es justamente entender de qué se trata esto, son cuestiones para nosotros muy sensibles, el tema de la protección de los datos personales en el WHOIS.

Y, sin lugar a dudas, debe tener una relevancia trascendental y por eso queremos mostrar o explicar de qué se trata esta cuestión, simplemente para hacer una pequeña reseña. El reglamento de protección de datos o GDPR fue aprobado por la Unión Europea en abril de 2016 y entra en vigor el 25 de mayo de 2018.

ICANN trabajó durante 2017 para adecuarse a esto que se venía y en abril de 2018, antes de que saliera la resolución que ponía en vigencia el General Data Protection Regulation de la Unión Europea, saca una especificación temporal para los datos de registración de los gTLD y que se ha vuelto a ratificar a principios de 2019.

Estos temas requieren de una upload, de una actualización que debe ser permanente porque obviamente, como decía Pablo también en su presentación, aquellos que se dedican al fraude o a trabajar con los datos para generar algún tipo de delito están a la orden del día y

entonces esta es una medida que debemos permanentemente estar atentos y estudiarlas.

Pero lo más importante y que a esto va apuntado la cuestión, es hacer entender de qué se trata esto, por qué es importante y, como les decía, estamos en la conformación del grupo, en el reclutamiento de todos los que estén interesados en participar y juntamente con el grupo de capacitación buscando a alguien que nos pueda dar un webinar claro, para dar el puntapié inicial en esta cuestión.

Esto es lo que estamos haciendo, esto es lo que estamos generando, todavía estamos en el principio de este curso, pero con muchas ganas de seguir adelante porque entendemos que este es un tema central en la discusión y no debe pasarse por alto, fundamentalmente por los usuarios de internet porque tiene muchísima relevancia para ellos. Esto es todo lo que puedo decir, Augusto, muchísimas gracias.

AUGUSTO HO:

Gracias a ti Carlos. Vamos rápidamente a darle la palabra al grupo de trabajo de comunicación, le vamos a pedir a Marcelo Rodríguez que está por acá para que nos dé su informe brevemente, por favor.

MARCELO RODRÍGUEZ:

Hola, ¿qué tal? Muy buenas noches, ¿cómo están ustedes? Aquí bueno, con los tiempos acotados, pero agradeciendo el poder participar y estar también, la posibilidad de estar aquí. El trabajo que se viene realizando en el ámbito de la comunicación estuvimos bastante atareados terminando de poder hacer entregas para su distribución, más luego

cuando ya se haga la traducción al inglés de lo que es LACRALO News número 2, así que ya hasta allí entregado el material para ser traducido.

Con mucho placer, ¿no? Y agradeciendo la participación principalmente de Sergio, de Franco y también de integrantes del grupo de comunicación que fueron dando sus aportes, y por los aportes de cada uno de ustedes también que allí tienen. Los aportes hicieron mucho hincapié, principalmente en la información regional reciente que se fue dando, relacionado con lo que tiene que ver con la infinidad en ICANN70.

Y luego, también las notas relacionadas en cómo es cada uno de sus participantes, ¿no? Acá me está diciendo Sylvia que lo envié, ya fue enviado el Word con el documento completo, así que esperamos tener prontamente esto en cada una de las casillas para su distribución.

Acerca del curso de Aceptación Universal, también allí estamos participando junto con Sylvia y con Adrián en cada de los grupos que fueron parte de esta actividad que nos llevó varias reuniones poder concretarla y también agradecemos el diseño que nos acercó también Sergio y que bueno, lo único que se cambió en sí creo que fue la fecha de inicio, el resto está todo difundido, más que claro, así que no queda más nada por agregar.

Agradezco muchísimo la posibilidad de continuar junto con ustedes en este equipo, también la posibilidad de tener el trabajo del grupo de comunicación, bueno, lo que se pueda desarrollar durante todo el año 2021, a pesar de las restricciones que tenemos. Saludos a todos ustedes, cuídense mucho, estamos en contacto.

AUGUSTO HO: Muchísimas gracias, Marcelo. Y si no me equivoco, debo dar ahora una actualización regional, voy a empezar por decir que en función de ICANN70, pues es la primera vez que se hizo una asamblea virtual bajo los nuevos procedimientos de ICANN, ¿verdad?

Básicamente tuvimos cuatro eventos para esa época, el primero fue una semana previa a ICANN70 donde específicamente el día 15 de marzo hubo una Asamblea General Virtual, posteriormente el 17 de marzo hubo una jornada de capacitación con David Plumb, que habló sobre el fortalecimiento de LACRALO para participar en esas reuniones políticas de ICANN y se habló también de la Aceptación Universal.

Fue un evento exitoso, muy bien recibido por todos y muy aplaudido. En tercer lugar, en la misma semana de ICANN70 tuvimos mesa redonda, se habló sobre los planes estratégicos de la región América Latina y El Caribe 2021-2025 y una mirada al futuro. Y, finalmente, en este informe breve quiero finalizar haciendo una especial mención al evento social con el que se finalizó ICANN70, fue exitoso y agradecimientos desde ya a todos los que participaron en la organización y a los que participaron también en este evento social.

Fue muy apreciado por el directorio. Hubo un tour por las regiones, arriba de 200 personas estuvieron conectadas en ese momento, muy aplaudido este evento social con la participación del ballet folclórico Nuevo Sol de la Península de Yucatán. Sergio Salinas, si está por aquí le voy a ceder la palabra para que nos acompañe, en vista de que ha llegado hace unos minutos, adelante Sergio.

SERGIO SALINAS PORTO: Gracias, Augusto. Creo que me toca el último tema a desarrollar, que es el tema de elecciones de LACRALO, pido disculpas por no haber podido estar antes, pero hoy tuve complicaciones con la agenda.

Como ustedes saben, tenemos una elección el viernes, elección que implica básicamente todos los cargos, la mayoría de los cargos que tenemos en LACRALO. Tenemos una elección para ALAC member que Sylvia Herlein se va, que era de la región D, le toca a alguien de la región A.

Tenemos también elección de vicepresidente de LACRALO, quien va a sustituir a Augusto cuando termine su mandato allá en el 2023, pero aún tiene dos años de acompañamiento al presidente y de asumir, como hoy asumió algunas responsabilidades que tienen que ver con conducciones y decisiones dentro del directorio.

Tenemos también dos elecciones de subsecretario, vicesecretario y esto es porque renunció Kerry Kerr, entonces vamos a tener una elección por un corto plazo que va a ser de mayo a noviembre para cubrir ese cargo, que va a ser el del próximo secretario.

Y, por el otro lado, vamos a tener una elección de vicesecretario para el período 2021-2023, que luego en el 2023 junto con el vicepresidente electo, van a ser los presidentes y secretarios formalmente constituidos y también tenemos el delegado de ALAC al NomCom, pero como ustedes saben hay una grata costumbre de que el delegado de ALAC...

En este caso, nuestra querida amiga, Vanda Scartezini, a su vez, tiene la posibilidad de renovar su mandato y nosotros en nuestras reglas le

garantizamos de alguna forma esa prolongación de su mandato, en realidad, para que cumpla dos años en el mandato y no uno.

Dicho esto, y ya justo en horario, si hay alguien que tiene alguna consulta, pregunta o algo por el estilo, me la puede hacer por email, ahí veo que Harold puso todos los links que tiene que ver con nuestras elecciones. Las elecciones van a ser en mayo, no recuerdo bien el día.

Silvia, si lo puedes poner en el chat mejor, pero tenemos que pensar en una renovación de cargos, renovación que tenemos que estar pensando en ver... El 10 de mayo, ahí lo dice Silvia.

Y me gustaría darle la palabra, que Alejandro tenía la mano levantada. Voy a cerrar con esto, Alejandro tenía la mano levantada y si te parece bien, Augusto, que estás conduciendo la reunión, dejarle que plantee rápidamente esa actividad que no quedó registrada y que sería bueno que Alejandro lo plantee.

Así que, nada más, creo que no me olvidé de nada y si me olvidé de algo pido disculpas, pero el tiempo es tirano. Adelante, Alejandro.

ALEJANDRO PISANTY:

Es sumamente breve. Aparte de felicitarte, Sergio, por todo lo que ha presentado hoy y por la conducción de la reunión.

El informe que mencionó Silvia, lo del comentario de ALAC sobre la revisión de seguridad, estabilidad y resiliencia del Sistema de Nombres de Dominios, que es una de las obligaciones de ICANN, el SSR2 fue construido a partir de un borrador que escribí justo con Greg Shatan, es

una contribución que nos fue solicitada directamente por haber tenido yo la responsabilidad del primer review de este tipo.

Pero quiero que quede registrada también para los canales de LACRALO como una contribución frente la región. Gracias.

SERGIO SALINAS PORTO: Qué bueno eso, qué bueno que vayamos sumando estas cosas.

AUGUSTO HO: ¿Cerramos? Sergio.

SERGIO SALINAS PORTO: Augusto, solo una cosita y es para Alex. Alex, necesito verte en lo posible, mañana, necesito que nos encontremos en algún momento.

ALEJANDRO PISANTY: Claro, Sergio, ahorita por correo nos organizamos.

SERGIO SALINAS PORTO: Perfecto, gracias.

AUGUSTO HO: Si es todo, entonces yo creo que más nada está pendiente en la agenda y estamos un poquito excedidos de tiempo. Agradecer a todos los que participaron en esta reunión, al personal, a los traductores, etc. Muchísimas gracias por todo, muchísimas felicitaciones y muy buenas noches a todos.

SILVIA HERLEIN-LEITE: Gracias a todos. Abrazos.

SERGIO SALINAS PORTO: Chao compañeros.

AUGUSTO HO: Gracias, un fuerte abrazo para todos. Gracias, que sigan muy bien.

[FIN DE LA TRANSCRIPCIÓN]