ICANN85 Mumbai | Foro de la comunidad – De la estabilidad a la supervivencia: el rol de la ICANN en el futuro de la resiliencia de Internet
Lunes, 9 de marzo de 2026 – 10:45 a 12:00 IST

KATHY SCHNITT

Esta sesión se está grabando y se rige por el código de conducta para participantes de la comunidad de la ICANN, los estándares de comportamiento esperado de la ICANN así como por la política antiacoso de la ICANN. Hay interpretación en esta sesión en inglés, francés, español, chino, árabe, ruso e hindi.

Observen las siguientes directrices para participar en esta sesión. También las voy a publicar en el chat. Existen tres maneras de hacer preguntas. Si están aquí, en la sala, acudan al micrófono de la sala y esperen. Si están en línea, pueden enviar la pregunta al recuadro de preguntas. Voy a leer la pregunta en voz alta. Pueden levantar la mano para tomar la palabra directamente. Hay un icono abajo en la pantalla para unirse a la cola y le avisaremos cuando le toque. Si está en persona o en remoto, por favor, digan su nombre y el idioma en que van a hablar si no es el inglés. Hablen de una manera clara y a una velocidad razonable. Le voy a dar la palabra a Ram Mohan.

RAM MOHAN

Buenos días. Namaste. Bienvenidos a esta sesión plenaria. Soy Ram Mohan. Soy el presidente del Comité Asesor de Estabilidad y

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.

Seguridad de la ICANN. Viendo las calles de Mumbai, hay una clase maestra sobre la resiliencia. Esta ciudad no para nunca y no es porque las luces estén en verde sino que tiene una capacidad increíble de rutear a través de los obstáculos.

Internet es así. Hoy en día la resiliencia de Internet ya no es una cuestión de que los paquetes lleguen a su destino sino que tiene que ver con que el sistema de confianza que hace circular estos paquetes, que puedan sobrevivir a las tormentas que existen. No solo estamos hablando de ataques sino de dependencias ocultas, energía, proveedores de servicios en la nube. Dependemos de todos ellos pero no los controlamos.

Conforme vamos a un mundo que se basa en la IA y a la conectividad constante entender estas vulnerabilidades va a ser la diferencia entre que algo sea un problema menor o un apagón global. La resiliencia es la habilidad de mantener una fuente única de verdad, incluso cuando el mundo parece fragmentado.

Hoy no estamos aquí para hablar de la política. Estamos aquí para hablar de los nexos técnicos, los protocolos, la infraestructura y la estabilidad operativa que nos ayudan a sortear cualquier tormenta. Estamos hablando de que los sistemas de los cuales dependen miles de millones de personas día tras día para la comunicación, los servicios públicos y la seguridad, que sigan funcionando a pesar de las fallas técnicas, el aumento de la tensión geopolítica y el aumento en el número de ataques.

Tengo aquí a un distinguido panel. Antes de llegar al panel quiero

compartir con el público que queremos utilizar Mentimeter para que participen. Van a ver en la pantalla un código QR. Cuando lo vean, agarren el celular y escaneen ese código. Van a ver algunas preguntas. Nos encantaría oír su perspectiva sobre esas preguntas. Los aportes que nos brinden los vamos a ir compartiendo con ustedes conforme avance la sesión.

Fiona y yo estamos aquí con cinco panelistas. Danny McPherson. Dirige las organizaciones de tecnología y seguridad de VeriSign. Ha participado activamente en operaciones de Internet, investigación y estandarización desde principios de la década de los 90. Esto incluye estar en la junta de arquitectura de Internet y presidir una serie de comités y grupos de trabajo de ingeniería de Internet. Ha sido autor de varios libros y numerosas patentes, estándares de protocolo de Internet y publicaciones de investigación de redes y seguridad.

También está aquí Bruce Tonkin. Es el director ejecutivo de la administración de dominios .AU. Está en ese puesto desde 2017. Anterior a eso estuvo 18 años en Melbourne IT, que fue uno de los cinco primeros registradores de ICANN. Además, estuvo en la junta directiva de la ICANN durante nueve años y medio, de 2007 a 2016. Fue presidente de la DNSO/GNSO durante cinco años antes de eso.

También está aquí el señor M.A.K.P. Singh. Actualmente es el director de tecnologías en CyberPeace. Fue miembro y director de seguridad de la información en el Ministerio de Energía del

gobierno de la India. En el marco de ese puesto dirigió iniciativas clave en el marco de la transición energética y la ciberseguridad hasta su jubilación. Cuenta con más de tres décadas de experiencia en el sector energético de la India guiando el cambio hacia fuentes de energía no fósiles como la energía solar, la eólica o la hidroeléctrica.

También está aquí Dan York. Dan es el director sénior de confianza y seguridad en línea en la sociedad de Internet donde lidera el desarrollo de su centro de confianza y seguridad en línea. Participa en las comunidades técnicas como el IETF y aquí en ICANN es miembro del comité de programación para el Taller de Seguridad y las DNSSEC desde 2014. Está en línea desde los años 80 y es autor de múltiples libros sobre redes, seguridad, IPv6 y Linux. Como miembro del personal de la sociedad de Internet desde 2011 ha trabajado en una amplia gama de iniciativas. Entre ellas la resiliencia de Internet, los apagones de Internet, la ciudad del DNS, IPv6 y satélites de órbita terrestre baja.

Por último, tenemos a Paul Vixie. Diseñó, implementó y desplegó varios protocolos y extensiones de protocolos de nombres de dominio. Además de aplicaciones que se utilizan en Internet hoy en día, incluyendo las actualizaciones dinámicas, las reputaciones de Internet y software de código abierto. Fue miembro del SSAC y actualmente está en el RSSAC. Fiona, ¿puede presentarse, por favor?

FIONA ALEXANDER Hola a todos. Soy Fiona Alexander. Llevo muchos años participando en ICANN. Es un placer estar aquí con ustedes hoy.

RAM MOHAN Gracias. Los cimientos originales de Internet, el DNS, IPv4, BGP, consiguen que sigan en línea miles de millones de personas. No obstante, el entorno en que funcionan estos protocolos se ha visto transformado por completo. Vemos que hay interrupciones en Internet que son graves y generalizadas, que son causadas por fallas en los sistemas externos críticos en los que se basa Internet como redes eléctricas, plataformas en la nube y cadena de suministro de software complejas. El problema no es la fragilidad de los protocolos sino que parece ser que el entorno es frágil. Nos encontramos en un punto de inflexión.

Hoy no nos vamos a focalizar en cómo funciona Internet. No estamos aquí para debatir los estatutos o el mandato de la ICANN sino que estamos aquí para hablar de qué pasa cuando los sistemas centrales de Internet se rompen. Qué pasa cuando las aplicaciones de usuarios que están encima de estos cimientos se rompen. Fiona.

FIONA ALEXANDER Gracias, Ram. Vamos a dar un poco de contexto a la conversación de hoy. Ram, Dan, Danny y los otros, hemos estado implicados en un esfuerzo en el marco de la sociedad de Marconi de estudiar esta cuestión. Se estableció un grupo de trabajo sobre resiliencia

de Internet, un consejo asesor que aborda varias cuestiones y que organiza talleres para estudiar estos temas de cara al futuro.

En noviembre de 2025 hubo un taller. Esto fue el resultado de un esfuerzo colaborativo para abordar las vulnerabilidades críticas en un Internet global. Hubo trabajo también en la Academia de Ciencias en Washington D.C. y trabajo en línea. Se hizo un mapeo de la cadena de suministro de resiliencia de Internet.

Yo estuve implicada en esto. Hubo participación de los hiperescaladores. Los dos grupos de trabajo elaboraron una serie de informes y lo que concluimos es que la resiliencia debe ser algo fundacional como principio de diseño y no es algo secundario.

Si miramos los temas que se pusieron de manifiesto en el informe de la Sociedad Marconi y el informe SAC132, hay varios temas que queremos tratar. Las fallas energéticas, lo que significa esto para Internet, las fallas en cascada de los apagones en la nube, las fallas de las API y las intervenciones regulatorias y de política. Cada panelista va a tener tres minutos para hablar sobre estas cuestiones. Me gustaría pedirles que se atengan a esos tres minutos. Le doy la palabra a Danny para empezar.

DANNY MCPHERSON Voy a centrarme en la infraestructura central de Internet. Los protocolos principales que permiten que funcione Internet, el ruteo del DNS, que permite navegar en línea han demostrado ser muy robustos. No obstante, estos protocolos no se diseñaron

pensando en la seguridad sino que existía una confianza implícita porque la comunidad era bastante reducida.

Sabemos que el mundo ha cambiado. Hay muchos más operadores y estos protocolos y su infraestructura subyacente se actualizan en pos de la seguridad. Tenemos por ejemplo la RPKI, para mejorar el sistema de ruteo. Tenemos también las DNSSEC, para garantizar la integridad de los datos.

Esto hace que haya más espacio donde operan estos protocolos y además hay más puntos potenciales de falla. Hemos creado una paradoja. Los mecanismos diseñados para proteger Internet pueden crear más dependencias y traer problemas. Las mejoras en materia de seguridad previenen una catástrofe mayor pero tienen que implementarse de manera rigurosa.

Los protocolos fundacionales que subyacen estos sistemas deben prevenir las dependencias, incluyendo las dependencias circulares pero a veces son necesarias. Hay que crear protecciones en varios niveles del sistema para que el sistema en su conjunto pueda absorber choques en lugar de que caigan en cascada.

Pensando en el destino compartido, tengo que pensar en qué es lo que me importa, dónde reside, cómo se permite y cuáles son los controles necesarios para operarlo, cuáles son las amenazas que hay que mitigar.

FIONA ALEXANDER Danny, ¿puede hablar un poquito más despacio para los intérpretes, por favor?

DANNY MCPHERSON En cuanto a las operaciones de infraestructura, esto tiene que ver con los sistemas de ruteo que incluye la RPKI. Varios aspectos del hardware, la diversidad de las aplicaciones, la resiliencia de los sistemas, la agilidad y el control del acceso y los controles de implementación de los sistemas.

La infraestructura es cada vez más interconectada y más concentrada en entornos amplios. Esto quiere decir que hay más potencial de que se produzcan problemas. Los hiperescaladores y otros actores tienen ciertas dependencias. Todo esto se tiene que tener en cuenta. Es crítico que los operadores integren estos aspectos en sus cálculos y que estudien todos los escenarios potenciales. Esa fue mi declaración de apertura.

FIONA ALEXANDER Gracias, Danny. Pasemos a Paul Vixie.

PAUL VIXIE Hola. Vamos a hablar un poquito de la cadena de suministro de software. Internet pudo crearse a través de interdependencias de protocolos de software que eran creados en otros lugares. Mucha gente a la cual le interesaba ver que todo funcionara. Eso no es lo habitual. Cuando se desarrollan software y se ponen en Internet,

tiene que haber una motivación de lograr algo más.

La motivación era que estas dependencias comerciales de larga data siguen hasta hoy. Todos sabemos que el software tiene bugs, que todos los software los han tenido siempre y que se espera que siempre los tengan. No deja de ser un problema que cuando uno descarga software, ya sea de código abierto o una app telefónica, saber que tiene bugs. Uno no sabe dónde están pero en algún momento vendrán los parches. Hay toda una constelación de dispositivos donde se espera que se produzcan actualizaciones de software para reparar los defectos.

Es claro para todos nosotros que esto ocurre y tenemos que hablar al respecto porque la escala es lo que está haciendo que estos problemas de software requieran de los creadores que entiendan cuáles son los defectos en su operación y los resuelvan. Tenemos que ver de qué manera estos defectos están relacionados con la seguridad. Es algo que se ha publicado mucho. Sabemos que hay muchos que utilizarán esto para realizar ataques y tenemos que ocuparnos antes de que los ataques ocurran. Es un problema terrible.

Yo le diría a esta gente que se ocupa de esto que el libertarianismo hace tiempo que está en la cultura de Internet. A veces las soluciones que se publican generan más problemas. Es por la naturaleza de que no existe una relación contractual en estas interdependencias.

El software puede propagarse a través de las vías de la Internet,

donde algunos bundlers, es decir, otras redes de aplicaciones, incluido nuestro propio software, está dentro de otra cosa. Si no sabemos quiénes son, no sabemos quiénes son nuestros clientes y ese es un problema.

Veámoslo desde el lado opuesto. Si nosotros dependemos del software de código abierto, no estoy hablando del teléfono o de la laptop. Estamos pensando en un contexto empresarial típico donde se necesita que funcione para que la compañía haga las cosas bien.

RAM MOHAN Gracias, Paul. Le voy a pedir a los presentes que escaneen el código QR. Las respuestas son anónimas. No quedarán almacenadas en la app. Por favor, con el teléfono lean la pregunta, mientras pasamos al siguiente panelista, el señor Singh.

M.A.K.P. SINGH Soy del sector de la energía. Quiero relacionar lo que se dijo con la seguridad de la red eléctrica. Necesitamos electricidad para operar los enrutadores y necesitamos enrutadores para operar la red eléctrica. Ambos son interdependientes. En la India tenemos varios sectores críticos que son interdependientes. El sector energético es uno de estos sectores críticos. En Estados Unidos tienen 16. En la India hay siete.

Si el sector energético falla, otros rápidamente tienen dificultades. Un ejemplo es el apagón en Estados Unidos y Canadá

del 2023. Fue manejable pero generó un colapso. Las torres de teléfonos móviles cayeron, los centros de cómputo. Ese tipo de impacto genera muchas instancias que se repercuten en otros impactos de red. Hay sistemas que no pueden funcionar, los centros de computación y los servidores consumen mucha energía, generan calor y, si no hay refrigeración, se apaga automáticamente el equipo para evitar un problema de apagón. Eso impide que funcionen los servicios de nube y el enrutamiento de Internet.

KATHY SCHNITT Vamos a solicitarle que hable un poco más despacio.

M.A.K.P. SINGH Los atacantes generaron ataques en las líneas terrestres eléctricas en Ucrania como un ciberataque. En el 2012 hubo un apagón en la India. Requerimos que cada instalación del sector eléctrico tuviera teléfonos satelitales para permitir la restauración de la red.

Del otro lado, cuando pasa un fallo de red, también hay fallos eléctricos. Las plantas eléctricas dependen de las comunicaciones que dependen también de la electricidad. Una única falla puede generar una cascada de fallos generando fallos diseminados.

Lo que pasa es que tenemos muchos dispositivos que operan en la Internet y aunque no sea una Internet pública, aunque sea privada, dispositivos IoT, necesitan la red eléctrica porque

detectan los parámetros sobre los operadores para saber en qué red operan. Esta visibilidad deja de estar, estos parámetros.

Tenemos instalaciones remotas pero en caso de un fallo energético no podemos operar nuestras redes remotamente tampoco. Eso es una causa de fallo eléctrico en caso de fallo de red. En el 2003 hubo un fallo, un apagón en el noreste que terminó en una crisis internacional masiva que afectó a 50 millones de personas.

Actualmente las empresas de servicios adoptan cada vez más los abordajes de manejo de eventos de crisis que utilizan las empresas de sistemas. Las comunicaciones por Internet deben existir y dependen de la red eléctrica. También están los aspectos de ciberseguridad. Hay muchos sistemas heredados que utilizan tecnología avanzada también. Como todo está interrelacionado, no podemos operar las redes en ciego. Tenemos que mantenerla segura y para que la infraestructura crítica esté segura necesitamos que la red eléctrica funcione. Eso es todo.

FIONA ALEXANDER Muchas gracias, señor Singh. Creo que nuestro próximo orador es Bruce Tonkin.

BRUCE TONKIN Voy a dar la perspectiva de .AU, de Australia. El DNS, el sistema de nombres, se trata quizá igual que una línea aérea. Es una infraestructura crítica al igual que las redes de agua de

telecomunicaciones y eléctrica en mi país. Hay una tendencia en algunos países desarrollados, incluido Australia, para crear roles específicos para manejar estos sistemas de la misma manera que se protege el agua o la electricidad.

Según la legislación australiana, en .AU tenemos que adoptar un abordaje de riesgos para manejar estos problemas. La ciberseguridad, hemos hablado en las reuniones de ICANN, es un riesgo pero también lo es el personal. Una persona, de manera maliciosa, puede dañar una infraestructura o quizá un error humano. La cadena de abastecimiento se ve cada vez más como un riesgo. Presenta sus peligros físicos o naturales.

Cuando existen desastres que pueden ser naturales, incendios, terremotos, huracanes, pandemias o generados por el ser humano como resultado de guerras o cibertecnología por parte de organizaciones criminales, cuando esto afecta partes de la infraestructura crítica en manera simultánea, aunque no solo afecte la red eléctrica, todo se ve afectado de la misma forma. Hay una mayor conciencia de estas dependencias entre las industrias interdependientes. Tenemos que usar proveedores comunes.

Las industrias utilizan, por ejemplo, los servicios web de nube de Amazon Web. Utilizamos software común, como dijo el señor Singh. Hay un estudio reciente del año pasado de CrowdStrike que vio que se afectaron partes críticos en la infraestructura al mismo tiempo. Hay una mayor conciencia de esta necesidad de analizar la cadena de abastecimiento tanto en términos de la

ciberseguridad como de sus interdependencias para asegurar tener una infraestructura realmente diversa y resiliente.

Otro aspecto es que nunca se puede predecir exactamente lo que va a suceder, qué desastres. Tenemos que practicar la restauración de los servicios para cuando ocurran estos desastres. Estas son prácticas no solo al interior de las organizaciones sino en otros elementos de la cadena de suministro. Fiona, le devuelvo la palabra.

FIONA ALEXANDER Gracias, Bruce. Concluimos con Dan.

DAN YORK Saludos y gracias a todos ustedes por organizar este panel en ICANN. Este es un momento crítico para la resiliencia. Es un momento crítico para pensar en la resiliencia pero yo quiero dar una orientación diferente un poquito. En Sierra Leona en este momento hay un contenedor de 40 pies montado sobre un camión que viaja por el país cambiando la vida de mujeres y niñas, que es parte de un proyecto que se llama Digi Truck Salon. Brinda capacitación, información a las personas. Muchas de ellas usan Internet por primera vez. Hace capacitación, mentoría y es un éxito.

Hay una mujer que transforma, genera calzado para publicitarse. Otra mujer, Mary, que es sastre, aprendió cómo comercializar sus diseños y de manera orgullosa modela sus creaciones en vídeo.

Tiene un negocio por WhatsApp y hay muchos casos como estos.

El DNS brinda servicios que les permite continuar brindando servicios a personas como estas. Por eso hablamos de resiliencia de Internet. La ICANN tiene un rol crítico en garantizar la resiliencia y operación continuada del ecosistema en el DNS y los identificadores únicos.

Cuando vemos en profundidad la resiliencia, vemos que la ICANN y la organización en África y en Asia-Pacífico tiene un índice, como muestra Internet Society, que tienen un puntaje de 30 a 40 en un rango de 100. Esto significa que ya están operando en una infraestructura frágil, que a veces está al borde del fallo, cuando la Internet cae en cualquier economía no solo es una disrupción de los servicios.

También corta los medios de subsistencia de las personas, el gobierno, el acceso a la salud. Ya no hay alternativas. Tenemos que ir a sistemas de infraestructura pública digital más generalizados, más servicios que aumenten la dependencia. También podemos aprender de las economías emergentes en este sentido. Estamos hablando de los cortes masivos que tuvimos en distintos lugares.

Hace un par de años hubo un apagón documentado en Puerto Rico donde el 90 % de la infraestructura eléctrica se cayó. De hecho, llevó tiempo pero de alguna manera se recuperó. La gente en Puerto Rico se preguntó por qué. Qué fue lo que mantuvo las operaciones. La gente no dependía de la red eléctrica. Asumían

que en algún momento iba a fallar. Entonces había un acostumbramiento. Había resiliencia. Había baterías y sistemas de respaldo. Es la resiliencia personal. Paneles solares.

Los operadores de telecomunicaciones entonces tienen sus propios generadores y sus sistemas. Hay lecciones en la resiliencia que podemos aprender en todo el espacio. Esto es crítico que lo hagamos. También hay mucho que tenemos que hacer y pensar porque a veces la conectividad es difícil. No solo estamos perdiendo el sistema de operación sino también inversiones. Tenemos que hacer mucho, tanto en la comunidad de la ICANN como en la comunidad más amplia de Internet. La gente en el mundo tiene que tener acceso a una Internet resiliente.

FIONA ALEXANDER Muchas gracias. Le doy la palabra a Ram, para que presente la próxima parte de la sesión.

RAM MOHAN Muchas gracias, Fiona. Tenemos tres temas importantes para nuestros expertos. El aumento de la complejidad del sistema y la prevención con fondos insuficientes, las dependencias circulares y los riesgos de la cadena de suministro y, por último, el papel de la ICANN en la resiliencia de Internet.

Para empezar este debate, vamos a ver la escala de los sistemas que operamos hoy. Internet ya no es solo una serie de enrutadores y cables sino que es una red masiva de servicios en la

nube, de proveedores externos. Hemos oído hablar de esto hoy. Tenemos que hablar acerca de qué sucede cuando esta complejidad supera nuestra capacidad de gestionarla.

La primera pregunta entonces. Las aplicaciones modernas pueden depender de 30 a 40 API diferentes y servicios externos. ¿En qué momento la complejidad misma se convierte en la amenaza y quién debe asumir la responsabilidad de gestionarla? ¿Quién quiere contestar a esta pregunta? Adelante.

M.A.K.P. SINGH

Cuando hablamos de este número de API y de servicios externos que están disponibles y el mantener el sistema en línea estamos hablando de un problema particular porque no hay una sola persona que entienda qué pasa aquí. Estamos superando nuestras fronteras de confianza y a veces eso hace que no sepamos manejar estos escenarios.

Habló uno de los ponentes sobre CrowdStrike. El apagón de 2024 puso de manifiesto que el parche no se había probado y esto tuvo un impacto sobre, por ejemplo, los servicios de tarjetas de embarque y de otros servicios para los pasajeros. Todo esto nos ha demostrado que tenemos que reducir las dependencias sobre los servicios de proveedores externos y API. Gracias.

RAM MOHAN

Paul, ¿está de acuerdo con lo que ha dicho el señor Singh? Si está hablando, no le oímos. Ahora sí.

PAUL VIXIE

Quiero añadir que la complejidad tiene el mismo panel en los sistemas digitales que el calor tiene en los sistemas físicos. Es un subproducto. No es fácil deshacerse de él. Cuanto mayor es la escala, más nos vamos a regir por la norma de los números grandes. Se asume una manera de ver todo esto pero si sigue creciendo, los problemas van a ser cada vez mayores.

RAM MOHAN

¿No tiene nada que decir sobre esto, Bruce? Muy bien. Gracias. Siguiente pregunta. Los hiperescaladores tienen los recursos de la disciplina operativa para probar escenarios de falla de forma rutinaria. ¿Qué sucede, Danny, con el sistema en su conjunto cuando los operadores más pequeños de los que dependen no lo hacen?

DANNY MCPHERSON

Sí. Esto lo vimos con CrowdStrike. Un operador de software no pudo actualizar. Modificaron ciertos aspectos. No tengo mucha experiencia en esto y ocurren muchas cosas. Vemos que los hiperescaladores tienen una gran capacidad para manejar estos escenarios de apagones. No quiero culpar a nadie. Diría que hay operadores con menos recursos que no tienen la misma capacidad para realizar estas pruebas. Yo creo que todos tenemos la responsabilidad de mejorar y de desarrollar las mejores prácticas para diseñar los sistemas para que sean resilientes y

robustos para evitar consecuencias graves.

RAM MOHAN Dan ha seguido esto y hace tiempo que estudia la resiliencia de Internet. Ha estado involucrado en la operación de un índice. Desde su perspectiva, cuáles son los escenarios de falla que más le preocupan hoy día.

DAN YORK Internet solo es tan resiliente como su eslabón más débil. Eso puede ser a nivel nacional o un IXP por ejemplo con poco presupuesto. Lo que a mí no me deja dormir es la habilidad o la capacidad que tienen las organizaciones a nivel local para recuperarse y lidiar con estas cuestiones.

No entendemos muy bien esta cuestión de las dependencias. Esto lo dijo usted, Ron. Tenemos que ver cómo todo se conecta en su conjunto. Las rutas, los sistemas de pago, etc. Cómo se vincula todo este sistema porque tenemos que lidiar con esta complejidad. Una manera de hacer eso es ver cómo podemos mejorar las capacidades técnicas a nivel local. Cómo hacemos que surjan estas comunidades técnicas a nivel local, cómo podemos formar a las personas para que sigan contribuyendo a Internet.

Hemos visto los protocolos. Cómo se crean, etc. Además, hemos visto que las comunidades locales se recuperan antes de los apagones que el sistema global. A raíz de lo que ha dicho Danny,

existe una necesidad de crear y compartir buenas prácticas. Existe la necesidad de que haya personas en el campo que puedan ir a arreglar esa infraestructura de alguna manera. Eso sí que es importante.

RAM MOHAN Carlos, ¿tenemos los resultados de la primera encuesta de Mentimeter? ¿Cuál va a ser la principal causa de la próxima interrupción global? Mientras esperamos a Carlos voy a plantear otra pregunta al panel. Seguimos oyendo que la resiliencia es un problema de prevención y que la prevención no atrae dinero. Bruce, ¿quién en este ecosistema, el ecosistema de resiliencia, quién controla los presupuestos y qué haría falta, qué tendría que pasar para que los presupuestos se asignaran a la prevención en lugar de a la reacción?

BRUCE TONKIN Creo que una parte de eso es el poder explicar el riesgo porque sí que está el dinero disponible. Cuando se trata de la resiliencia, es importante explicar de manera clara cuáles son los riesgos y qué puede suceder y cómo ayudaría asignar más recursos a prevenir estos riesgos.

RAM MOHAN Gracias, Bruce.

M.A.K.P. SINGH

¿Puedo añadir algo? Cuando yo fui director de seguridad muchas veces se piden fondos para la ciberseguridad o la resiliencia. Lo que preguntaba la junta siempre, siempre quería tener más información sobre qué iba a suceder. Una empresa sufrió una pérdida de casi 2.000 millones de euros. Esta empresa fue Jaguar Land Rover. El gobierno británico tuvo que ayudar a esta empresa. Después se dieron cuenta de que tenían que haber invertido anteriormente para evitar sus problemas y garantizar la resiliencia de sus procesos de manufacturado. Tenemos que pasar de un modelo reactivo a un modelo proactivo.

RAM MOHAN

Carlos, supongo que vas a publicar los resultados cuando los tengas. Si aceptamos que la complejidad está superando nuestros presupuestos para la prevención tenemos que ver dónde reside esa complejidad y cada vez más los eslabones más débiles son los sistemas invisibles que se encuentran completamente fuera de nuestras propias redes. Fiona, le voy a pasar la palabra para que nos presente el segundo tema, las dependencias circulares y los riesgos.

FIONA ALEXANDER

Gracias. Como dijo en la primera sesión, quedó claro que existen dependencias circulares. Internet necesita que funcione bien la red eléctrica y la red eléctrica necesita Internet para recuperarse. Muchas veces el código abierto está enterrado en cinco capas de

software.

La primera pregunta es para el señor Singh. El apagón ibérico de 2025 nos mostró que las fallas de energía se convierten en fallas de Internet que se convierten en fallas de energía. ¿Sabe el sector energético que tiene un problema de Internet y la comunidad de Internet que tiene un problema de energía?

M.A.K.P. SINGH

Esta falla en la Península Ibérica afectó a casi 60 millones de personas. Es importante saber que esto tuvo que ver sobre todo con la generación de electricidad a partir de fuentes renovables. Cuando caen estas fuentes, la red no puede estabilizarse.

Si tenemos una capacidad importante de energías renovables, estas fallas pueden ocurrir. Es en ese momento que necesitamos de la infraestructura digital para tener más seguridad. En el caso de Portugal y España, cayó el tráfico de Internet en Portugal en un 90 %. En España fue menor. Esto es porque había más planes de contingencia. Si tenemos una fuente de energía de contingencia podemos recuperarnos antes y reinstaurar la infraestructura más rápido.

Hemos visto que muchos dispositivos necesitan una cantidad mínima de energía. Por ejemplo, cuando encendemos los interruptores de ciertos dispositivos necesitamos que la batería esté a un 75 %. Hay requisitos que son importantes y se deben tener en cuenta.

FIONA ALEXANDER Gracias. Los operadores de los ccTLD se encuentran en un punto crítico entre la política de la ICANN y la infraestructura nacional. ¿Cuán expuestos están los operadores de registro a los riesgos de la cadena de suministro?

BRUCE TONKIN Creo que es importante que los proveedores elaboren un mapeo de cómo se articula el sistema para saber cómo es el diseño físico de la red. He visto que en todas las organizaciones suele haber una o dos personas que entienden esta complejidad pero solo en su mente. Si se va esta persona, muchas veces toda esta información no está escrita.

No existe un plan de contingencia por lo que la clave para la infraestructura propia y también para la cadena de suministro es que se proporcione esta información. Un gráfico, por ejemplo, del sistema que quede constancia del plan de contingencia y que proporcionen copias de auditorías externas, por ejemplo. Una auditoría ISO y que se realicen ejercicios de ciberseguridad conjuntos para entender qué es y qué está en la cadena de suministro.

FIONA ALEXANDER Gracias, Bruce. Un mensaje clave aquí es que en nuestros sectores cuando se produce un fallo en cascada se genera vulnerabilidad. Tenemos que preguntarnos cuál es la función, el trabajo de la

ICANN y de su comunidad.

RAM MOHAN

Antes de esto, Carlos, no sé si estamos listos para la tercera encuesta. Tenemos otra pregunta. Le voy a pedir al público que tome el teléfono y escanee el código. La pregunta que estamos preguntando, cuando aparezca en pantalla, es: Si el proveedor principal de su país de la red eléctrica o de servicios de nube entrara en un fallo, ¿qué confianza tienen de que los servicios van a sobrevivir? Esa es la pregunta que va a aparecer en pantalla.

Mientras van contestando, entremos al último tema, que es la ICANN. No podemos nosotros arreglar las redes eléctricas ni arreglar las librerías de código abierto ni manejar los problemas geopolíticos pero colectivamente somos los que almacenamos el sistema de identificadores únicos de Internet.

De qué manera el mandato de la ICANN se cruza con la realidad de la fragilidad ambiental o del entorno que se observa tan claramente en el mundo a nuestro alrededor. Danny, ¿qué se necesitaría en realidad para que la fragilidad de los sistemas como RPKI o DNSSEC, sus problemas en cascada afecten a los servicios?

DANNY MCPHERSON

Creo que los protocolos de la DNS heredados y las prácticas operativas y los protocolos lo han hecho cada vez más seguro. Es un sistema robusto. Yo creo que el sistema de servidores raíz o las

operaciones, si consideramos el sistema de actividad y los registros de seguimiento del sistema, superan lo que ocurre con las operaciones en la nube.

El DNS ha tenido fallos pero, con la experiencia, se ha producido una higiene operativa básica. Hay algunos escenarios que podemos imaginar donde existan fallos que generen inestabilidad de enrutamiento y que a su vez causaría problemas con el DNS. Eso inhibiría el funcionamiento del DNS, ¿verdad? Pero sería la peor hipótesis.

La mayoría de los operadores han implementado buffers, otros controles tales como hacer un downgrading de las preferencias de enrutamiento en lugar de un corte total, que representaría como si fuera un ataque a la seguridad de los controles. Hay que hacer concesiones operativas prudentes pero yo creo que RPKI depende del DNS y el DNS depende de los enrutadores y es circular las dependencias. Estas dependencias son problemáticas. Sin duda, la resiliencia en el caso de un fallo es necesaria. Es una buena pregunta.

RAM MOHAN Gracias, Danny. Dan, la sociedad civil, los usuarios y la economía en general son los más expuestos cuando los sistemas fallan. Señor Singh, esto es algo que también le voy a pedir que responda después. Primero le pregunto a Dan, ¿cuáles son los costos para la humanidad de los cuales no estamos hablando lo suficiente?

DAN YORK

Muy buena pregunta, Ram. Creo que los retos, los costos humanos son que no estamos cambiando el mundo. La sociedad civil, si vemos las organizaciones sin fines de lucro, en primer lugar no tienen los recursos que tienen las empresas, la financiación, los fondos, no necesariamente se centran en ese sector. No se centran en el sector de sistemas.

La defensa de los derechos humanos en línea, sea una escuela, una iglesia, la idea es también que se cambie un poco la misión. La infraestructura de Internet para esos sectores es de baja prioridad. Como se pregunta en la encuesta, muchos dependen de sistemas de terceros y no necesariamente pueden ellos mismos tener un backup. Requiere que las comunidades técnicas locales, los grupos locales, ayuden en la recuperación para construir esta resiliencia humana y trabajar en conjunto.

Creo que usted está preguntando qué puede hacer la ICANN. Creo que la organización y la comunidad de la ICANN pueden jugar un rol aquí para generar esta resiliencia. De hecho, ya tenemos una gran comunidad en la ICANN mundial que puede ayudar.

Hablando de mejores prácticas, creo que la ICANN puede tomar medidas. Primero, analizar las dependencias. Luego, analizar cuáles pueden ser los potenciales puntos de fallo en el ecosistema y encontrar mejores prácticas, servidores de raíz, registros, resolutores, las entidades sin fines de lucro que puede ser la comunidad de ICANN para promover estas prácticas en las

distintas unidades constitutivas y grupos de partes interesadas.

Hablar con los ISP, la comunidad técnica, hablar con cada una de las partes para generar resiliencia y garantizar las operaciones continuadas y resiliencia del DNS. Esto es algo más tangible que puede hacer la ICANN porque estos costos humanos significan que no se puede cumplir la misión ni hacer lo que la sociedad civil se presume debe hacer. Su trabajo depende de sistemas de mayor escala. Se necesita el expertise local y crear la capacidad y las habilidades humanas.

RAM MOHAN Gracias, Dan. Ya habló Dan brevemente del costo humano de la resiliencia. ¿Qué puede decirnos usted, señor Singh?

M.A.K.P. SINGH Les voy a dar un ejemplo clásico. Cuando se afecta el suministro eléctrico a la mañana en la sesión de apertura se mencionó que la mitad de los centros de sistemas en la India están en Mumbai. Hubo varios cortes aquí, varios apagones. Si estos cortes hubieran continuado mucho tiempo, se hubieran perdido muchísimos datos.

Recientemente ocurrió algo similar en varias partes del mundo, en especial en las zonas de conflictos bélicos debido a las disrupciones. La mayor parte de las instalaciones de infraestructura digital dejaron de estar disponibles. Fiona preguntó sobre la Península Ibérica. La gente no podía comprar

siquiera sus alimentos porque todo estaba digitalizado.

Si no había Internet, nadie podía llevar a cabo una transacción. Estos son los costos. La ayuda humanitaria que se necesita también depende de estas circunstancias. Hay que ser más activo cuando suceden estos cortes. Por ejemplo, cuando ocurrió el ciberataque en Myanmar, para hacer llegar la ayuda humanitaria tuvimos que implementar operaciones móviles, terrestres.

RAM MOHAN Gracias. Tenemos en pantalla la cuarta pregunta del Mentimeter que dice: "Analizando el panorama más amplio de la resiliencia de Internet, ¿cuál es el punto ciego más crítico de la comunidad de la ICANN en este momento?"

Ahora pasemos a la comunidad. Aquí hay dos micrófonos, en el pasillo central. Si ustedes tienen alguna pregunta, les voy a pedir que se acerquen al micrófono y en el caso de los participantes remotos vamos a pedir que usen el panel de preguntas. Como no tenemos mucho tiempo, vamos a pedirles que sean sucintos, breves, no más de 90 segundos. Kathy.

KATHY SCHNITT Michael Palage ha solicitado preguntar.

MICHAEL PALAGE Espero que puedan oírme. Gracias, Ram. En la sesión de apertura se habló del rol crítico de los RIR y el ecosistema de Internet. Mi

pregunta es por qué este aspecto de la discusión fue pasada por alto en la segunda parte de la presentación. La segunda pregunta es la siguiente. A diferencia de los nombres, ICANN tiene contratos con la mayoría de los gTLD. Solo tienen un memorándum de entendimiento con NRO, que es una entidad sin personalidad jurídica. Ese es un punto de vulnerabilidad. La tercera pregunta. Cuáles son las consideraciones de defensa del consumidor.

RAM MOHAN Voy a pedirle a Danny que cubra una de esas tres preguntas.

DANNY MCPHERSON Nosotros trabajamos muchos con los miembros considerando la perspectiva de trabajar con los RIR y seguir la industria de cerca. RPKI tiene cada vez más operaciones directas que impactan en la infraestructura y queremos asegurarnos de que esta infraestructura sea robusta y segura.

Hay inversiones importantes para asegurar que las personas operen según las normas para operar de la manera segura y estable que se espera de los proveedores. Destinamos mucho tiempo a esto. Pensamos que es cada vez más relevante. Hace cinco años yo no me tenía que preocupar por RPKI ni las capacidades de mis proveedores.

Yo pienso que los RIR han hecho varias cosas para ser más robustos. Antes había sistemas acoplados de una manera un poco más débil y ocurrían fallos. En este momento hay cortes

planificados en algunos servicios para simular fallos. El DNS, sin duda, está mejorando las capacidades pero el estado de la cadena de abastecimiento está mejorando con RPKI y el financiamiento, los fondos asignados y estos son aspectos muy importantes para garantizar que los proveedores continúen mejorando sus capacidades y sigan siendo seguros y robustos. Esto es todo lo que voy a decir al respecto.

RAM MOHAN Vamos ahora a tomar una pregunta de la sala. Vamos a pedirle al orador que hable más cerca del micrófono.

ANAND RAJE Soy Anand, de la India Internet Foundation. Estamos rodeados de API y servicios con identidades en Internet que dependen de arquitecturas centralizadas. Mi pregunta al panel es la siguiente. ¿Cuál es el impacto en esta arquitectura de confianza centralizada?

RAM MOHAN Voy a repetir la pregunta. ¿Cuál es el impacto que tiene la arquitectura centralizada sobre la resiliencia?

PAUL VIXIE Por defecto, es preocupante. En otras palabras, hemos visto varias veces que no hubo una resiliencia adecuada de la conectividad entre algunas regiones y el resto del mundo. Hay

dependencias acopladas. Los sistemas locales no encontraban otros sistemas locales o no podían decidir si confiar o no en otros sistemas locales porque ninguno podía llegar al sistema más distante. Esto es por defecto. Es algo que los diseñadores deben analizar y no solo en las implementaciones.

RAM MOHAN Gracias, Paul. ¿Alguna pregunta en línea?

KATHY SCHNITT Tenemos una pregunta para Bruce. Australia tiene una cartera con un ministerio dedicado. ¿Esto ha cambiado significativamente el abordaje a la seguridad del DNS y a la resiliencia más amplia o el desafío sigue estando en la implementación de los agentes de la industria?

BRUCE TONKIN Es una pregunta complicada. Desde el punto de vista gubernamental en Australia se ha creado un departamento dedicado a las cuestiones internas. Bajo este paraguas han creado una agencia que se ocupa de la seguridad de la infraestructura crítica.

El Ministro de Ciberseguridad trata más preguntas como por ejemplo los temas relacionados con las empresas pequeñas. Por ejemplo, cómo podemos crear conciencia en el marco de estas empresas pequeñas y qué medidas pueden tomar para mejorar su resiliencia. Como operadores de registros, creo que tenemos

interacciones con otros actores.

RAM MOHAN Una pregunta del público.

IDIL KULA Hola. Soy de Turquía. Soy becaria por segunda vez. Hablan de la resiliencia, de la robustez y la infraestructura de Internet en su conjunto. Como dijeron, es una red de infraestructura que incluye API, servicios externos y otros componentes. No he oído sobre las cadenas de suministro de energía. No he oído hablar de la resiliencia medioambiental que es necesaria para poder tener una red de energía resiliente.

Cómo creen que la ICANN puede animar a todas las partes interesadas para que haya un uso más sostenible y más prácticas sostenibles. Somos una comunidad que procede de todo el mundo. Si hay una parte que puede alentar a las personas a tener prácticas más sostenibles, me parece que es aquí, es el sitio, este es el lugar.

Mi pregunta es entonces cómo podemos trabajar conjuntamente para incidir en esto porque si vamos a esperar a los gobiernos para que hagan valer estas responsabilidades en torno al clima, no sé cuánto vamos a tener que esperar. Si fallan las cadenas de suministro, falla todo el sistema.

RAM MOHAN Dan, ¿qué opina? ¿Qué puede hacer la ICANN para ayudar con la resiliencia ecológica y medioambiental?

DAN YORK ¿Cuánto tiempo tenemos? Creo que hay una pregunta mayor aquí. No hemos oído bien la pregunta en línea. Si puede repetir la pregunta.

RAM MOHAN He resumido la pregunta para usted. ¿Qué puede hacer la ICANN para mejorar la resiliencia ecológica y medioambiental? Este es el resumen.

DAN YORK Gracias. Se está trabajando mucho en el ecosistema más amplio de Internet en torno a estas cuestiones climáticas. Está la cuestión de la computación verde, cómo operar sistemas, centros de datos utilizando menos energía, menos carbono. Hay muchas cosas. No tengo una recomendación específica pero si tomamos la cadena de suministro en su conjunto y todas las piezas en cada pieza se puede estudiar cuál es el impacto que tiene sobre la crisis climática. Cómo puede cada una reducir su huella del carbono. Hay muchas cosas que se pueden hacer a cada nivel de la jerarquía. Los registradores, registros, registratarios, las personas que operan los servidores autoritarios. Estas preguntas se pueden plantear en cada nivel. Quizá la ICANN podría asumir el papel de ver cómo estos sistemas que componen el DNS pueden ser más

sostenibles.

RAM MOHAN Gracias, Dan. Carlos, ¿puede compartir con nuestro público los resultados de las encuestas en Mentimeter? Esto es lo que han dicho sobre cuál va a ser la principal causa de la próxima interrupción global. Próxima pregunta. Estoy repasando las respuestas del Mentimeter. ¿Hay alguna respuesta más? Sí.

Con diferencia, lo que están diciendo es que la coordinación intersectorial, es decir, entre los sectores de las telecomunicaciones, etc., es el principal ángulo muerto de la ICANN según lo que estoy viendo aquí. ¿Es todo, Carlos? Muy bien, gracias. Muchas gracias a todos.

Voy a volver a los panelistas. Bruce, voy a comenzar con usted. Esta es la pregunta. Si tuviera poco tiempo para hablar directamente con el liderazgo de la ICANN después de esta reunión, ¿qué les diría primero?

BRUCE TONKIN Creo que tenemos que hacer un mapeo de los proveedores de servicios y los operadores de la cadena de suministro y realizar pruebas de los posibles escenarios. Por ejemplo, qué pasaría si hubiera un problema con BIND.

RAM MOHAN Paul, ¿qué le diría al liderazgo de la ICANN? ¿Qué tiene que hacer

primero, después de esta sesión? ¿Qué sería lo más urgente?

PAUL VIXIE No hemos abordado mucho en esta sesión la cuestión de la presión regulatoria. Sé que algo como COICA puede surgir de la nada. Si no vamos a California y decimos, vale, han pedido verificación de edad para el código abierto y para los sistemas no contratados, ¿qué más intereses tienen? Hablar más con todo el mundo, incluyendo las democracias para ver qué se espera de Internet y así podremos empezar a construirlo para ellos y a hablar de estas cuestiones.

RAM MOHAN Señor Singh, ¿qué pediría?

M.A.K.P. SINGH Creo que los fallos en las políticas tienen un efecto en cascada en todo el sistema por lo que tenemos que entender cómo los proveedores de servicios y todo el sistema existe para proteger los puntos críticos del sistema en su conjunto.

RAM MOHAN Gracias. Dan, ¿qué diría?

DAN YORK Diría que habría que pensar desde una perspectiva organizativa acerca de esta cuestión de la resiliencia. Tiene que haber una

resiliencia técnica. Lo ha dicho Bruce y el señor Singh también. Han hablado de mapear las dependencias ocultas del sistema del DNS, las buenas prácticas y también la resiliencia humana. La organización, el aspecto técnico y el aspecto humano.

Tenemos que ver qué tenemos y sé que muchas organizaciones están trabajando ya en estos espacios y la ICANN puede aprovechar su trabajo. Tenemos que llegar a un punto en que las personas tengan un acceso seguro a Internet.

RAM MOHAN Danny.

DANNY MCPHERSON Creo que hay muchos aspectos que hemos abordado y que ya se integran en la planificación estratégica de la ICANN. Los sistemas técnicos y los equipos técnicos han hecho un trabajo encomiable para mantener los sistemas durante todo el tiempo que llevan existiendo.

Existe una oportunidad más amplia para centrarse en los aspectos externos y en el impacto sobre los sistemas. Veo esta respuesta de la coordinación intersectorial. Me parece que muchas partes interesadas de la comunidad de la ICANN dedican mucho tiempo a estudiar los escenarios de catástrofes, de las comunicaciones urgentes, la resiliencia, etc. Quizá la ICANN no tiene que hacer eso de manera tan directa pero sí que desde una perspectiva más estratégica.

Lo que echo en falta es la previsión de las amenazas, una previsión más estratégica, las fuerzas que existen en las economías, las tecnologías, que pueden desestabilizar la comunidad de la ICANN. Creo que entender todo esto es clave. Sí que cae dentro del alcance del trabajo de la ICANN.

RAM MOHAN Gracias, Danny. A los que están en la sala, que levanten la mano, ¿piensan que la ICANN tiene que hacer de la resiliencia de Internet una prioridad estratégica? Muy bien. Fiona, le devuelvo la palabra para que nos dé sus comentarios finales.

FIONA ALEXANDER Creo que no voy a decir nada. Solo voy a dar las gracias a los que han presentado y a los que han participado tanto en la sala como en remoto. Creo que sí que hay que hacer hincapié en que es importante que todos deben asumir su papel.

RAM MOHAN Muchas gracias a los panelistas. Se cierra la sesión.

[FIN DE LA TRANSCRIPCIÓN]