ICANN84 | Reunión General Anual – ccNSO: recuperación ante desastres de la IANA
Miércoles, 29 de octubre de 2025 – 13:15 a 14:30 IST

CLAUDIA RUIZ

Hola y bienvenidos a esta sesión de la ccNSO. Recuperación ante desastres y la IANA. Soy Claudia Ruiz y junto con mi colega Joke Braeken seremos las coordinadoras de participación para esta sesión. Tengan en cuenta que esta sesión se está grabando y se rige por el código de conducta de los participantes de la ICANN, las normas de comportamiento esperados de la ICANN así como la política antiacoso de la comunidad de la ICANN.

Tengan en cuenta las siguientes pautas para participar en esta sesión. También las copiaremos en la ventana de chat. Durante esta sesión, las preguntas o comentarios en el chat se leerán en voz alta solamente si se presentan en el formato adecuado que se describe en el chat.

En esta sesión habrá interpretación en inglés, español y francés. Si quieren tomar la palabra durante la sesión, por favor, levanten la mano en Zoom. Cuando se diga su nombre, los participantes virtuales podrán activar su micrófono en Zoom. Los participantes presenciales utilizarán el micrófono presencial para hablar. Por favor, digan su nombre para los registros y el idioma en el que

hablarán si no es inglés. Muchas gracias. Con esto le doy la palabra a Peter Koch. Muchas gracias.

PETER KOCH Gracias, Claudia. Buenas tardes a todos. Bienvenidos después del almuerzo. Soy Peter Koch, del registro gTLD de Alemania. Les doy la bienvenida a esta sesión. El tema de esta sesión es recuperación ante desastres y, en especial, el posible rol de la IANA.

Vamos a hablar sobre la experiencia de diferentes ccTLD. Vamos a ver la experiencia de la IANA y de la ICANN. Quiero darles un poco de contexto primero porque algunos de ustedes recordarán que había una especie de brecha o vacío en la política y un grupo trabajó para preparar una serie de recomendaciones que llevaron a la preparación de la carta orgánica de dos grupos de estudio. Uno es el grupo de estudio sobre el rol de la IANA en caso de recuperación ante desastres. Este tema ya se había empezado a trabajar y ahora estamos abordando este tema en realidad desde dos puntos de vista.

El grupo de estudio, y algunos de los miembros de este grupo están en esta sala ahora, van a compartir los resultados o las experiencias y lo que se diga aquí lo van a utilizar como material para el trabajo del grupo de estudio. Después voy a hablar quizá sobre el grupo de estudio.

Veamos rápidamente la agenda. Régis va a hablar sobre la perspectiva de TLD Ops, que es un comité permanente de la ccNSO.

Kim Davies va a hablar un poco desde la perspectiva de la IANA. Vamos a recibir información de Francisco Arias que va a hablar sobre lo que está sucediendo y cuál es la práctica actual en el espacio de los gTLD. Lo va a dar como información que podamos utilizar en el debate.

Después Régis, nuevamente, va a tomar la palabra desde otro rol y va a compartir las observaciones que surgen de su rol en AFNIC y después vamos a resumir todo. Esa va a ser mi función. Espero que todos ustedes escuchen todo esto y aporten y compartan sus experiencias. Régis, ¿está listo para empezar? Le doy la palabra.

RÉGIS MASSÉ Gracias, Peter. Parece que hay un ciberataque en la sala. Hola a todos. Soy Régis Massé. Soy el director de tecnología de AFNIC, un registro. En primer lugar voy a hablar sobre lo que hace TLD Ops. Ya hace dos años que estoy trabajando allí. Para los nuevos participantes que están en la sala, les voy a decir que el grupo TLD Ops es la comunidad de seguridad operativa para los ccTLD.

El objetivo de este grupo es brindar una lista de contactos y de correos electrónicos para compartir información y para tener una plataforma para cooperar y compartir información entre los operadores de ccTLD, para coordinar la respuesta a las amenazas. La participación está limitada a todos los ccTLD, no solo a la ccNSO. Después voy a volver a esto porque es importante.

El objetivo principal, como ya dije, es crear una lista confiable de contactos para compartir información y para luchar contra los ataques. Tenemos gente de operaciones de los ccTLD. Nosotros creamos esta lista y después empezamos a desarrollar herramientas para los ccTLD. Preparamos un manual sobre ataques de denegación de servicio, DDoS, para que se pueda luchar contra los ataques DDoS. También desde hace cinco años estamos trabajando en diferentes áreas. La próxima diapositiva, por favor.

Para estar seguros de que todos entendamos lo mismo por recuperación ante desastres y continuidad de operaciones, la definición es que es la capacidad de una organización de seguir brindando sus productos y servicios que son importantes para el negocio del operador de registro de ccTLD y para todas las partes interesadas a un ritmo y a niveles aceptables después de un incidente.

Debemos seguir prestando los servicios de DNS. Debemos seguir prestando los servicios relacionados con los nombres de dominio y debemos trabajar con todas las partes interesadas. En esta continuidad de operaciones tenemos un plan de recuperación de desastres que está relacionado con el plan de continuidad de operaciones. La continuidad de operaciones es un plan de acción.

La recuperación ante desastres incluye procedimientos y planes. La continuidad de operaciones contiene algunos planes pero tenemos planes técnicos, planes de recursos humanos, planes de comunicaciones. La continuidad de operaciones incluye todos

estos planes. Es una forma de mostrar la diferencia porque a veces los dos conceptos se confunden. La próxima diapositiva, por favor.

Preparamos algunos entregables. Lo hizo el grupo de TLD Ops. Desarrollamos un manual y todo esto está disponible a través del vínculo que ven allí, que los lleva a la página de Confluence, que está en el sitio de la ccNSO de la ICANN. Tenemos un manual que define plantillas y define qué tenemos que tener en cuenta en caso de un desastre. Tenemos una lista de contactos. También debemos tener procedimientos para estar preparados, encontrar y restaurar el sistema si se cae.

Después de esto también preparamos documentos de ejercicios de simulación. La idea es capacitar y hacer un ejercicio de simulación con tarjetas de acción. Es un ejercicio de simulación, por supuesto. Tenemos cinco pasos en este escenario. Cuando hacemos este ejercicio todos los años durante 20 minutos recibimos nueva información para que todos los actores y participantes puedan decidir qué hacer.

En cuanto a este ejercicio de simulación, la idea es simular que hay un registro comprometido. En el sitio web tenemos dos escenarios hoy por hoy porque ya hicimos dos sesiones, durante la reunión 66 de la ICANN en Montreal y durante la 81 en Seattle.

El segundo punto es importante porque trabajamos con un grupo europeo. Fíjense en las tarjetas. A la derecha son los cuatro roles que pueden desempeñar los participantes cuando hacemos este

ejercicio. Por supuesto, el rol técnico pero también un rol de gestión, de comunicación y de acciones regulatorias.

Estos perfiles deben estar mezclados en los diferentes equipos porque la idea es que todas las partes involucradas y todos los elementos de la crisis sean tenidos en cuenta en cada paso de este ejercicio. Fíjense entonces. Estas son imágenes del último ejercicio. Algunos se reconocerán en las fotos. La idea es jugar a este juego.

La segunda parte también es muy importante porque al final se analiza lo que se hizo y se discute por qué un grupo eligió hacer algo determinado. En el último ejercicio, creo que hubo ocho equipos y hubo ocho respuestas diferentes. Es muy interesante ver en primer lugar, mientras se hizo el ejercicio en la ICANN, es muy bueno porque trabajamos muchos registros compartiendo información sobre los ccTLD.

Además, podemos decir: Somos registros grandes. Quizá haya registros más pequeños pero todos tenemos los mismos problemas y los abordamos de manera diferente. Es interesante aprender aquí y ejercitarse. La próxima diapositiva, por favor.

PETER KOCH Gracias, Régis, por tu presentación y la experiencia de lo que está haciendo el equipo de TLD Ops. Voy a preguntar a ver si hay alguien que necesite alguna aclaración sobre lo que se dijo. Lo hacemos ahora. Si no, las preguntas generales las dejamos para el final. No veo a nadie que haya levantado la mano en forma presencial ni en

forma remota. Ya están las diapositivas. Voy a invitar a Kim a que hable desde la perspectiva de la IANA.

CLAUDIA RUIZ: Antes de que continúen, los intérpretes piden que por favor hablen más lentamente. Gracias.

KIM DAVIES: Gracias, Peter. Voy a hablar sobre la recuperación ante desastres desde la perspectiva de la IANA. Supongo que todos ustedes saben esto pero estoy hablando desde la perspectiva de la IANA. La génesis de lo que se está discutiendo con la ccNSO en los últimos años se retrotrae hace tres o cuatro años cuando hubo un incidente operacional con un ccTLD. En ese caso, la IANA tuvo que actuar para restaurar los servicios del ccTLD en una situación bastante especial pero esta situación en realidad no estaba cubierta por las políticas.

Al abordar esta realidad operacional, nos dirigimos a los líderes de la ccNSO y les explicamos lo que pensábamos hacer. Por suerte, esa cuestión se resolvió y no vamos a hablar de eso hoy pero como resultado de esa colaboración con los líderes de la ccNSO se invitó a la IANA a aportar a su experiencia general en las operaciones del día a día donde pensamos que había algunas brechas, algunos huecos en las políticas, donde no se tenían las facultades necesarias o no había una posibilidad de abordar los temas específicos.

Se creó un grupo de trabajo de análisis de políticas y empezó a trabajar con una serie de observaciones que presentó en la IANA sobre áreas donde falta una política. No quiero decir que la IANA no pueda hacer nada sin esa política pero la ccNSO quizá quiera ver la situación y definir que quizá haga falta una política.

Como parte de ese ejercicio identificamos algunas oportunidades y una de ellas fue lo que yo llamaría la falta de operaciones de recuperación cuando la ccTLD no está operando continuamente. Si decimos recuperación ante desastres siempre pensamos en un desastre natural, un terremoto, una inundación, ese tipo de cosas. Por supuesto, eso es un desastre del cual habría que recuperarse si afecta a un ccTLD pero cuando yo pienso en desastres pienso en una definición más amplia. Esto es parte de eso pero el tipo de desastres que hemos visto a lo largo de los años que ameritaron una respuesta de la IANA, o quizá las partes se acercaron a la IANA para buscar una respuesta, son otro tipo de desastres.

Uno de estos escenarios sería, por ejemplo, cuando no funciona bien el negocio de un administrador de la ccNSO. Cuando la empresa deja de operar. Estos escenarios no significan que el TLD no está haciendo las resoluciones. Muchas veces las situaciones son complejas. Quizá hay un proveedor de servicios de registro que sigue operando. Quizá hay servidores de nombre que siguen operando pero el administrador del ccTLD no sigue operando. Otro caso es una violación no corregida de los requerimientos de

políticas que tienen los ccTLD en general. Después voy a hablar de esto en la próxima diapositiva.

En este contexto, con una definición más amplia de lo que implicaría la recuperación ante desastres, esta es la pregunta que se presentó a este grupo de trabajo. ¿Qué requerimientos deberían establecerse en relación con la recuperación ante desastres y/o la habilidad de continuar las operaciones del dominio en el caso de un desastre o en el caso de que no se cumpla con las políticas globales? Esta sería la pregunta fundamental, básica, que relaciona todo lo que se hace en esta área. La próxima diapositiva, por favor.

PETER KOCH ¿Podría acercarse al micrófono, por favor?

KIM DAVIES Cuando hablamos de las razones en las que tenemos que intervenir en una operación de un ccTLD que no funciona como debería, hay una sólida conexión con la política de revocación porque está en su corazón. Implica acciones que se pueden tomar de manera apropiada conforme a la política local.

La ccNSO creó algo de trabajo publicado en 2013 que brindó la base para la revocación como resultado último. Esencialmente es cuando la IANA considera que inclusive la conducta del administrador implica un posible efecto adverso importante en la comunidad y también una amenaza a la comunidad. No está cumpliendo los objetivos requeridos como conectividad de

Internet apropiada. Una configuración adecuada y administración de los archivos de zona. Los servidores de nombre, que pueden realizar las tareas de resolución de nombre esperada, con puntos de contacto operativos y un mínimo de requisitos de presencia local en los que puede y debe rendir cuentas en la jurisdicción pertinente.

Estas fallas son egregias o persistentes. Esto puede llevar a quedar sujeto a revocación, esto está ya desde hace 12 años. ¿Ha sucedido alguna vez? No. Pero hay casos que sí se han explorado y se han presentado solicitudes a la IANA para considerar ccTLD para revocación.

Quizá se pregunten por qué traigo esto a colación. La razón por la que lo traigo a colación es que inclusive en situaciones en las cuales las razones de revocación no son controvertidas, puede haber un administrador de ccTLD que esté sujeto a revocación pero la realidad práctica es que aunque la IANA tome esa determinación es difícil prever una situación en la cual esta pueda revocar un ccTLD. Por falta de opciones puede hacer una revocación pero el tema es que siga operando el ccTLD.

Algunas situaciones pueden ser un desafío. Esto es algo hipotético, no es algo que haya sucedido, pero hay escenarios que tuvimos que explorar. Puede llegar a ser un tema en el que identificamos el administrador. Los criterios que se indican en la parte superior de la diapositiva tenemos que dar al administrador la opción de resolver el tema y un tiempo suficiente pero quizá pueden no

responder y pueden llegar a decir: “No me interesa. No es un problema mío”.

En estos escenarios, si no cooperan con la IANA, pueden tener que cooperar con partes locales que están tratando de resolver la misma situación. Normalmente la política favorece la acción local. Normalmente viene la IANA después de haber agotado todos los posibles recursos. Por supuesto, la falta de jurisdicción es importante. Normalmente se ven casos en los cuales el ccTLD está operando fuera de la jurisdicción del país y el recurso local, imagínense una sentencia se puede emitir pero no tendría jurisdicción fuera del país en el que se emite.

Esta definición de desastre, se puede ver muy afectada la operación por inundaciones, terremotos, fallas en los servicios públicos. Puede ser guerra, personal reubicado para verificar su seguridad personal. A menudo el ambiente es muy dinámico. Cambia con rapidez. En este tipo de situaciones a menudo lo que sucede es que se expone un único punto de falla en el que el administrador por accidente o por la realidad operativa se basa en una instalación local que ya no está disponible. Esto puede llegar a ser un problema significativo.

Se habla de fallas a nivel negocio. La empresa de pronto puede dejar de operar o también se prevé un escenario en el cual puede haber situaciones en las cuales no pueda operar la empresa. Por ejemplo, una sentencia de un tribunal que no le permita operar.

Otro tema vinculado que se presentó al grupo de brechas, algunos ccTLD quieren hacer las cosas correctas y esto se ha visto. En la mayoría de los casos los administradores quieren hacer lo que está bien, conservar sus operaciones y en ese contexto hay una serie de operadores de ccTLD que lo han pensado mucho y tienen planes muy definidos, que en este tipo de falla o escenario de negocios se identifican otras partes en el país con las que se trabaja y puede haber una relación con ellas.

Si estamos incapacitados de alguna manera podemos recurrir a ellos porque tenemos un vínculo con ellos y queremos que participen. Esencialmente nos dicen: "Podemos establecer una relación privada en la cual la IANA puede hablar con esta otra entidad y trabajar con ellos en caso de que nosotros no podamos cumplir", pero no hay una disposición en la política que permita que la IANA, en caso de transferencia de ccTLD, hay una política enorme que pide un proceso debido que lleva meses con todas estas revisiones e inspecciones. No hay una política en el libro que dice que en una emergencia con consentimiento expreso o un consentimiento previo, la IANA pueda tomar determinadas acciones para restaurar el servicio con un asociado. ¿Debería haber alguna política sobre el tipo de regímenes? ¿La IANA puede establecer tal tipo de convenio? Dicho convenio pueden prever no aplicar los requerimientos de política en emergencias necesarias temporariamente.

Una pregunta adicional. Si se nos permitiera realizar tal tipo de convenio, ¿tienen que ser privados o informados de manera

transparente? Hay algún requisito de rendición de cuentas implícito. Siguiente, por favor.

Antes les decía que se favorecen las soluciones locales, que la IANA es un último recurso para este tipo de situación, ¿pero son la respuesta completa? La política general es clara. Los ccTLD están diseñados para su administración local. La realidad local es que no todos los países tienen los mismos tipos de sofisticación como para hacerlo de manera efectiva.

La realidad es que si el ccTLD está en una situación comprometida, quizá la comunidad de Internet local no tiene la preparación esperada. Quizá el administrador no tiene planes de recuperación de desastres. ¿Qué hacen entonces? Se comunican con nosotros buscando soluciones.

A menudo tenemos que decir: “Perdón, pero no podemos hacer nada”. Cuando hablamos con los ccTLD de los países y su infraestructura crítica, creo que podríamos estar todos de acuerdo en que queremos que sigan funcionando y que hace falta que tengan herramientas en los escenarios correspondientes que permitan restaurar las operaciones de alguna manera.

Parte del debate con el que comienza esta sesión en los meses por venir es cuál es el papel de la IANA, de los ccTLD, las cosas que se tratan a nivel local pero cuando fallan las soluciones locales, ¿qué tipo de situación hay que encarar a nivel global? Siguiente, por favor.

Esta es la última diapositiva. Sí, es correcto. ¿Qué hacemos hoy? Tenemos estos debates privados con los administradores de ccTLD. Cuando se consulta, se informa que los administradores de ccTLD tienen mecanismos locales considerados.

Hemos notado que parte del desafío que enfrentamos es que aunque las partes cooperen hoy, no hay garantía que de aquí a 10 años sigan haciéndolo. En esencia, cuando se asume este tipo de escenarios, quizá las relaciones se pueden degradar y tenemos que tener opciones disponibles para mantener el servicio cuando esas relaciones ya no son viables.

Algo que vemos más que otros cuando tenemos un administrador de ccTLD, quizá no pueda confiar en un proveedor de servicio o quizá no esté en la jurisdicción o sí. Puede haber un contrato con ellos pero si no están en su país, si no son locales quizá digan: “Mala suerte”. Quizá no sea una definición clásica de desastre del que recuperarse pero les digo que en esos escenarios el administrador considera un desastre cuando no funciona un proveedor de servicios.

Esa es un área general en la que cae la ICANN. La IANA no tiene mecanismos para hacer un receptor de una custodia per se aunque las partes así lo deseen. Alguno dice: “Sí. Queremos que la IANA participe” pero no es nuestra competencia. Buscamos alternativas válidas a esto. Para reiterar el punto que comenté antes, si no hay mecanismos locales para manejar el ccTLD dentro del país podemos decidir que no se puede revocar porque la IANA no puede

obligar a un proveedor de servicio de registro que maneje esto. Se basa en mecanismos que no se pueden disparar en este tipo de escenario.

Habiendo dicho esto, lo que mencioné sobre ccTLD, también tenemos los gTLD. Hay una estructura con disposiciones de custodia obligatorias. Hay maneras en que la IANA puede participar con notificación de por medio para restaurar la operación de un gTLD y para explicar eso en mayor detalle mi colega Francisco va a explicar qué es lo que sucede en el espacio de gTLD con la ICANN. Ese es el final de mi presentación. Muchas gracias.

PETER KOCH Gracias, Kim, por aportar una perspectiva tan amplia. Veo que hay dos manos levantadas en Zoom. Si están en la sala y quieren levantar la mano deben agitarla. Si no, no vamos a verlo. Tenemos una pregunta en la ventana de preguntas y respuestas. Le voy a pedir a la secretaría que lea la pregunta.

Estoy tratando de que contestemos inmediatamente las preguntas que tienen que ver con la presentación en curso pero al final de las presentaciones vamos a ver todas las preguntas. ¿Alguien podría leer la pregunta, por favor?

CLAUDIA RUIZ La pregunta es del Dr. Gopal, de Nueva Delhi. ¿Hay un plazo estipulado para la detección del desastre y la recuperación?

KIM DAVIES

Desde el punto de vista de la IANA, no. Si hay que hacer un cambio en la zona raíz por una emergencia, podemos pedirle a la IANA que lo haga rápidamente. En realidad, de lo que estamos hablando ahora no tiene que ver con la capacidad de cambiar rápidamente la zona raíz, cosa que sí podemos hacer. Tiene que ver con muchos otros elementos pero no conozco ningún plazo específico para lo que usted pregunta.

PETER KOCH

Yo diría que esto sirve para el grupo de estudio porque si estamos pensando en términos amplios qué es un desastre, esto forma parte del mandato entre las cosas que tenemos que considerar. Ahora tengo a Chris Disspain, por favor.

CHRIS DISSPAIN

Gracias, Peter. Gracias, Kim. Fue muy interesante su presentación. Tengo una serie de puntos que mencionar. Sé que todo lo que usted dijo es correcto pero me preocupa un poco esto de mencionar los temas que se dan de vez en cuando en forma ocasional en la misma categoría que recuperación ante desastres. Quizá yo sea la única persona que piense esto pero quizá haya una brecha.

En este caso el grupo tiene que pensar en recuperación ante desastres. Usted también mencionó una calamidad en el país, etc. Debería haber una distinción clara entre los dos elementos. En el

caso de una revocación, todo lo que usted mencionó se da porque falta cooperación del administrador de ccTLD y entiendo que esto puede ser un problema.

La recuperación ante desastres en la que yo pienso se da cuando el administrador del ccTLD necesita la ayuda de ustedes. Quisiera asegurarme de que entendamos bien de qué hablamos porque estas dos cosas tienen soluciones diferentes e independientes.

No podemos utilizar los temas de revocación, lo que no se puede hacer, todo lo que usted dijo, que es cierto, para tatar de utilizar todo esto en el caso de una recuperación ante desastres. Quizá sea algo totalmente diferente pero quizá esté equivocado.

PETER KOCH Kim, ¿quiere responder?

KIM DAVIES Gracias, Chris. No estoy en desacuerdo necesariamente con lo que usted dijo. No me compete a mí cómo diferenciar estas cuestiones pero una observación que haría es que puedo pensar en un escenario donde la respuesta por recuperación ante desastres, como consecuencia de un desastre, qué pasa si el administrador del ccTLD no coopera. Quizá no quiera no cooperar sino que quizá no pueda cooperar. Por eso hay una relación. Tratamos de crear dos temas diferentes aquí. Como dije antes, esto es una expresión de los temas y cuestiones que vemos. Cómo la comunidad los va a abordar, la comunidad lo debe decidir.

PETER KOCH

Sí. Chris, lo tuve en cuenta. Hay un tema técnico o administrativo en este tema. Cuando empezamos yo dije que esta sesión y el grupo de estudio estaban empezando a trabajar desde dos puntos al mismo tiempo. No todo lo que se diga hoy aquí estará dentro del mandato del grupo de estudio necesariamente pero todos los aportes y comentarios pueden ser lo más amplios que ustedes quieran y vamos a tomarlos y ver de trabajar desde allí. Sin más, Rocío, le doy la palabra.

ROCÍO DE LA FUENTE

Rocío, de LACTLD. Quería mencionar que las organizaciones regionales de ccTLD también ayudaron en el caso de recuperación ante desastres. Esto es algo importante a tener en cuenta en la conversación. Incluso los ccTLD individuales de la misma región desempeñan un rol ayudando a restaurar las operaciones en casos de desastres naturales. Tenemos incluso un proyecto que es una nube Anycast y nosotros brindamos un servicio secundario para muchos ccTLD. Así tratamos de ayudar en el caso de estos escenarios. Quería mencionar esto.

PETER KOCH

Gracias. Ahora tenemos a Jordan Carter.

JORDAN CARTER

Gracias, Peter. Soy de .EU y presidente de un grupo de análisis de brechas que trabajó durante muy poco tiempo. Llegué a la misma

conclusión que Chris obviamente en cuanto a la definición del alcance y creo que la forma en que usted describió los desafíos que presentamos cuando un registrador o un registro no quiere cooperar, esta es una brecha en la política en la que no había pensado.

Si hay una política que tiene que ver con la responsabilidad de los ccTLD, quizá si falta cooperación la política no se pueda implementar. Hablando de la brecha, si creemos que podemos revocar en algunos casos, en realidad no lo podemos hacer. Quizá esa sea otra brecha diferente que debamos considerar. Cuando hablamos de desastres, esto es diferente a un desastre natural. Otro tema para pensar. Muchas gracias.

PETER KOCH: Gracias, Jordan. Vamos a tomarlo en cuenta. Quizá lo vamos a presentar al consejo en algún momento. Creo que Eberhard levantó la mano.

EBERHARD LISSE: Soy presidente del grupo de trabajo técnico que se formó después de una reunión de la ICANN donde vimos esta misma situación. Estoy totalmente de acuerdo con Chris en que sí deberíamos separar por un lado la revocación como decisión de ayuda o de recuperación ante desastres pero el proceso en cada caso para mantener la seguridad y la estabilidad de Internet es el mismo.

Debemos asegurarnos de no confundir estos dos puntos de partida. Por supuesto, estoy muy de acuerdo con la forma en que la IANA manejó la crisis .LB. Debemos separar estas dos cosas. Cómo llegamos a ese punto y qué hacemos.

PETER KOCH: Muchas gracias. No veo ninguna mano más levantada. Jordan, ¿la tiene levantada desde antes? Le damos la posibilidad de una pregunta más. Todo esto es muy valioso pero quiero que todos los presentadores tengan tiempo de presentar.

TOM BOLT: Tom Bolt, de .VI, de las Islas Vírgenes. Nosotros enfrentamos desastres una y otra vez. Mi pregunta es si no deberíamos tratar de pensar en medidas preventivas. ¿Hay un modelo, un plan de recuperación para desastres que afecten a TLD? Si estamos en una zona de desastres naturales como las Islas Vírgenes, nosotros tenemos nuestros servidores en Canadá, en Vancouver. Hay un tema con dónde están los servidores.

Otra cuestión que yo veo con Internet y con la ICANN es esta segunda generación que empieza a participar. La pregunta es si hay un plan de sucesión. Lo vemos todo el tiempo en el campo jurídico y legal donde hay un solo experto, un solo abogado. Es necesario tener un plan de sucesión publicado. ¿Qué va a pasar? Creo que deberíamos implementar medidas preventivas y no

pensar solamente en la revocación, que es algo muy difícil, como dijo Kim. Las medidas preventivas, creo que deberíamos hacer eso.

PETER KOCH

Gracias. Yo también creo que esto es muy valioso para el trabajo del grupo de estudio y los invito a participar de este grupo. Ahora quiero darle la palabra a Francisco, que va a dar una breve presentación sobre EBERO y los servicios de custodia. Una vez más, no estamos publicitando esto como solución. Este es solamente un aporte para todo el tema general. Gracias.

FRANCISCO ARIAS

Gracias, Peter. Soy Francisco Arias. Trabajo en la ICANN. Mi equipo se ocupa de tecnologías de TLD pero yo vengo de la comunidad de ccTLD. Fui el director de tecnología en .MX durante mucho tiempo.

En el espacio de los TLD esto es una presentación de lo que tenemos en cuanto a continuidad de servicio en el área de los gTLD. El primer elemento que van a ver aquí es la custodia de datos. Este es un servicio crítico para que la ICANN pueda restaurar los servicios de registro en el caso de una falla catastrófica a nivel del registro o el proveedor de servicios de registro.

Los registros gTLD deben poner en custodia los datos de registración con un agente de custodia de datos aprobado. Este es un tercero. Se firma un contrato y la ICANN es beneficiaria de los datos cuando se dan ciertos casos. Es importante depositar estos datos en forma diaria, los datos de registración. Se hace un

depósito completo, sean los datos de todo el día o diferenciales, es decir, solamente lo que es diferente con respecto al depósito anterior de datos.

Los depósitos de custodia de datos cumplen con las normas RFC. Es un formato de custodia que estandarizó el IETF hace no mucho tiempo. Es lo que vemos en pantalla. Los acuerdos de registro, los contratos que tienen con la ICANN, especifican qué datos deben ser puestos en custodia a través de estos depósitos.

Encontrarán más información sobre la custodia de datos y el programa sobre el tema que tiene la ICANN, que está centrado en el espacio de los gTLD. Encontrarán información sobre lo que hacemos, sobre todo lo que hacemos. La próxima diapositiva, por favor.

El siguiente elemento que tenemos para este programa de continuidad de servicios en la ICANN es el siguiente. Tenemos un monitoreo activo de estos servicios de registro. Tenemos uno de los sistemas más complejos que tiene la ICANN. Este sistema monitorea el cumplimiento de los acuerdos de nivel de servicio para los registros y registradores. Está basado en Zabbix, que es una plataforma de monitoreo. Esta plataforma Zabbix, para quienes no la conozcan, es una empresa en Letonia que ofrece soluciones de código abierto para monitorear servicios en línea y se centra básicamente en los servicios financieros pero creemos que también es útil para nosotros, por eso estamos usando su plataforma desde la ronda anterior de gTLD.

Tenemos a fin de hacer un sondeo de los servicios que brindan los registros, tenemos una red de 40 sondas distribuidas a nivel global. Tratamos de colocarlas en redes que concentran la mayor cantidad de usuarios de Internet. Esas sondas envían consultas de DNS, RDAP a los servidores de registro y la información después se centraliza, se compila, se analiza y nosotros recibimos los resultados de todos esos cálculos.

También tenemos un centro de operaciones de red que opera 24/7. De esta manera podemos manejar las alertas que envía el sistema. El sistema puede informar al personal que debe actuar. Tenemos siempre personal de guardia para resolver estos temas. La próxima diapositiva, por favor.

Con ese sistema de monitoreo tenemos una API. La llamamos MoSAPI. Es una API REST que permite que los registros y los registradores tomen la información que nosotros publicamos, información de SLAM, la información condensada. También publicamos aquí información que surge del programa Domain Metrica relacionada con el uso indebido del DNS. Cada TLD puede ver la información sobre sí misma, no la información sobre otros TLD. Quiero aclarar esto.

Ahora, lo que mencioné antes, el monitoreo proactivo de servicios también monitoreamos además el servicio de DNS para todos los TLD y la raíz aunque no tengamos un acuerdo SLA con los ccTLD o el servicio. Lo monitoreamos para ver qué pasa si hay un problema.

Lo importante es tener un contacto. No es un régimen formal. En el caso de los gTLD simplemente compartimos información.

Por eso tenemos información con respecto al desempeño de cada uno de los ccTLD con respecto al servicio de DNS. En el caso de que les interese acceder a esta API, está disponible y algunos ya tienen acceso a esa API. En esta diapositiva pueden ver cómo se puede solicitar acceso a esa API si les interesa ver la información sobre ustedes mismos, sobre su organización.

Les decía que teníamos la custodia de los datos en caso de falla catastrófica. Hablé del sistema de monitoreo para verificar constantemente el estado del servicio. En el contrato con los gTLD tenemos los umbrales de emergencia que definen los umbrales en los cuales la ICANN tiene el permiso de asumir la operación temporaria del TLD para restaurar el servicio.

Solamente lo hacemos en momentos en que no podamos contactarnos con el registro, con el RSP o inclusive cuando no tengan una solución que garantice una restauración rápida del servicio. Algo que tener en cuenta aunque tengamos una emergencia con una EPP que no monitoreamos, en ese caso del umbral es un poco más complejo que lo que dice aquí pero hay una simplificación. Es un poco más sencillo de entender en la próxima ronda. Por eso lo utilicé. Cuando digo semana allí en realidad es un periodo de siete días corridos. En el momento actual, siete días antes. Es lo que consideramos la ventana para estos umbrales de emergencia.

El último elemento que tenemos en el programa de continuidad del servicio es lo que llamamos el operador de registro del backend de emergencia o EBERO. Una vez que podemos monitorear los gTLD, los servicios de registros, tenemos los umbrales de emergencia en los contratos que especifican lo que se puede hacer en caso de llegar al umbral con este elemento, el EBERO.

Son proveedores que contratamos, que están en contrato, que se pueden activar 24/7 y que temporariamente se pueden activar para asumir un gTLD dado en cuanto a las funciones críticas. DNS, DNSSEC, EPP, RDAP y la custodia de los datos o Data Escrow.

Hemos utilizado el elemento EBERO siete veces desde que comenzamos el programa con el lanzamiento de la ronda de 2012. Hemos asumido siete gTLD enviados a EBERO. Pudimos restaurar el servicio con gran rapidez. En caso de que les interese saber más de estos casos, tengo una presentación sobre este tema, que voy a hablar de este tema en el día técnico de la ccNSO. Si están anotados en el archivo van a encontrar en reuniones previas este tema y creo que aquí termina mi presentación.

PETER KOCH Gracias, Francisco. Quiero avanzar al siguiente operador. El orador es Régis Massé, que va a hablar de la observación como CTO de APNIC.

RÉGIS MASSÉ

Otra vez yo. Le voy a dar algo de testimonio sobre las cosas, sobre recuperación de desastre y lo que vemos en la vida real. En primer lugar es difícil definirlo pero hay algunas cosas más que el desastre propiamente dicho y el ciberdesastre. Tengo una visión bastante genérica de las categorías de amenaza.

Algunos de ustedes habrán visto el desastre en Corea del Sur hace un mes. Un centro de datos grande tuvo un incendio que duró 22 horas. Hizo caer más de 600 servicios gubernamentales. No el registro pero podría haber sido. Puede existir este tipo de problema si se ve afectado un centro de procesamiento de datos. Durante el mantenimiento, una batería nueva explotó y se incendió. Sucede.

Pasa en Francia también de vez en cuando. Tienen temas de ciberdesastres, recursos humanos y médicos, tensiones externas, financieros, tecnologías de infraestructura y falla de alimentación. Voy a compartir con ustedes. Hay un ejemplo reciente. Algo que sucedió hace un mes. Tengo la autorización del CEO de .MG para hablar de este tema. Lo conocemos bien porque es parte de la junta de APNIC.

El 25 de septiembre, el registro .MG sufrió un robo de noche. Se robaron todas las computadoras, equipos eléctricos. Sin ninguna herramienta de producción en las oficinas. La infraestructura de resolución de DNS no se vio afectada pero el sistema de registración y todos los elementos del mismo fueron robados con gran coraje porque son un equipo pequeño y nos pidieron ayuda y

tratamos de hacerlo pero también hubo ayuda de la comunidad de África.

Durante cinco días implementaron los procedimientos de recuperación que tienen implementados con nueva infraestructura de grabación en un operador local. Reinstalaron CoCCA con backups externos y restauraron la registración. Dijeron, creo, que estaban como antes y que estarán así para fin de año. Fue un problema grave, muy grave para ellos.

Esperamos que tengan procedimientos de recuperación de desastres pero no fue un desastre propiamente dicho. Fue un problema local. Quisiera acotar lo que decía Federico recién. Tienen respaldo, backup, fuera de las instalaciones del registro. Eso es importante porque es una manera de estar seguros de que pueda comenzar a partir de algo.

Algunos de ustedes conocen al CEO de .MG. Viene a menudo a ICANN. No pudo venir esta vez por los problemas que tuvo en su país pero le pedí que comparta con ustedes este tipo de cosas porque pueden suceder. Está la comunidad para ayudar a los registros, a todos los registros grandes o pequeños, cuando surgen estas cosas.

Por eso nuevamente las operaciones de TLD, todos los registros de esta lista todavía no están en TLD Ops. Si alguno los conoce, yo conozco a algunos. No soy un buen ejemplo pero si conocen alguno de estos, vamos a tratar el año que viene de ponernos en contacto con ellos y probarles que es importante ser parte de esta

comunidad, si quieren serlo. No es algo que obligatorio y hacen lo que desean al respecto pero creo que es importante.

Voy a compartir con ustedes alguna que otra cosita como estoy con tiempo. No está en la diapositiva pero estaba hablando de capacitación en la primera parte de la presentación y creo que la capacitación es una de las maneras que tenemos para estar seguros de tener en cuanto estas cosas.

Les voy a contar que en Francia hace un mes la Agencia Nacional de Seguridad organizó un ejercicio de crisis nacional y más de 1.050 organizaciones participaron en todo el país. No está en la diapositiva porque necesitábamos la autorización de la autoridad nacional para compartirlo en un evento internacional, por eso no está escrito. Sí tengo la autorización de contarles.

Hubo dos organizaciones que trabajaron juntas para ver si había una crisis de seguridad en una de las dos. La organización podría tener su propio proceso implementado y con sus propios equipos. Lo divertido de esto es que el ejercicio en Francia se dio el día en que había un paro nacional, que agregó un poco de tensión adicional al ejercicio. Llegamos al lugar del ejercicio a pesar de la huelga, fue un poco raro.

Se implementaron las unidades de crisis y deberían recibir un correo electrónico. En AFNIC decidimos adaptar el escenario y 18 unidades recibieron el mail durante el día del ejercicio de crisis y

tuvimos que adaptar los mails para nuestro registro con nuestros procedimientos, con nuestras tareas.

Para que el ejercicio sea más realista para los participantes con nuestro software, los nombres reales, mejoró el ejercicio. Las unidades de crisis pudieron hacer una prueba mejor y tomar mejores decisiones con el mecanismo y procedimiento propio.

Se recopiló información para aprender del ejercicio y ver qué elemento se puede consolidar y mejorar. El futuro próximo todavía no lo sabemos. Tenemos que preguntar al gobierno a ver si podemos compartir el ejercicio con la comunidad y adaptarlo para los ccTLD. Quizá puede llegar a ser interesante de alguna manera. La capacitación y la educación son muy importantes para entrenar a los equipos para este tipo de cosas. Siguiente diapositiva, por favor. Creo que es todo de mi parte.

PETER KOCH Gracias, Régis, por toda la información. Muchas gracias al TLD de Madagascar, por permitirle compartir la información. Tenemos tiempo para una o dos preguntas para Régis. Antes les voy a decir que tendremos una sesión interactiva con preguntas en Mentimeter al final. Si no lo tienen todavía conectado en sus laptops, vayan a menti.com, ingresen ese código o por favor escaneen este código QR. Le damos la palabra a Eberhard.

EBERHARD LISSE

Nosotros también utilizamos CoCCA y lo utilizamos en DAAR. Tenemos un hardware, no una máquina virtual, en un centro de datos en Alemania. Ellos también tienen ironDNS y también brindan servicios a varios registros. Es decir, su infraestructura incluye el failure automática a otro centro de datos. Es decir, automáticamente hacemos un backup de los datos cara dato en el mismo equipo y cada dos o tres horas en un segundo equipo fuera del continente.

Es una replicación pero si nuestro hardware falla, tenemos un equipo standby en el centro de datos que empieza a funcionar rápidamente. Incluso para los ccTLD saber qué hacer si pasa algo por el estilo aceleraría la recuperación. ¿Es importante si el problema dura unas horas o unos días si no se afecta al DNS? No podemos renovar, no podemos registrar, no podemos dar de baja. Mi pregunta, que era para Francisco en realidad, es cuando un TLD tiene algún problema, ¿qué pasa con DNSSEC? Necesitamos una clave DNSSEC en la raíz. ¿Qué pasa?

PETER KOCH

Es una pregunta técnica muy interesante. Sugiero que la dejemos para el final porque queremos ver todas estas preguntas. Si seguimos hablando de lo que usted dijo entramos demasiado en aspectos técnicos. Ahora, el equipo que preparó esta reunión presentó una serie de preguntas. Entramos al Mentimeter y empezamos con la primera pregunta. Es: ¿Trabaja usted con una ccTLD o lo representa? Esto es para que se familiaricen con el

sistema. Invitamos a los que están presentes aquí, les decimos que cuando se hace una pregunta que tiene que ver específicamente con los ccTLD, que solo contesten las personas que trabajan con un ccTLD. No es obligatorio pero sería bueno que respeten esta sugerencia. Dicho esto, tenemos cinco personas por lo menos aquí que no son del mundo de los ccTLD. Bienvenidos.

La próxima pregunta. ¿Su TLD o su ccTLD tiene un plan de recuperación de desastres y continuidad de operaciones? Muy bien.

ROELOF MEIJER Tosas las respuestas tienen colores parecidos. El azul sería sí, el no debería ser amarillo. Hay un problema con los colores. Estoy un poco confundido.

PETER KOCH ¿Nos podrían explicar, por favor, qué significan los colores? ¿Está tomando esto en cuenta las respuestas a la pregunta anterior? Sí. No estaba tan confundido como pensé. Hay muchas respuestas de sí y de no son las personas que contestaron no sé en la pregunta anterior. Aquí tenemos un 81 %. El equipo que preparó esto está muy satisfecho por el grupo con el que estamos trabajando porque aquí hay gente de gTLD y otros que no lo son. ¿Alguien quiere agregar algo en forma verbal a sus respuestas? ¿Alguien quiere agregar algo, hacer una intervención oral? No. Pasamos a la siguiente pregunta.

Por favor, diga en qué medida está de acuerdo con la declaración que aparece abajo. Mi TLD puede recuperarse de sus operaciones después de un desastre dentro de las 24 horas. También pueden compartir lo que creen que es. Cuál creen ustedes que es la respuesta. Otra vez, un 80 % de las respuestas son positivas. Cuatro de cinco. Es un poco menor de lo que vimos antes, entre aquellos que sí tenían un plan. Quizá esto sea interesante para las personas de organizaciones que no tengan un plan. Muchas gracias. Vamos a tomar esta información. ¿Hay alguien que quiera decir algo con respecto a qué contestó y por qué contestó lo que contestó? No. Muy bien. Pasemos a la siguiente pregunta.

EBERHARD LISSE: La próxima vez no utilicen esta barra deslizante porque se desliza un poco y no siempre tenemos una respuesta precisa. Debemos utilizar columnas y no una barra deslizante.

PETER KOCH: Lo que usted dice es correcto pero aquí estamos simplemente viendo cuál es la opinión general. No es un ejercicio científico. Igual vamos a tener en cuenta su sugerencia. ¿Qué parte de sus operaciones es más vulnerable en una situación de crisis? Seleccione todas las que correspondan, todas las respuestas correctas.

La resolución de DNS aparentemente tiene mucha importancia. Interferencia legal y gubernamental. Esto es interesante. El sistema de registro. ¿Alguien quiere decir algo con respecto a otros?

ROELOF MEIJER Roelof, de .NL. La resolución del DNS, sistemas de registros, gestión de las claves de DNS, continuidad de la organización. Todas esas son operaciones. ¿Qué tiene que ver la interferencia legal o gubernamental? No es un tema de operaciones. Es una interferencia.

PETER KOCH Es interesante que tantas personas hayan elegido esto. Una vez más, quizá la redacción no sea la mejor. Les pido disculpas por esto. En este caso la interferencia no puede ser vulnerable pero los sistemas se volverían vulnerables si hay intervención gubernamental o de los entes reguladores. Espero que se haya entendido así, porque así es como lo pensamos al redactar esta pregunta.

¿Hay alguna otra pregunta o alguien tiene algún comentario? ¿Alguien quiere decirnos por qué eligió lo que eligió? ¿No? Todos quieren formar parte del gran grupo. Está bien. Creo que queda una más, ¿no? Una palabra. Queremos crear una nube de palabras. ¿Qué es lo que más le preocupa cuando hablamos de la continuidad de su ccTLD? Sucesión. Conocimiento. Conciencia

acerca de la seguridad. El cisne negro. ¿Podrían explicar algunas de las cosas? El cisne negro. Adelante. Explíquenos esto, por favor.

ROELOF MEIJER Un cisne negro es algo totalmente inesperado. Algo en lo que nunca se había pensado hasta que sucede.

PETER KOCH Gracias. Bien. A ver si se estabiliza. Podemos parar aquí. Este es un resultado muy interesante o no centrado en la geopolítica considerando el trabajo que hacemos todos juntos en la gobernanza de Internet mundial. Muchas gracias. Creo que hay una más, ¿no?

CLAUDIA RUIZ Tenemos dos más.

PETER KOCH Imaginen que su ccTLD dejara de funcionar o de operar mañana. Cuál sería la mejor forma en que la IANA les podría ayudar. Muchas gracias. Se ve que estamos llegando al final del día. Tomemos todo lo que tenemos aquí, en la pantalla, en cuenta. ¿Hay alguien que quiera explicar alguno de estos puntos? No. Vamos a la última pregunta de esta sesión entonces.

¿Qué es lo que le gustaría que su ccTLD tuviera hoy para mejorar su situación y estar mejor preparados en el caso de un desastre? Custodia en mayúscula y en minúscula. Muchas gracias. Con esto

terminamos con esta parte. Vamos a llevar todo este material al grupo de estudio. Muchas gracias por participar en forma activa. Esto es muy importante. Espero que también lo hayan pasado bien. Preparar la sesión o las preguntas por lo menos fue entretenido.

Todavía no terminamos la sesión. Me queda agradecerles a Kim Davies, Francisco Arias y Régis Massé, por sus aportes. Al equipo que preparó esta sesión, la secretaría y el personal de TI que hizo que esto fuera posible desde el punto de vista técnico. También los miembros del grupo de estudios. Si les interesa quizá incorporarse a este grupo de estudios todavía pueden hacerlo. Si quieren información más detallada y quieren saber cuál es el mandato y qué compromiso deberán asumir al participar del grupo, acérquense a mí y a mis colegas o a los miembros del consejo y les podemos dar esta información. Les damos la bienvenida a todos los voluntarios. Con esto quiero agradecerles a todos y cerrar la sesión. Se levanta la sesión.

[FIN DE LA TRANSCRIPCIÓN]