ICANN84 | Reunión General Anual – Reunión conjunta: GAC y SSAC
Martes, 28 de octubre de 2025 – 15:00 a 16:00 IST

NICOLÁS CABALLERO: Damas y caballeros, bienvenidos nuevamente. Por favor, tomen asiento. Vamos a dar inicio en un minuto.

GULTEN TEPE: Bienvenidos a la reunión del GAC con el SSAC el martes 28 de octubre a las 15:00 UTC. Por favor, tomen nota de que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN, el código de conducta de los participantes de la ICANN y la política antiacoso de la comunidad de la ICANN. Durante la sesión se leerán en voz alta las preguntas y los comentarios si se presentan en el formato adecuado en el chat de Zoom.

Hay interpretación de esta sesión en los seis idiomas de Naciones Unidas más portugués. Si quieren hablar durante la sesión, por favor, levanten la mano en la sala de Zoom y digan su nombre para los registros y el idioma en el que hablarán si no lo hacen en inglés. Por favor, hablen a una velocidad razonable para permitir una interpretación correcta. Ahora le doy la palabra al presidente del GAC, Nicolás Caballero. Gracias.

NICOLÁS CABALLERO

Muchas gracias, Gulten. Bienvenidos nuevamente. Espero que todos hayan disfrutado del fantástico café irlandés. Tengo el placer de presentar a un muy buen amigo, Ram Mohan, del SSAC. También tenemos a Suzanne, Maarten y Tara. Bienvenidos. Vamos a tener una reunión muy interesante, al menos desde mi punto de vista dividida en cuatro partes. La primera y la más importante obviamente según mi opinión tiene que ver con la importancia de un software libre y de código abierto en la industria del DNS. Sé que hay otros también.

También lo que tiene que ver con la colisión de cadenas de caracteres similares, el uso indebido del DNS, que es casi inevitable en este momento y después de la posibilidad de cooperación entre el SSAC y el GAC. Después de todas estas presentaciones habrá tiempo para preguntas y respuestas. Ahora le voy a dar la palabra a Ram Mohan, mi buen amigo.

RAM MOHAN

Es un placer, Nico, estar aquí nuevamente con ustedes en Dublín pero también con ustedes en el GAC. Realmente ha sido un honor para nosotros que ahora, después de varias reuniones, ustedes hayan seguido invitándonos, dedicarnos un tiempo dentro de su agenda tan abultada porque además valoramos este tiempo con ustedes. Nos hemos preparado intensivamente para esto. Queremos asegurarnos de que la información que brindemos en la comunicación, las interacciones que mantenemos con ustedes

estén el nivel correcto pero también que sean información sobre la que puedan tomar acciones.

Esta es la base de lo que nosotros hemos preparado. Es por eso que, sin más, lo que querría es concentrarme en la primera parte, que tiene que ver con la importancia de un software libre y de código abierto en la industria del DNS, y presentar este tema, hablar algunos detalles con ustedes. Ahora le voy a dar la palabra a Maarten Aertsen, que es uno de los copresidentes del grupo de trabajo sobre este tema. Maarten.

MAARTEN AERTSEN Gracias, Ram. Gracias, Nico. Hoy voy a hablar de software. El SSAC en general escribe documentos que son bastante técnicos pero este no es uno de ellos. La comunidad de la ICANN en sí misma no es su público. Esto está redactado para los reguladores y los formuladores de políticas de todo el mundo. Es por eso que creo que estoy en el lugar correcto. Si no son ustedes, supongo que tienen colegas que sí se encargan de la ciberseguridad. Es por eso que vamos a hablar de software. Perfecto.

Si condensamos el informe en una única oración nos damos cuenta de que el DNS está construido en un software libre y de código abierto. Esto no es nada más que para defender que el software libre y de código abierto es mejor sino que es una declaración sobre cómo el DNS está realmente construido.

FOSS significa software libre y de código abierto. Libre significa libre, como libertad de expresión, y no precio, como por ejemplo una Guinness gratis después de esta charla. FOSS está definitivo por cuatro libertadas. De uso, el estudio, porque se puede estudiar el código, de intercambio, porque se puede redistribuir copias del software y después modificación o cambio, porque lo pueden cambiar según lo necesiten y además después compartir estos cambios.

Estas cuatro libertades generan un ecosistema fundamentalmente diferente para el desarrollo del software pero también para la distribución y el mantenimiento en comparación con los que son software de propiedad exclusiva. Hay una diferencia filosófica entre lo que es el software libre y el código abierto, porque aquí en FOSS tenemos los dos conceptos concentrados en estas cuatro libertades. Siguiente imagen.

El modelo de FOSS tiene distintos perfiles de riesgo diferentes de los de un software de propiedad exclusiva. En general este software libre de código abierto es mantenido por los voluntarios, donde la motivación realmente tiene un rol fundamental. Si una persona está trabajando en software como voluntario, también puede sufrir un agotamiento profesional y abandonar un proyecto.

Es por eso que otro de los riesgos de FOSS es que no existe ninguna garantía, ningún apoyo garantizado por defecto. Los operadores necesitan entonces asumir la responsabilidad para retener dentro de sus empresas a quienes tengan un conocimiento específico para

hacer el desarrollo, solucionar problemas de software o también generar contratos donde esto suceda.

No se trata entonces de voluntarios sino que son las organizaciones profesionales las que asumen este desarrollo de software. Tenemos estos beneficiarios gratuitos, donde puede haber una situación donde el financiamiento no está vinculado al uso, donde quien hace el mantenimiento se basa en una iniciativa que le paga a los mantenedores pero esto genera diferencias en el financiamiento que tiene que ver con nuevas cargas regulatorias. Por ejemplo, un modelo de financiamiento puede verse amenazado. Esto es real y es lo que sucede en el modelo FOSS. La reglamentación que no considera estas concesiones puede empeorar estos riesgos o mejorarlos. Siguiente imagen.

También hay algunas fortalezas en el modelo FOSS. Aquí vamos a hablar específicamente del DNS. En la transparencia anterior hablábamos de FOSS en general pero cuando miramos al DNS en particular podemos ver que hay mayor transparencia y una seguridad de colaboración porque las comunidades, tanto académicas como operativas mantienen una cultura activa y robusta sobre la revisión del software de DNS en FOSS. Esto sucede durante décadas.

Podemos ver documentos del 90 donde hay fallas en FOSS y que fueron tratadas de solucionar, que es lo que sucede en la realidad y los operadores que nosotros encuestamos, fueron más de 100, que pudieron realmente diagnosticar, verificar y solucionar los

problemas de las vulnerabilidades porque no dependen de un proveedor sino que pueden actuar proactivamente en caso de fallos.

En el DNS en particular hay distintos proyectos de DNS que son mantenidos por los voluntarios y también por organizaciones de larga data y estables. Esto significa mantener la implementación de software durante más de 20 años. Esta longevidad genera entonces un registro sobre el que confían los operadores.

Otra de las fortalezas del FOSS en el DNS es que hay una flexibilidad operativa a través de la diversidad porque puede haber distintas implementaciones de FOSS para que los operadores hagan correr distintos software, que ejecuten distintos software y bajan los obstáculos para las organizaciones para tener su propia infraestructura, lo que evita el riesgo de concentración. Se vio en un tema candente reciente los equilibrios entre entidades extranjeras y sus dependencias.

Vamos a hablar ahora de seguridad. El SSAC se concentra en la seguridad y es muy importante entender qué significa seguridad en software porque la seguridad no está determinada por un código abierto o un código cerrado. Tampoco si los desarrolladores están pagados o son voluntarios. Tampoco lo determina si el software proviene de una empresa comercial o sin fines de lucro. Lo que sí determina la seguridad tiene que ver con la revisión del código, cómo está disponible esta revisión y también mantener la sostenibilidad de los recursos para mantener este software.

Tenemos en este caso que considerar la calidad de los procesos de desarrollo y mantenimiento, y no la visibilidad del código fuente. Escuchamos muchas veces que nos dicen: ¿FOSS es más o menos seguro que el software de propiedad exclusiva? La respuesta es ni uno ni lo otro. La seguridad está determinada por la calidad del proceso de desarrollo y no por el modelo de otorgamiento de licencias. El desafío de la política es que FOSS tiene un perfil de riesgo diferente. No se puede hacer copiar y pegar de lo que sucede en el mundo del software de propiedad exclusiva para llevarlo a la realidad del FOSS.

Al principio dije cosas muy importantes pero ahora voy a mostrar datos sobre eso. Vamos a comenzar con el sistema de servidor raíz. Hicimos una encuesta a los 12 operadores de servidores raíz para tratar de identificar el software que utilizaban. Vimos una dominancia del software libre y de código abierto. 9 de los 12 operadores de servidores raíz utilizan software libre y de código abierto exclusivamente. Incluso los operadores que utilizan un software de propiedad exclusiva para esto en general también ejecutan FOSS al mismo tiempo. No se trata de un porcentaje bajo sino que es la gran mayoría que utiliza FOSS dentro del DNS.

Vamos a ver ahora a los operadores de TLD, dominios de alto nivel. Estas entidades tienen servicios autoritativos de DNS y lo que encontramos es que los operadores que sirven a la gran mayoría de TLD, 9 de 10 utilizan FOSS como infraestructura del DNS. Para esta

audiencia quizá sea mucho más pertinente saber cómo funciona en el ámbito de cada uno de los países con dominios de alto nivel.

Podemos ver que 20 de los 25 operadores de ccTLD utilizan FOSS. En general, los operadores atienden a 234 ccTLD exclusivos que utilizan FOSS y esto es nada más que en el ámbito que vimos estos resultados. Pueden ser aún mayores esas cifras. Esto no es para operadores experimentales sino los que atienden a cientos de nombres de dominio. Por ejemplo, Nominet en el Reino Unido, CNNIC en China, nada más que para nombrar a algunos.

Vamos a ver los sistemas de registros que son las bases de datos que aguardan los dominios dentro de los TLD. Vemos dos modelos. El primero de los modelos completamente es FOSS. Existe, no es una mayoría pero sí muestra que es posible. Es un punto importante.

El modelo más popular es donde tenemos los registros con propiedad exclusiva pero aquí podemos ver que estos sistemas de propiedad exclusiva no empiezan desde cero sino que son integraciones que corren por encima de las plataformas con software libre y de código abierto. Incorporan elementos de FOSS. Si bien hablamos de propiedad exclusiva, el fundamento, la base es FOSS.

Vamos a hablar ahora del ecosistema de los resolutores que es más difícil. Aquí sí vemos que hay un gran uso, una presencia sustancial de software libre y de código abierto. El 80 % de los usuarios de todo el mundo utilizan un resolutor local y aquí FOSS es lo

dominante, incluso cuando miramos las soluciones comerciales y sabemos que existen muchos, en la mayor parte de los casos, cuando vemos dentro de lo que venden, encontramos FOSS.

Lo mismo se aplica a los resolutores públicos. Muchos de ellos son FOSS. Hicimos por ejemplo un caso de estudio en CloudFlare donde tiene un núcleo de propiedad exclusiva per que está rodeado por FOSS. También tenemos que los hiperescaladores más importantes utilizan FOSS para la resolución del DNS y otros utilizan las bibliotecas de FOSS como resolutores.

Vamos ahora a la siguiente imagen. Lo que podemos citar entonces del informe es que en las partes más críticas de la infraestructura del DNS FOSS es la norma. El software de propiedad exclusiva es la excepción. No es una exageración sino que es lo que nosotros hemos encontrado en la investigación rigurosa que hicimos. También podemos hablar de sistemas de nombres que tienen un software desarrollado de manera colaborativa y distribuido de manera gratuita. Siguiente imagen, por favor.

El abordaje regulatorio para la cadena de suministro tradicional impone algunas condiciones en términos de seguridad y normas, y las impone a los operadores de la infraestructura crítica. En general, los consideran responsables en caso de falla y hay requisitos que se establecen a los proveedores a través de los contratos.

Con FOSS se supone que puede no haber una relación de proveedor en el sentido tradicional. No hay un contrato de

operación. No hay un proveedor con el cual establecer una regulación. Es algo voluntario. Supone este modelo de proveedor y cliente con transacciones financieras. Eso en el modelo tradicional pero aquí no lo hay.

Al imponer una carga de cumplimiento sobre los operadores se afecta la cadena de suministro y esto puede ocasionar una desestabilización de las pequeñas organizaciones que mantienen el software. Si son voluntarios, pueden utilizar la posibilidad de abandonar su proyecto, cambiar de licencia propietaria o evitar determinadas jurisdicciones. El software, del que todos dependen, acaba estando menos disponible y siendo menos seguro.

Hicimos algunos estudios de caso porque en algunas jurisdicciones como Estados Unidos, el Reino Unido, la Unión Europea han desarrollado políticas que tienen en cuenta FOSS. No voy a entrar en todos los detalles a menos que exista el interés para que lo haga pero esto se puede hacer. Siguiente, por favor.

Estas son las cinco directrices sobre las cuales se puede actuar y que nosotros desarrollamos. SSAC es indiferente si ustedes quieren regular o no. No tenemos posición al respecto pero si ustedes consideran aplicar regulaciones, por favor, tengan en cuenta el papel crítico que tiene FOSS. Reconozcan que la infraestructura global depende de FOSS y que es necesario que se preserve.

También consulten con la comunidad de código abierto, con la comunidad FOSS. Hablen con las entidades encargadas del mantenimiento, con las fundaciones y los operadores de desarrollo

de políticas y eviten las consecuencias no intencionales. También utilicen casos contemporáneos para entender cuáles son los efectos, los modelos emergentes. Incentiven la sostenibilidad del FOSS a través de distintos recursos y aborden los riesgos sistémicos que existen en el espacio de software en general, no solamente en FOSS, de manera colectiva. Encuentren soluciones para todo el ecosistema en lugar de poner la carga en entidades de mantenimiento individuales. Creo que con esto llego al final de esta presentación y espero sus preguntas.

MARCO HOGEWONING Gracias, Maarten, por esta presentación tan completa. También a Ram le agradezco. Los aliento a todos a leer el informe que se mencionó anteriormente. Tenemos tiempo para algunas preguntas. La primera la hace alguien que está a mi lado. Vamos a la Comisión Europea en primer lugar.

GEMMA CAROLILLO Gracias, señor Presidente y vicepresidente. Nico, si usted quiere hablar primero, puede hacerlo. Continúo. Soy de los que están recibiendo esta información con tres de los cuatro estudios de caso. Esto es sumamente importante para nosotros.

Nosotros, como entes reguladores, también hemos aprendido a lo largo del proceso respecto de cómo incorporar las distintas características del código abierto en la reglamentación sobre cuestiones digitales. Ha sido un proceso doloroso pero también

muy útil y hay un aprendizaje colectivo en este sentido. Estamos logrando buenos resultados por el momento.

Mi pregunta tiene que ver con la seguridad de la cadena de suministro. Esto sigue siendo un problema. Aun cuando tratemos de evitarlo, sigue siendo un problema. ¿Tienen alguna postura con respecto a iniciativas con respecto a las listas de materiales para el software y cómo esto podría abordar la cuestión de la seguridad en la cadena de suministro?

MAARTEN AERTSEN Gracias, Gemma. ¿Me está preguntando si SSAC tiene una opinión sobre la lista de materiales de software? Lamentablemente, hablando en nombre del SSAC, no hemos analizado esa medida en particular. Le puedo compartir mi opinión personal pero esta es la exención de responsabilidades que tengo que hacer.

Sí. Hay un problema en el espacio de software con la seguridad cuando hablamos de software propietario y también de software de código abierto. Creo que la lista de materiales de software puede ayudarnos cuando alguien, una organización adquiere software que es propietario pero más que nada está construido sobre la base de FOSS porque aquí es donde entramos en una situación, donde un componente es vulnerable y es vulnerable para todos. Incluso para los productos que están en el mercado. Si no se sabe qué es lo que hay dentro como proveedor, incluso como comprador, cómo puede comenzar a corregir las cosas. En ese

sentido es un instrumento interesante. También en sus primeras etapas.

Realmente le agradezco por su comentario sobre el aprendizaje colectivo. Yo ahora estoy hablando a título personal pero me parece fascinante ver el proceso de desarrollo de políticas, cómo se dio en la Unión Europea y estoy muy contento de que tengamos un estudio de caso que pudiéramos incluir en este informe.

MARCO HOGEWONING Gracias, Comisión Europea. Gracias, Maarten. Le voy la palabra a Bangladesh. Luego cerraré las intervenciones con el presidente.

DR. SHAMSUZZOHA Muchas gracias por esta presentación tan completa, sobre todo siendo de una organización que trabaja con distintos organismos de normalización en Bangladesh. Creo que esto es muy interesante. En dos sentidos, por un lado trabajando con el ccTLD de Bangladesh con las normas de seguridad y los procedimientos para asegurarnos de tener también el software correcto y, en segundo lugar, colaboramos con quienes están a cargo de la infraestructura crítica, viendo las soluciones que podemos tener para la ciberseguridad.

Considerando el sistema de compras, en el gobierno estamos promoviendo la compra de software de código abierto pero uno de los argumentos que nos plantean tiene que ver con la capacidad inherente del FOSS en lo que respecta a los cambios. Si uno no

tiene capacidad para hacer los cambios, esto es un gran riesgo a toda la infraestructura nacional y también puede llevarnos a un gran costo. Quisiera saber cómo ven el tema de la infraestructura crítica sensible en este sentido.

MAARTEN AERTSEN

En ese sentido creo que hay menos diferencia entre el software propietario y el FOSS. Es menor la diferencia de lo que uno esperaría porque si uno opera la infraestructura crítica, el operador tiene la responsabilidad de hacer que todo funcione de manera ininterrumpida y si deciden utilizar FOSS, lo que la mayoría decide en realidad, entonces tienen un conocimiento interno que representa un costo. Por supuesto, necesitan contratar expertos o tienen que encontrarlos en otra parte. En muchos casos, si ustedes se fijan en el software más popular, estas organizaciones están financiadas a través de contratos para brindar soporte. Si solamente hablamos de software propietario, tal vez pagarían un costo por licencia y posiblemente recibirían soporte.

Creo que no hay una gran diferencia en ese sentido considerando todas las fortalezas que se vieron en la presentación. Podemos tener una diferencia que no haya que atarse a un único proveedor pero la infraestructura crítica es especial porque tiene estos requisitos donde se necesita el conocimiento especializado, la pericia. Cada operador puede elegir dependiendo de cuánto ancho de banda le da el gobierno para justamente tomar esas decisiones.

MARCO HOGEWONING Gracias a ambos. Le voy a dar a Nico la palabra. Es un gran defensor de FOSS.

NICOLÁS CABALLERO Voy a ser muy breve. Gracias, Maarten por esta presentación fantástica. ¿Podría brevemente hacer un comentario sobre cómo el código abierto evita estas situaciones en que uno está atado a una determinada entidad, sobre todos los países en desarrollo? No solamente desde el punto de vista de costo sino desde el punto de vista… Lo voy a decir así. Los costos de ciberseguridad.

MAARTEN AERTSEN Estar atado a un proveedor significa que uno decide invertir en un cierto producto y luego no puede migrar porque la investigación que hicieron es demasiado grande y los costos para cambiar de proveedor son muy altos. Incluso en la ciberseguridad, cuando uno queda atado a un determinado proveedor no está obligado a mantener la relación con la entidad de mantenimiento original. A veces hay otras organizaciones que le pueden dar apoyo en la implementación, sobre todo para la aplicación de parches pero siempre va a depender del desarrollador original, para que desarrolle los parches. No es como en el caso del software propietario, donde solamente hay una entidad con la que tiene que trabajar.

Tal vez un país con un presupuesto más pequeño podría ver esto como un impulso a la innovación para desarrollar ese conocimiento especializado a nivel local en lugar de tener que pagarle a otras entidades fuera del país, pero supongo que esto es algo que deben elegir. Eso es lo que puedo decir con respecto a estar atado a un proveedor. Esta es mi opinión personal porque no hacemos referencia a esto en el informe.

MARCO HOGEWONING: Gracias, Nico, por la pregunta. Gracias, Maarten, por su respuesta. Creo que por cuestiones de tiempo vamos a pasar a la siguiente parte, el siguiente tema. Quiero decir que invitamos a SSAC para que también nos ayudara a desarrollar capacidades y sobre todo para beneficio de los miembros más nuevos del GAC que están aquí en la sala. Este es un tema relativamente nuevo pero está cobrando cada vez más importancia a medida que nos acercamos a la próxima ronda. Le voy a dar a Suzanne la palabra, creo.

SUZANNE WOOLF: Gracias, Marco. Gracias, Maarten. Siempre es un placer hablar después de usted. Como dijo Marco, a mí me toca hablar de NCAP, la colisión de nombres. Yo estoy a cargo del proyecto de análisis de colisión de nombres, que fue algo originalmente propuesto por SSAC pero luego fue desarrollado por un grupo en toda la comunidad.

Como dijo Marco, primero teníamos algunos desafíos con la colisión de nombres a raíz de la ronda anterior pero tuvimos que revisarlo porque hubo algunas cosas que cambiaron desde la tecnología y las expectativas y también el ecosistema en el que tenemos que movernos. Volvemos una atrás, por favor.

¿Qué es una colisión de nombres? Es muy difícil definir la colisión de nombres. Se dan esas cosas en las que es muy difícil verlo, identificarlo rápidamente. Podemos pensar en una analogía. Los nombres de dominio como direcciones de una casa. Si dos casas tienen la misma dirección, es difícil entregarle el correo, los productos del mercado. Hay cuestiones de seguridad. Piensen en las implicancias desde la seguridad.

En el DNS, las colisiones de nombres ocurren cuando un dominio utilizado en el espacio de nombres global de DNS también se utiliza en un espacio de nombres diferente. Por ejemplo, de una empresa privada. Puede ser un proveedor de VPN, donde se utilizan distintos nombres que son válidos y eso está bien pero si es el mismo nombre, lo que uno busca puede ser interpretado erróneamente y genera confusión rápidamente. Siguiente, por favor. Las próximas diapositivas las voy a ver bastante rápido porque vamos a evitar los detalles para tratar de llegar a hablar en un nivel general pero esta presentación va a estar disponible y con gusto siempre podemos entrar en los detalles técnicos.

¿Qué no es una colisión de nombres? Algunos de estos términos quizá les resulten conocidos porque los pueden haber visto en la

guía del solicitante o el trabajo que tiene que ver con los nuevos gTLD. La colisión de nombres no es lo mismo que una similitud en cadenas de caracteres o cadenas de caracteres confusamente similares.

La colisión de nombres es un problema técnico que genera cuestiones de estabilidad y seguridad porque se delega exactamente el mismo TLD que se utiliza en un contexto privado. Por ejemplo, example.corp en una red pública puede ser lo mismo que example.corp en la Internet abierta y esto podría generar problemas.

Los riesgos son entonces que las consultas por los nombres privados pueden filtrarse al DNS público y generar entonces conflictos técnicos y fallas de seguridad. La similitud en la cadena de caracteres también es un desafío para el proyecto de nuevos gTLD y la guía del solicitante, pero también tiene que ver con la percepción del usuario. Esto tiene que ver con la posibilidad de confusión a través de diferentes TLD públicos que pueden sonar o pueden verse iguales según el ojo humano.

Aquí tenemos .example, con una l minúscula, y un .exampIe con una i mayúscula. Esto puede resultar confuso para el ojo humano y ahí entonces tenemos posibilidades de falla de confianza, phishing, fraude. Esto impacta en los usuarios. Lo que tenemos que recordar es que siempre hay temas de colisión que pueden surgir.

El tema es que cuando la computadora confronta esta similitud puede haber entonces resultados peligrosos y confusos. Es por eso

que, dejando los detalles técnicos de lado, hay que entender que la colisión de nombres es importante para la seguridad de Internet y que tiene que ver con la responsabilidad de la ICANN para la estabilidad, seguridad y flexibilidad de Internet. Hay consecuencias cuando las empresas han utilizado nombres de sus TLD internos, que pueden filtrarse a la Internet global. También si tenemos más gTLD tenemos más posibilidades de tener estos problemas porque hay más nombres que pueden ya estar siendo utilizados en contextos privados pero que también pueden delegarse al espacio de nombres públicos.

Medir la colisión de nombres resulta difícil porque hay una infraestructura de red y tecnología que evoluciona, sobre todo cuando hablamos de la última ronda de gTLD. Ha habido mejoras en la privacidad en el DNS que hace más difícil qué es lo que está sucediendo, porque son las mejoras en la privacidad, también sistemas de nombre alternativo que han hecho que el panorama del DNS sea más complejo y que sea más difícil de medir. Por favor, una transparencia más para adelante. Gracias.

En el 2012 hubo una nueva ronda de gTLD que aceleró el crecimiento y dijo: “¿Qué es lo que va a pasar cuando se agregan nuevas cadenas de caracteres que ya quizá estén utilizados en otro contexto que no sea el público?” En el 2013 el SSAC tomó este tema y emitió un asesoramiento resaltando los problemas significativos de seguridad y estabilidad que podrían resultar de las colisiones de nombres.

La colisión de cadenas de caracteres más importantes detectadas fueron en el caso de .HOME, .CORP y .MAIL, que se utilizaban en el contexto privado y hubo muchos datos, muchos riesgos para identificarlas y tratar de delegarlas en el sistema de nombres de dominio públicos.

En el 2017 la junta directiva de la ICANN le pidió al SSAC que realizara estudios amplios para permitir las posibles futuras delegaciones de gTLD en una manera predecible, segura y estable. Hubo dos proyectos que surgieron de esto y entonces también generaron algunas otras preguntas. En la etapa final, tuvimos el estudio dos del NCAP, que fue publicado en 2024, porque queríamos asegurarnos de que los hallazgos que tuvieran pudieran unirse y que se realizaran recomendaciones para formar parte de la próxima ronda de nuevos gTLD. Teníamos un equipo de toda la comunidad, no solo miembros del SSAC. Eso funcionó bien para nosotros. Fue bueno pero obviamente tomamos el trabajo anterior con investigación más reciente. Siguiente, por favor.

Lo que teníamos que llevarnos del proyecto NCAP era analizar la situación actual que tenía que ver con luchar y mitigar la colisión de nombres. También pensar en todo esto para la próxima ronda. Esto también tenía que ver no solamente con ver cuál era la colisión de nombres sino ver cuáles eran las medidas posibles que se podían tomar para evitarlo.

Tenemos que señalar que la evaluación fue mucho más difícil por distintos motivos. Ya estamos hablando de esto pero lo más difícil

es la cantidad de nombres en los datos que se buscan. Esto también tenía que ver con los que se utilizan en el ámbito privado. Esto puede ser bueno para los usuarios pero no para el esfuerzo que nosotros estamos realizando para entender.

Hubo grandes desafíos para enfrentar en el camino pero pudimos trabajar con lo que teníamos y pudimos cumplir con los objetivos. El número 1 era garantizar que podía evaluarse la colisión de nombres y, habiendo dicho esto, tenemos un marco de niveles de examinación que pueden ser escalables en cuanto a los detalles para ver qué es lo que está presente dentro de determinadas colisiones de nombres.

El objetivo número dos es darle un proceso a la ICANN para poder evaluar planes de mitigación y remediación en el caso de colisiones de nombres identificadas. Lo que vimos es que, más que en el pasado, todos estos casos al menos van a ser muy diferentes unos de otros. Siguiente, por favor.

No vamos a tomar examen pero este es el diagrama que está en el informe y que surgió del estudio dos de NCAP. Tomar en consideración las colisiones de nombres y los desafíos que enfrentamos en el futuro. También tiene que haber un equipo técnico para realizar una revisión y enviar sus informes a la junta directiva.

Suponemos que en muchos casos no tiene que haber un riesgo continuo porque la mitigación y la prevención son posibles pero, como no son iguales los dos casos, podemos ver que se necesita de

mucho juicio específico para saber que se está enfrentado bien el tema del riesgo de colisión de nombres. Hay un marco que tiene que ver con medios automatizados y quizá otro que se dirija a un panel de expertos, un equipo de expertos, que es lo que utiliza la ICANN en otros contextos donde los problemas pueden complicarse, donde necesitamos de cierto juicio y evaluación para informar y dar forma al proceso.

Los beneficios de este marco de evaluación de riesgos de colisión de nombres, que es el estudio dos de NCAP y que fue lo que se publicó para toda la comunidad, es que las funciones tienen que ver con una gestión de riesgos proactiva, identificar los riesgos de colisión de nombres y permitir el desarrollo y revisión de estrategias de mitigación antes de que causen daño.

Tratamos de trabajar para el marco sea uniforme y eficaz, un enfoque centralizado que garantice una evaluación de riesgos profunda y mitigación en todas las aplicaciones de los nuevos gTLD. Debido a la responsabilidad también para la zona raíz trabajamos con ICANN. El marco está impulsado por los datos. Es decir, tiene decisiones informadas para la expansión segura del espacio de nombres de Internet y también pudimos enfrentar varias de las inquietudes de privacidad, porque si bien el riesgo es inherente en la evaluación de colisiones de nombres, el riesgo de la privacidad que encontramos es que el riesgo de privacidad no puede evaluar con precisión y exactitud las colisiones de nombres. Es mayor que los riesgos asociados con la evaluación.

Nosotros creemos que el riesgo de privacidad de no evaluar exactamente la colisión de nombres es mayor que el riesgo asociado con la evaluación. El riesgo de actuar en comparación con el de no actuar, esto nos da una herramienta adicional para analizar este tipo de casos. En realidad la detección temprana del riesgo y la mitigación informada son cruciales para la seguridad y la estabilidad del DNS. Este entonces es un pantallazo general. No sé si hay tiempo para preguntas.

MARCO HOGEWONING Gracias, Suzanne. Agradecemos mucho. Me parece que el tema de la colisión me quedó un poco más claro para ver que colisión de nombres no es lo mismo que cadena de caracteres similares. Vamos a seguir hablando con el SSAC durante todo el año. No veo a nadie. Nico, no sé si quiere decir algo al respecto.

NICOLÁS CABALLERO ¿Podemos volver a la página 23? Perfecto. Aquí tenemos cuatro pasos y mi pregunta tiene que ver con los plazos. En promedio, ¿cuál es el plazo? Estamos hablando de días, semanas, meses, porque quería comparar esto con los 32 pasos. No sé si recuerdan ayer que hubo una presentación con la GNSO y estuvimos hablando de la eficiencia y la velocidad y de muchas otras cosas. En promedio, ¿cuánto llevaría todo esto?

SUZANNE WOOLF

Esa es una pregunta que estuvimos debatiendo y todavía no tenemos un consenso sobre qué recomendar porque, como dijeron, hay presiones en la dirección de que esto sea lo más rápido posible pero nosotros tampoco queremos dejar de lado riesgos importantes. Estamos pensando en semanas, meses, años. Eso es algo que tenemos que dejar para la comunidad, para que el personal tome la decisión final al respecto.

MARCO HOGEWONING

Gracias. Creo que podemos tomar otra pregunta pero no veo ningún pedido de palabra en la sala. Gracias, Suzanne, por la explicación. Podemos pasar entonces al siguiente tema que va a estar a cargo de los líderes del tema del uso indebido del DNS. Ahora tenemos un documento de cuestiones. Ustedes y los colegas del SSAC pueden quizá compartir algunas recomendaciones técnicas.

RAM MOHAN

Gracias, Marco. Antes de responder su pregunta quiero informar al GAC con respecto a la diapositiva anterior sobre un trabajo que acaba de comenzar y que se vincula con el espacio de nombres. Comenzamos con un grupo de trabajo que se concentra en la integración responsable del DNS en el sistema de nombres. ¿Qué pasa con los identificadores en otros espacios de nombres cuando se quiere interactuar con otros identificadores que están en otros sistemas?

Comenzamos este trabajo para empezar a llegar a algunas conclusiones. Nos preocupa el ciclo de vida del nombre de dominio, la confusión de los usuarios, el fraude. Ese tipo de cosas. La seguridad, la estabilidad, riesgos que podrían introducirse al sistema del DNS cuando tenemos sistemas con otros espacios de nombres que utilizan palabras o nombres que son similares a los nombres de dominio que nosotros tenemos, aunque no son necesariamente iguales. Comenzamos con este trabajo apenas. Los vamos a mantener informados.

Con respecto a la pregunta que usted hacía, Marco, estamos muy complacidos de decir que hay un documento sobre política, un trabajo por lo menos que comenzó para desarrollar política relacionado con el uso indebido del DNS. En años anteriores, lo que hizo el SSAC fue hacer comentarios y brindar asesoramiento después de que se formularan las recomendaciones de política.

Ahora cambiamos este modelo en colaboración con los colegas de la GNSO. Nos han invitado a estar representados en ese proceso de PDP. No estamos participando en los debates sobre si es una vía, dos vías o tres vías de trabajo o todo combinado.

Eso le corresponde a la gente que se ocupa de desarrollo de políticas pero nosotros tratamos de incorporarnos para hablar sobre cuestiones específicas que tienen que ver con el uso indebido presentando nuestras observaciones. Sobre todo porque dedicamos mucho tiempo a ver la evolución del uso indebido y hacia dónde se encamina.

Estamos muy focalizados en esa área. Creemos que es un tema muy importante en las conversaciones que mantenemos con la junta directiva de la ICANN. Sobre todo cuando pensamos en las prioridades para 2026. Respaldamos algunas cosas que viene diciendo la Cámara de Partes Contratadas de la GNSO con respecto al lugar prioritario que tiene que tener el uso indebido del DNS.

Si esto no lo hacemos bien, no solamente se van a ver afectados los usuarios sino también la reputación de este modelo de múltiples partes interesadas que es autorregulado. Nosotros queremos presentarlo como un gran ejemplo. Tenemos que concentrarnos mayormente en el uso indebido del DNS. Estamos involucrados para participar más en la etapa de diseño, más que lo hicimos en años anteriores.

MARCO HOGEWONING Gracias, Ram. Es maravilloso escucharlo. Me pregunto ahora si las personas que se ocupan más del tema de uso indebido del DNS quieren hacer algún comentario o alguna pregunta adicional a los miembros del SSAC. Cualquier otra persona, por supuesto, que pueda tener alguna consulta sobre este tema. Sí, Comisión Europea.

JANOS DRIENYOVSZKI Gracias por estar aquí con nosotros. Gracias por sus presentaciones. Me pregunto lo siguiente. Con los PDP es importante tener el alcance correcto. Se invierte mucho esfuerzo.

Me pregunto cuáles son sus opiniones con respecto al trabajo sobre las registraciones masivas porque entiendo que al final de cuentas queremos tener algo que tenga impacto como resultado del proceso de desarrollo de políticas.

Hablamos de las API pero me pregunto si este enfoque va a cubrir la mayoría de las tecnologías o de las medidas que faciliten las registraciones en grandes volúmenes. Quiero saber si ustedes consideran que este es un buen enfoque o deberíamos definir el alcance de manera que también esté a prueba de lo que ocurra en el futuro. No sé si hay una respuesta, si hay algo técnico que pueda existir, que permita estas registraciones masivas.

RAM MOHAN

Hay distintas salvedades que debemos hacer aquí o distintos matices. Hay motivos legítimos por los cuales se pueden hacer registraciones masivas de una empresa que quiere proteger su nuevo producto y registra cientos de estos productos. También pueden hacerse las registraciones en múltiples TLD. Dentro de un TLD hay algunas cosas específicas en ese sentido.

El acceso por API no es la única manera para manejar las registraciones masivas. Hemos visto muchísimos casos en los que personas con malas intenciones han registrado utilizando un modelo no basado en API donde se puedan ocultar porque todo lo de API se observa.

Habiendo dicho esto, creo que este es un buen ámbito para investigar. Las registraciones masivas tienen que definirse. Una de las inquietudes que compartimos con otros integrantes de la comunidad es que si se establece un umbral, todo lo que está por debajo de un determinado número, no se va a someter a un escrutinio a determinado nivel. Creemos que eso puede lograrse pero hay trabajo para hacer.

Yo confío en que podría haber una política generada para establecer el marco adecuado, para el tipo de conductas que queremos prevenir en lugar de tener métodos específicos a través de los cuales se comete esa actividad o se ejecuta esa conducta. Creo que esa es la distinción que queremos hacer con un proceso de desarrollo de políticas.

MARCO HOGEWONING Gracias, Ram. Veo que no hay pedidos para hacer uso de la palabra. Me da la oportunidad a mí de hacer un comentario. Le agradecemos por sus aportes. Agradecemos todo lo que nos dijo con respecto al PDP. Seguimos fortaleciendo el vínculo entre el GAC y el SSAC. Ahora creo que tenemos que responder esta pregunta. Dónde podemos encontrar oportunidades para colaborar, para ser parte de este PDP. Tanto el SSAC como el GAC. Tal vez no haya un único camino y vamos a pasar a la siguiente diapositiva. India, ¿quiere hacer un comentario sobre uso indebido del DNS o sobre lo que acabo de plantear?

INDIA

Tiene que ver con el uso indebido del DNS. Quería conocer la opinión de Ram con respecto a cuál podría ser la reducción de esta ventana de 15 días para el WHOIS desde el punto de vista del uso indebido del DNS. Creo que esto es uno de los pasos prácticos que podemos llevar adelante.

Hemos avanzado mucho para trabajar en la mitigación del uso indebido del DNS y hoy se presentó esta modificación a través de la validación, la verificación, que podría haber sido un desafío hace 10 años pero que ahora se hace varias veces al día. Uno ingresa a un hotel y hace autenticación en un aeropuerto. Cómo podrían permitir que alguien tenga un nombre de dominio incluso sin la autenticación. Ni siquiera lo están identificando. Es una autenticación. Quisiera que comente cuál es su opinión al respecto. No entiendo por qué la ventana debería ser esa.

MARCO HOGEWONING

Entiendo que tiene que ver con estas dos semanas que se han establecido para la verificación.

RAM MOHAN

Muchas gracias. Dimos nuestra opinión sobre las solicitudes urgentes de información antes. Para ser breves, si realmente es urgente, tiene que significar algo. En nuestra opinión, allí se requiere un tiempo de respuesta muy breve. Es el equivalente de llamar a un servicio de emergencia en la vida real. Cuando uno

llama a un servicio de emergencia, uno no espera obtener una respuesta en 15 días o en 2 días hábiles.

Nuestro enfoque es que eso es importante. Con respecto a la pregunta de la validación y la verificación, desde el SSAC, no sé si necesariamente tenemos un punto de vista compartido en todo el SSAC pero sí sabemos que hay investigadores en cuestiones de seguridad y algunas personas de los organismos de aplicación de la ley que dicen que se ven impedidos por la falta de acceso a alguna información de los registratarios. Por lo menos no tienen una forma fácil de acceder. Venimos promoviendo el desarrollo de sistemas de acceso que puedan divulgar la información a aquellas partes que tienen un interés legítimo en acceder a esa información. Ahí es donde estamos parados.

Con respecto a las solicitudes urgentes sobre todo cuando el GAC y la junta directiva trabajan sobre este tema, tienen que en cuenta la definición del diccionario de urgente y no solamente atenerse a lo que es comercialmente razonable.

INDIA

Pero mi pregunta tiene más que ver con el potencial de mitigación de uso indebido del DNS reduciendo ese periodo de 15 días de la verificación y la validación, y la registración del dominio. Esto es algo que todavía no logro comprender.

RAM MOHAN

Sí. Gracias por aclarar. Una vez más. No sé si puedo hablar en representación del SSAC porque esto es algo que necesitamos analizar profundamente. Tenemos que ver cuál es el daño para los usuarios, medirlos, compararlos contra otros requisitos contractuales y otros procesos de desarrollo de políticas. En esta área tenemos que pensar sobre todo en el daño.

MARCO HOGEWONING

Gracias, India. Gracias, Ram, del SSAC. ¿Hay alguna otra pregunta? Nos quedan dos minutos. Podría empezar a cerrar esta sesión. Sé que es lo que se interpone con el café pero, como dijo Nico, podemos seguir cooperando en el futuro.

NICOLÁS CABALLERO

Tengo una pregunta sobre la cooperación en lo que tiene que ver con el software de código abierto. ¿Eso sería parte de este paquete? En el último IGF en Noruega el gobierno de Noruega básicamente compartió distintas soluciones y hay más de 45 países que en este momento se están beneficiando de esto. Cuál sería la forma en caso de que nosotros tengamos algún colega distinguido del GAC en caso de que haya interés para ver de qué forma cooperar en ese sentido. Cuál sería el procedimiento.

RAM MOHAN

Creo que se pueden poner en contacto conmigo como presidente o con todo el personal excelente del SSAC porque entonces nosotros vamos a promover el diálogo y encontrar la mejor forma

para poder brindar contenido y otro tipo de apoyo a ustedes y también trabajar junto con ustedes. Para quienes están interesados en esta área, este es uno de los pocos informes del SSAC que está con esa idea. Nosotros quisimos hacer este trabajo para ustedes. Es por eso que si ustedes quieren trabajar con nosotros, podemos validar que el hacer este tipo de trabajo para trabajar con ustedes es bueno.

MARCO HOGEWONING Gracias. Muchísimas gracias, Ram, Suzanne, Maarten, Tara. Muchas gracias por estar con nosotros. Espero, como líder del tema, poder seguir con la colaboración en el futuro. No sé si hay algún comentario final, Nico.

NICOLÁS CABALLERO No. Solo temas administrativos. Ahora vamos a ir a una pausa para el café y nos volvemos a reunir a las 4:30. Con esto damos por cerrada la sesión. Gracias, Ram.

[FIN DE LA TRANSCRIPCIÓN]