ICANN77 | Foro sobre políticas – ccNSO: iniciativas legislativas que afectan a los ccTLD
Jueves, 15 de junio de 2023 – 10:45 a 12:15 DCA

CLAUDIA RUÍZ: Hola y bienvenidos a la sesión de la ccNSO sobre iniciativas legislativas que afectan a los ccTLD, yo soy Claudia Ruíz y junto con mis colegas, Bart Boswinkel y Kimberly Carlson, seremos los coordinadores de participación remota de la sesión, tengan en cuenta que esta sesión está siendo grabada y se rige por los estándares de comportamiento esperado de la ICANN. Durante la sesión las preguntas y comentarios presentados en el chat solo se leerán en voz alta si se presentan en el formado adecuado, tal como indiqué en el chat.

Leeré las preguntas y comentarios en voz alta durante el tiempo establecido por el moderador o presidente de esta sesión, la interpretación para esta sesión incluye español, francés y árabe. Hagan clic en el ícono de interpretación en Zoom y elijan el idioma que van a escuchar durante esta sesión, si desean tomar la palabra, por favor, levanten la mano en la sala de Zoom y una vez que el facilitador de la sesión los llame por su nombre, por favor, habiliten su audio y tomen la palabra. Antes de tomar la palabra asegúrense de haber elegido el idioma en el que van a hablar en el menú de interpretación.

Por favor digan su nombre para los registros y el idioma en el que van a hablar, en caso de que no hablen en inglés, al tomar la palabra, por favor, asegúrense de silenciar todos los demás dispositivos y

notificaciones, hablen con claridad y a una velocidad razonable para permitir una interpretación adecuada. Esta sesión incluye transcripción automática en tiempo real, tengan en cuenta que esta transcripción no es oficial ni autorizada, para acceder a la transcripción en tiempo real hagan clic en la tecla de "closed caption" en la barra de herramientas del Zoom.

Para garantizar la transparencia en la participación del modelo de múltiples partes interesadas de la ICANN les pedimos que, por favor, inicien sesión en las sesiones de Zoom utilizando su nombre completo, por ejemplo, nombre y apellido, quizás los saquen de la sesión si no se conectan utilizando su nombre completo. Muchas gracias y habiendo dicho esto, le doy ahora la palabra a Annaliese Williams.

ANNALIESE WILLIAMS: Gracias. Bienvenidos a todos, gracias por participar en esta sesión de ccNSO organizada por el comité de enlace de gobernanza de internet de la ccNSO, yo soy de la administración del dominio .AU, también soy presidente de IGLC. La sesión de hoy será sobre iniciativas legislativas relacionadas con la seguridad cibernética y la forma en que afectan a los ccTLD, tendremos disertantes hoy de Canadá, Vanuatu, Mozambique, Costa Rica y Eslovenia, cada uno de los disertantes hablará acerca de las iniciativas legislativas que afectan a sus ccTLD y explicarán si esto influye sobre el desarrollo o la implementación de la legislación, también hablarán sobre el impacto que estas iniciativas podrían tener.

Cada uno de los disertantes tendrán 15 minutos para su presentación lo cual incluye tiempo para preguntas del público, así que, por favor manténganse y aténganse a ese tiempo para que cada disertante tenga el tiempo asignado, pero si al final de la sesión queda tiempo voy a dejar abierto el espacio para preguntas y comentarios del público. Recuerden que hay interpretación disponible para esta sesión, así que, les pido a todos que hablen despacio y con claridad para que los intérpretes nos puedan seguir.

Quisiera presentar a la primera disertante, Sabrina Wilkinson, que es la gerente del programa de políticas en la autoridad canadiense de la registración de internet, tiene licenciatura en comunicaciones y ha llevado a cabo muchísimos proyectos de investigación en el área de política digital, periodismo y temas generales. Le doy la palabra, Sabrina.

SABRINA WILKINSON: Muchas gracias, es un placer estar hoy aquí con ustedes y quisiera hablar acerca de la participación de CIRA y la relación con la legislación propuesta sobre seguridad cibernética que llamamos ley C-26, que ahora está atravesando el proceso legislativo en Canadá. Me voy a centrar en la segunda parte de este proyecto de ley. Siguiente imagen, por favor.

Hoy quisiera referirme a tres temas claves, en primer lugar, quisiera hablar acerca de qué es lo que se propone en la segunda parte de la ley en la que está también trabajando CIRA, quiero contarles de qué forma

se involucró CIRA en este diálogo relacionado con la ley C-26 hasta el momento en las posiciones de política, también quisiera referirme a la forma en que CIRA piensa y tiene pensado continuar participando de manera continua.

La ley C-26 está formada por dos partes claves, yo me voy a centrar en la segunda parte, dado que esta es la parte en la que está involucrada CIRA. Lo que se propone sería la protección del sistema crítico de seguridad cibernética, la idea es identificar sectores de infraestructura crítica, empresas de telecomunicaciones, bancos, energía y transporte, estos son sectores de infraestructura crítica. Esta forma de gobierno podría establecer requerimientos para operadores designados específicos dentro de estos cuatro sectores regulados, para garantizar que tomen determinadas medidas en torno a la seguridad cibernética, que desarrollen programas de seguridad cibernética, por ejemplo, que presenten informes sobre eventos de ciberseguridad que podrían darse y que mantengan registros específicos relacionados con la seguridad cibernética también.

La ley propuesta también establecería reglamentaciones, le daría al gobierno la facultad de designar operadores en estos cuatro sectores para que tomen determinadas medidas, para abordar un incidente de seguridad cibernética y también establece distintas facultades de aplicación de la ley que tendría el gobierno en aquellos casos en los que no se tomen estas medidas o no se cumplan con estos requerimientos.

¿Por qué es importante la ley C-26 para CIRA? ¿Por qué nos importa esta ley? ¿Por qué nos involucramos en este diálogo continuo sobre políticas? Por varias razones. Por un lado, la parte 2 de esta ley C-26 tiene el potencial de incluir a una amplia gama de operadores, más allá de los que se describen actualmente en la ley, además, los objetivos de la parte 2 están eliminados, es decir, los objetivos de la propuesta de ley que eleva el nivel basal de ciberseguridad en toda la infraestructura de telecomunicaciones es un objetivo que también está alineado con la misión de CIRA para desarrollar un internet de confianza para los canadienses.

También CIRA tiene la oportunidad de participar y mejorar la ley para que la ley no solamente sea pertinente para nosotros como operadores con nuestra misión de generar confianza en internet, sino también nos parece que es un espacio en que podríamos tener un impacto significativo y positivo sobre determinadas cláusulas de la ley y al estar en Ottawa, la capital de Canadá, también geográficamente estamos cerca de lugares donde se toman las decisiones y donde se están desarrollando los hechos en este momento.

Finalmente, también pensamos que participar en el diálogo de políticas entorno a la ley C-26 es una forma de actuar como un referente y también una forma de generar consciencia, es decir, es un espacio en el que CIRA puede contribuir de manera significativa como operador técnico con experiencia y conocimientos en relación con la ciberseguridad y otros temas relacionados incluidos en la ley, también

es una oportunidad para mostrar nuestros productos como proveedor de seguridad cibernética.

Entonces al hacer una revisión de la ley, CIRA se encontró con distintos temas de preocupación, si bien estamos alineados con los objetivos descritos en la parte 2 de la ley C-26, hay algunas áreas en donde vemos que hay algún espacio para mejorar y esta es la base sobre la cual participamos, esta es la exposición de política que nosotros planteamos en las reuniones y conversaciones acerca de la parte 2 de la ley C-26.

En el nivel muy general estas preocupaciones están relacionadas con tres temas claves, tenemos preocupación con respecto a la vigilancia y supervisión, como dije, la ley C-26 le daría al gobierno grandes facultades en particular, le permitiría al gobierno que les pida a operadores designados que tomen determinadas medidas en situaciones de emergencia.

Hay algunas cláusulas relacionadas con la supervisión que ya existen, pero son más limitadas, CIRA también tiene ciertas preocupaciones con respecto a la información compartida considerando una cantidad de información que se va a recopilar en virtud de la ley, en caso de que se convierta en ley, y en la medida en que esa información va a ser compartida entre varias partes.

Finalmente, CIRA también tiene ciertas preocupaciones respecto de la transparencia, sin duda, reconocemos el hecho de que, en cuestiones

de seguridad cibernética, la confidencialidad es necesaria e importante, pero, sin embargo, pensamos que hay espacio para la mayor transparencia que le daría a los canadienses información con respecto a cómo se ha estado utilizando estos requerimientos que se aplican a los operadores canadienses.

A modo de respuesta frente a estas tres preocupaciones, nosotros planteamos tres recomendaciones correspondientes. En un nivel muy general en nuestro trabajo en relación con la ley C-26 y nuestra interacción con las otras partes, solicitamos que se agregue un mecanismo adicional de supervisión a este proceso de emisión de directivas de ciberseguridad, también sugerimos que la información compartida se limite específicamente a algunos propósitos en particular porque hay cierta ambigüedad en torno a la medida en la cual la información recopilada en virtud de la ley puede compartirse.

Finalmente, también apoyamos informes de transparencia anuales que deberían publicarse para que los canadienses y los operadores dedicados tengan más información acerca de la información, las medidas que puede tomar el gobierno y en qué forma se está utilizando esta información.

Entonces tenemos esas tres recomendaciones que están avanzando hacia una serie de modificaciones legislativas propuestas y entre nosotros tenemos ciertas preocupaciones, hemos estado trabajando para ver cómo podemos desarrollar este proyecto de ley, cómo se debería modificar en el proceso legislativo, estamos en este momento

en el proceso legislativo, tenemos que ver quién está participando, en qué medida este proceso ha sido exitoso y en términos generales desarrollamos tres actividades o hay tres áreas en las que participamos por así decirlo.

En primer lugar, tuvimos una serie de reuniones con decisores y otras partes interesadas, entonces nos reunimos con otros actores que participan en este diálogo acerca del C-26 y la forma en que se debería mejorar este proyecto de ley, hablamos con los decisores o quienes apoyan a decisores como el personal, por ejemplo, también nos reunimos con una serie de funcionarios públicos de alto nivel que están involucrados en el desarrollo de este proyecto de ley y que trabajan en el área de seguridad cibernética e infraestructura crítica.

También interactuamos en espacios como este y participamos en paneles públicos, en una conferencia importante de telecomunicaciones que tuvo lugar en Canadá donde compartimos nuestra perspectiva y la perspectiva de CIRA también, interactuamos con otras personas que están involucradas en este debate y que tienen conocimientos y experiencia en este campo.

Hicimos algunas publicaciones entorno a nuestras perspectivas con respecto a la política y con respecto a lo que nosotros pensamos que debería agregarse a este proyecto de ley. Entonces, ¿cómo tenemos pensado continuar trabajando a medida que este proyecto de ley avance en el proceso legislativo? En este momento el proyecto de ley está en lo que se llama la etapa de comité, es decir, está esperando a

que la revise un grupo de miembros del parlamento que estudian temas relacionados con seguridad pública y seguridad cibernética, vamos a seguir de cerca el avance de este proyecto de ley a medida que atraviesa esta etapa de comité, es revisada y analizada por los parlamentarios, así como otros testigos expertos.

Continuaremos reuniéndonos con decisores y partes interesadas, vamos a compartir las perspectivas de CIRA, vamos a tratar de entender un poco más qué piensan las otras partes, qué es lo que los impulsa, qué motivaciones tienen, cuál es la información que tienen y también vamos a continuar apoyando públicamente la posición de CIRA en particular con respecto a la parte 2 del C-26 en foros públicos como congresos internacionales, espacios internacionales como este y también dentro del país.

Espero haberles dado una idea general de cómo es este proyecto de ley, espero que entiendan de qué manera participa CIRA hoy en este tema y también espero haber podido explicarles cómo pensamos seguir trabajando en el futuro. Con todo gusto voy a responder cualquier pregunta que puedan tener.

ANNALIESE WILLIAMS: Muchas gracias, Sabrina. ¿Alguien tiene alguna pregunta para Sabrina?

SEAN COPELAND: Por supuesto, tengo una pregunta para usted. Yo soy de NICVI, pero quisiera saber, ¿cómo ha sido recibir su posición con respecto a esta supervisión o vigilancia?

SABRINA WILKINSON: Muchas gracias, Sean, yo diría que todas las recomendaciones fueron recibidas de forma positiva por parte de los decisores, con respecto al mecanismo de supervisión, en particular tratamos de alcanzar ese equilibrio entre tener un nivel de supervisión adicional y mantener al mismo tiempo la velocidad y la naturaleza secreta de estas cuestiones porque entendemos que en cuestiones de seguridad pública esto es fundamental, esperamos haber alcanzado ese equilibrio adecuado y la retroalimentación positiva que recibimos muestra que es así, que este es el caso.

ANNALIESE WILLIAMS: Gracias, Sabrina. ¿Alguna otra pregunta? Creo que no hay más preguntas, así que, pasamos al siguiente orador que es Norman Warputt, es administrador de ICT y de la organización de telecomunicaciones, radios de difusión y comunicaciones electrónicas. Adelante.

NORMAN WARPUTT: Yo soy el administrador de ICT para el ente regulador de las telecomunicaciones de Vanuatu y también soy delegado para el ccTLD .VU. Mi presentación hoy va a ser sobre ciertas iniciativas en las que

estamos trabajando junto con el gobierno, también tienen que ver con el ccTLD, .VU, del que ahora soy administrador.

Entonces vamos a hablar, en primer lugar, del ente regulador de telecomunicaciones y radio difusión, es un órgano que opera indirectamente del gobierno, pero no tenemos ninguna comisión, actuamos como ente regulador. Entonces tenemos el ente regulador y el personal, nosotros tenemos que regular el sector de telecomunicaciones, así como el de radio difusión, dependemos directamente del primer ministro y brindamos asesoramiento sobre todo lo que tiene que ver con políticas en el ámbito nacional vinculados con las ICT.

.VU es nuestro espacio de dominio de alto nivel con código de país y lo administra esta oficina que yo mencioné, anteriormente era la compañía de telecomunicaciones la que estaba a cargo de este ccTLD, estamos hablando de la década del 90' y cuando se estableció el regulador, la ley que creó el regulador estableció que este ente iba a ser el administrador, entonces tuvimos una transición de la compañía de telecomunicaciones que empezó en el 2017 y que finalizó exitosamente en enero del 2020.

Desde la perspectiva de la seguridad del internet, nosotros cuando pensamos en la transición el ente regulador se aproximaba GoDaddy para que fuera el operador del registro del ccTLD .VU, entonces el operador de registro es el que brinda el servicio que cumple obviamente con las mejores prácticas internacionales y con la ICANN.

Las políticas de .VU como ccTLD se realizaron, desarrollamos reglamentación al respecto en el 2016, en la actualidad tenemos 34 registradores internacionales y cinco son locales, ellos cumplen con los estándares de seguridad internacionales que exige el operador de registro. Obviamente el ente regulador es el que apoya y asiste al gobierno, el que hace la redacción de algunas leyes porque tenemos reglamentación de protección al consumidor que nos permite de esta manera informar a los consumidores de los riesgo de la seguridad de internet y también lo que es la protección a las infancias en línea.

En 2021 hubo una ley que se publicó y que se debatió en el parlamento, una de las iniciativas con la que trabajamos con el gobierno junto con la dirección de información del gobierno es establecer un CERT, que es un equipo de respuestas de emergencias informáticas, esta oficina empezó a funcionar en 2018 y sigue operando en la actualidad. Otra de las iniciativas fue establecer un foro de gobernanza de internet de Vanuatu y nosotros, de hecho, en el 2018 tuvimos una reunión de IGF, esta es una plataforma para poder hablar de todo lo que tiene que ver con las políticas públicas, tiene el respaldo del ente regulador y también de la dirección de información del gobierno.

También desarrollamos una reglamentación para el registro de la SIM, esto tiene que ver con una instrucción recibida de la oficina de gestión anti desastre del gobierno nacional, se estableció una reglamentación de emergencia para que todas las tarjetas SIM queden registradas y se

les dio una identificación nacional valida, esto concluyó, ya está operativo en el mercado y particularmente las compañías de telefonía móvil utilizan esta registración de tarjetas SIM.

Esto nos sirve también para agregar valor a todas las iniciativas que existen en el país sobre seguridad cibernética, también hay otra iniciativa en la que ayudamos al gobierno junto con la dirección de información nacional, en este momento la idea es ir al parlamento con varios proyectos de ley, como pueden ver en pantalla esta legislación nacional, tenemos lo que es la comunicación digital perjudicial, la protección de datos y privacidad, y la protección de la infancia en línea, entonces estos son los proyectos del leyes, también queremos otras iniciativas sobre ciberseguridad.

Tratamos de generar sensibilidad en la comunidad sobre lo que tiene que ver con protección al consumidor, la registración de la SIM para hablar sobre cuáles son los límites, los riesgos de utilizar el internet y cómo esta legislación pues impactar a los habitantes del país, es parte entonces de nuestro programa de generación de consciencia que es anual, participamos también con la comunidad escolar, con lo que tiene que ver con el foro nacional de IGF y otras organizaciones dentro del país que se dedican a estos temas. Esto es todo lo que tenía para mostrar. Muchísimas gracias.

ANNALIESE WILLIAMS: Gracias, Norman. ¿Alguna pregunta para Norman? Bueno yo voy a hacer una, Norman, porque sé que como ente regulador no son

responsables, pero en Vanuatu tuvieron un ciberataque muy grande hace poco, ¿pudieron ofrecer alguna reflexión sobre eso o qué fue lo que hicieron desde su oficina?

NORMAN WARPUTT: Gracias por lo pregunta. No tengo información detallada sobre el ransomware que sucedió el año pasado, creo que los hackers eran unos de los servicios que teníamos como familiar, entonces creo que hubo que cerrar el servidor, pero desde .VU y desde nuestra perspectiva, nosotros no sufrimos un gran impacto, pero el gobierno sí tuvo que desconectar varios de los servidores en línea para garantizar que podían volver y restaurar los datos del backup que tenían.

Entonces creo que el impacto más grande fue el proceso de pago, el control de los portales, los sitios web, correo electrónico, todos estos servicios tuvieron que ser cerrados por el gobierno debido a este ataque. Gracias.

ANNALIESE WILLIAMS: Gracias, Norman. ¿Alguna otra pregunta? Veo a Angela.

ANGELA: Buenos días a todos. Yo quería preguntar sobre si existe alguna reglamentación específica que tenga que ver con los derechos radiales porque está así en las políticas que tienen que ver con radio difusión, pero ¿ustedes lo tratan de manera diferente porque ahora tienen una radio que corre sobre un nombre de dominio? Es decir, las políticas de

ccTLD que hablan del uso, también hablan del contenido de radio cuando corre en una plataforma con nombre de dominio, ¿verdad?

NORMAN WARPUTT: Gracias por la pregunta. Nosotros no regulamos contenido, nosotros lo único que regulamos es el servicio de telecomunicaciones cuando sale al mercado, pero la verdad no regulamos ningún tipo de contenido de ningún sitio web o cualquier cosa que se haga a través de radio difusión. Espero haber respondido la pregunta.

ANNALIESE WILLIAMS: Gracias, Norman. ¿Hay alguna otra pregunta? No veo nada, entonces vamos a pasar ahora a nuestro siguiente orador que va a participar de manera remota, tenemos a Lourino Chemane, él es parte del instituto de ICT nacional de Mozambique, fue asesor del Ministerio de Educación Superior y Tecnología de la Información. Le doy la palabra, adelante, Lourino.

LOURINO CHEMANE: Hola, gracias por darme esta oportunidad. Soy de Mozambique y voy a compartir lo que estamos haciendo en Mozambique en el campo de seguridad cibernética y las iniciativas relacionadas con los ccTLD. Nosotros representamos al Instituto Nacional de Información y Tecnologías de la Información en Mozambique, estos son los temas que voy a cubrir, una breve introducción, el mandato y las competencias del INTIC, manejo de ccTLD en Mozambique, legislación aprobada, la política y estrategia de ciberseguridad nacional, acciones

de seguimientos, desarrollo de un marco legal y una breves conclusiones.

INTIC fue creado en 2011, luego hubo decreto que lo revisó en 2020 y ese regulador de ICT en Mozambique tiene su propia autonomía administrativa, su propia personalidad jurídica, es supervisado por el ministerio que supervisa el área de información y tecnologías de las comunicaciones, actualmente trabaja con el gobierno el Ministerio de Ciencia y Tecnología.

Como parte del mandato de INTIC tenemos diversas actividades, por ejemplo, regular, supervisar y vigilar el sector de tecnología de la información y las comunicaciones en Mozambique, desarrolla propuestas para políticas, normas y reglamentaciones que garantizan la seguridad e integridad de los sistemas de tecnología de la información y operaciones contra posibles usos indebidos. Una de las áreas de nuestros mandatos específicamente es garantizar la implementación y gestión del domino .MZ, también trabajamos en otras áreas como la certificación digital de Mozambique, trabajamos con los operadores digitales y los proveedores de servicios intermediarios.

Dentro del alcance de los ccTLD en particular .MZ quisiera compartir un poco de información histórica, .MZ se estableció en 2015 y fue operado por la Universidad Eduardo Mondlane que es una institución académica, pero con la aprobación de la ley de transacciones electrónicas en 2017 se estableció como la entidad responsable de la

gestión de los TLD de Mozambique y ahora estamos trabajando con la universidad para transferir una parte de su fusión y su responsabilidad a INTIC, pero dejamos toda la parte de operaciones técnicas en el área de la universidad y todo lo que tiene que ver también con el .MZ.

Hay muchas competencias incluidas en la ley, pero una de ellas consistía en dar instrucciones claras para el desarrollo de las reglamentaciones para el uso del dominio .MZ, hicimos ese trabajo, esta reglamentación fue aprobada en 2020 y como indiqué llevamos a cabo el procedimiento para la gestión de .MZ, trabajamos con los ministerios responsables de esta área y hay claras indicaciones de que los estados miembros deben trabajar para implementar DNSSEC en todos los países y nosotros en Mozambique también lo estamos haciendo.

Seguimos los desarrollos legislativos internacionales, nos adherimos al Convenio de la Unión Africana sobre seguridad cibernética y protección de datos, Mozambique es uno de los países firmantes de este convenio y también seguimos de cerca el trabajo de Naciones Unidas en preparación para la propuesta de la convención de Naciones Unidas contra el uso de tecnologías ICT con fines delictivos y también trabajamos para adherirnos al Convenio de Budapest.

Con respecto a las secciones específicas en materia de seguridad cibernética el gobierno de Mozambique aprobó la política y estrategia de ciberseguridad en 2021 e identificó los mecanismos de coordinación y la gobernanza de la ciberseguridad, la estructura que

comparto acá podrá ver… En el comité encabezado por el ministro que está a cargo de las ICT e INTIC desempeña la función técnica y los miembros de este comité incluye a las agencias de aplicación de la ley, el departamento del Ministerio de Justicia, los reguladores de telecomunicaciones, los reguladores de ICT, el sector académico, la Sociedad Civil y el sector privado.

Entonces seguimos el abordaje de múltiples partes interesadas al establecer esta comisión para supervisar el proceso de implementación de leyes de seguridad cibernética en el país. La estrategia de ciberseguridad nacional identifica 25 iniciativas divididas en siete áreas, aquí el rojo muestra aquellas áreas relacionadas con el tema que estamos tratando hoy, el desarrollo de pautas, instrumentos regulatorios y jurídicos para la protección de infraestructura crítica, reforzar el marco jurídico sobre seguridad cibernética y establecer el centro para análisis e investigación en tráfico de internet, también una red de sistema nacional así como mapean la infraestructura crítica, consideramos que estas actividades en cierta forma están relacionadas con la seguridad cibernética debido al papel que desempeñan las infraestructuras críticas.

Con respecto al desarrollo quisiera compartir el trabajo en curso a modo de preparación para la sanción de leyes, estamos trabajando en la ley de seguridad cibernética, la ley de protección de datos y también la ley de delitos cibernéticos, estamos trabajando sobre la regulación de registración de proveedores de servicios electrónicos intermediarios y también operadores de plataformas digitales. En los

próximos años también trabajaremos y vincularemos esto con la seguridad cibernética.

En términos del desarrollo del marco jurídico nosotros consideramos que podemos desempeñar un papel importante porque somos el organismo que está a cargo de preparar las propuestas legislativas que se presentan al gobierno y que luego sigue el proceso legislativo para poder influir sobre estos instrumentos relacionados con los ccTLD.

Podemos proponer cambios en los instrumentos normativos, los administradores y ccTLD son responsables de gestionar el dominio .MZ y de brindar los servicios e infraestructura crítica y necesaria para llevar a cabo el trabajo, también brindar servicios a los registradores, esto podría incluir o crear nombres de dominios y actualizar los servicios de nombres.

También consideramos que en esta área podemos desempeñar un papel muy importante en cuanto a alinear los instrumentos normativos de ciberseguridad con el trabajo técnico de implementación de los mecanismos de seguridad cibernética relacionados con los ccTLD. Esta es la última imagen. La revisión de las políticas de registración de nuevos dominios para los ccTLD de Mozambique incluidos algunos aspectos de seguridad, implementación de la infraestructura de seguridad de ccTLD haciendo hincapié en DNSSEC, cumplir con las recomendaciones de los intermediarios que brindan proveedores de servicios, así como la

nueva legislación de seguridad cibernética y la reglamentación para la registración de proveedores de servicios intermediarios.

También estamos trabajando para cumplir y adherirnos al Convenio de Budapest en cuanto finalice este proceso de adhesión, vamos a cumplir con las políticas de la ICANN para ccTLD, para otros TLD y otros aspectos relacionados con la gestión de internet. Gracias por su atención y les pido disculpas al equipo técnico y a los intérpretes por haber hablado un poco rápido.

ANNALIESE WILLIAMS: Gracias, Lourino. ¿Alguien tiene alguna pregunta para Lourino?

ANIL JAIN: Muchas gracias. INTIC actúa como regulador y también como administrador de ccTLD, ¿no le parece que esas funciones están en conflicto entre sí?

LOURINO CHEMANE: Gracias por su pregunta, de hecho, no solamente somos regulador de ICT, también trabajamos como autoridad de seguridad cibernética y tenemos la responsabilidad de los ccTLD, en general, tenemos la función de supervisar el desarrollo de internet en el país, entonces el papel regulador de servicios digitales es solo una de nuestras funciones, pero no es la única.

Usted pregunta si no hay intereses de conflicto entre estas funciones, hay mecanismos de gobernanza establecidos con la participación de todas las partes interesadas en el país y esto nos ayuda a supervisar las actividades que lleva a cabo INTIC, somos un país en desarrollo con una considerable limitación de recursos y no estamos en condiciones de tener varios organismos para cada una de estas áreas relacionadas con el desarrollo de las tecnologías digitales, por el momento tenemos dos organismos de regulación, uno para las telecomunicaciones y, por otra parte, INTIC que es el regulador de tecnologías de la información y la comunicación incluye las funciones que acabo de mencionar. Espero haber respondido su pregunta.

ANIL JAIN: Gracias.

ANNALIESE WILLIAMS: Gracias. ¿Alguna otra pregunta? No veo ninguna pregunta por parte de alguien que esté en la sala, veamos si hay una pregunta en Zoom, tampoco hay preguntas, así que, pasamos al siguiente orador.

Nuestra siguiente oradora es Rosalía Morales, directora ejecutiva de NIC Costa Rica, Rosalía trabajo en .CR desde 2012, ha liderado proyectos relacionados con la gobernanza de internet, ciberseguridad, infraestructura de internet y políticas de internet, anteriormente era miembro de la Junta Directiva de LACNIC, trabajó en grupos de trabajo de la ccNSO en la ICANN, LACTLD e IGF local de Costa Rica. Rosalía, tiene la palabra.

ROSALÍA MORALES: Hola a todos, voy a decirles, en términos generales, lo que tiene que ver con la ciberseguridad y cómo esta legislación sobre seguridad cibernética ha afectado al ccTLD, en primer lugar, voy a dar un contenido general de qué significa la seguridad cibernética en nuestro ccTLD y hablar en términos generales de la legislación con la que contamos. Para .CR ciberseguridad es un tema de mucho interés, hemos estado trabajando en este tema en los últimos 12 años y somos parte de la Junta Directiva del ccTLD, hemos trabajado con otras organizaciones, como pueden ser las que reúne CSIRT.

Nos hemos también relacionado con otros proyectos de cooperación internacional para que nos ayuden también dentro de nuestra organización, nosotros le hemos dado al primer equipo al gobierno, entonces empezamos con las capacidades técnicas y las capacitaciones para que pudieran hacer en el ámbito local iniciativas sobre seguridad cibernética. También hemos hecho campañas de capacitación y sensibilización en escuelas.

Nuestras políticas, como muchos mencionaron anteriormente en las presentaciones previas, nosotros no tenemos nada que ver con el contenido y cualquier cambio que podamos hacer para un dominio vamos a necesitar una orden de algún tribunal, todo lo que tenga que ver con cuestiones de seguridad cibernética tanto a nivel local como internacional. Nosotros nos hemos adherido a la convención de Budapest en el 2017, en este momento hay una cierta demora en lo

que es la legislación complementaria, que nosotros tenemos que sancionar para que esta convención realmente pueda funcionar y exista una respuesta rápida de nuestros organismos nacionales.

Uno es funcionar como agente encubierto, que es una ley que tiene que ser sancionada y promulgada, en este momento estamos hablando de ese tema, se está discutiendo en Costa Rica. Y la segunda tiene que ver con evidencia digital porque hay un protocolo sobre cómo tienen que tratar las autoridades estos datos que tienen que ver con la convención de Budapest. Hay un sello oficial para que puedan brindarse los datos para la velocidad que lo necesitan las autoridades internacionales.

Hemos aceptado el segundo protocolo adicional de la convención de Budapest en el 2022, todavía no fue ratificado por el congreso, yo entiendo que todavía hay algunos países que tienen que ver si esta enmienda puede ser sancionada por los gobiernos nacionales y hay mucha discusión para ver cuál es el impacto que esta enmienda va a tener en el WHOIS. Todavía estamos esperando que el congreso lo apruebe y obviamente creo que nuestras contrapartes europeas van a hacer un gran trabajo al respecto y eso nos va a ayudar.

Después tenemos también la legislación sobre ciberdelitos que afecta directamente los temas que tienen que ver con ciberseguridad, esta ley se sancionó en 2013 y nos ha ayudado para poner en marcha nuestras operaciones y nuestras políticas, nos ayudó porque nos dio una vía para que los clientes locales supieran cómo proceder en caso de que

hubiera algún problema, antes era un área bastante gris, no se sabía bien qué hacer, pero ahora ha quedado más claro cuál es el camino que hay que seguir, cómo llegar a las autoridades locales para hacer algo si existe algún delito de ciberseguridad de sus dominios.

Y, finalmente, está el tratado de Naciones Unidas sobre ciberdelitos. Costa Rica es bastante neutral al respecto, hasta el momento hemos actuado como espectadores para ver qué es lo que surge de esas deliberaciones. Existen otras iniciativas que han afectado el espacio de ciberseguridad en el ámbito local y cómo nosotros operamos un ccTLD que no necesariamente es una ley sancionada por el congreso, pero que sí afecta las operaciones.

Como yo mencioné, tenemos el equipo nacional de respuesta ante incidentes, o CSIRT, en la actualidad en el último semestre ha crecido el interés para fortalecer este equipo, el equipamiento que tiene la capacitación, el personal y también una capacitación local de los entes nacionales y otras organizaciones como .CR, que son los que generan la estabilidad de internet en Costa Rica.

El gobierno de Estados Unidos también nos ha financiado para fortalecer la ciberseguridad, somos parte de una organización que está ayudando al gobierno para realizar capacitación en ciberseguridad, todavía no se dio inicio a estos cursos de capacitación, pero bueno, pedimos ser parte y vamos a ver qué es lo que sucede porque es un plan quinquenal de capacitaciones. Entonces el interés en la ciberseguridad o el foco de la ciberseguridad que tiene en el gobierno,

incluso también la función que nosotros cumplimos dentro del gobierno y depende del gobierno que esté en ese momento.

No es algo estable, hay algunos gobiernos que participan mucho y otros no tanto, en este caso, están bastante involucrados, el año pasado Costa Rica sufrió un incidente, un hackeo, muy importante en el tesoro y en el sistema de salud, durante más de seis meses estuvo hackeado y generó una crisis nacional. A partir de ese momento empezamos a recibir ayuda del exterior y es un punto muy importante para el gobierno actuar, y obviamente para nuestra organización.

También hay una estrategia de ciberseguridad que fue creada y finalizó el año pasado en 2022, es una estrategia creada por el Ministerio de Ciencia, Tecnología y Telecomunicaciones junto con la Organización de Estados Americanos, OEA, y esta estrategia no tiene un impacto sobre nuestras políticas o nuestro trabajo diario, pero fuimos parte de las deliberaciones, hicimos nuestros comentarios. Es una estrategia bastante amplia y es un esfuerzo también que hizo la OEA en distintos países de la región, es por eso que es muy similar a otras estrategias que tienen otros países miembros de la OEA.

No se aplica necesariamente y en forma directa a la realidad del país exactamente, sino que es más amplia para ver… No afecta directamente en la manera en la que operamos, como dije anteriormente. Hay una ley que se está probando para crear un organismo de ciberseguridad, puede haber sí un impacto en el ccTLD en nuestra operación porque tiene que ver con cómo se procesan los

datos, todavía no fue aprobada por el congreso, todavía obviamente se está discutiendo en el congreso y la ley puede cambiar porque ustedes saben que cuando están estas deliberaciones se pueden hacer agregados, modificaciones, uno tiene que estar atento y ver qué es lo que está sucediendo para garantizar que no afecten nuestras operaciones de manera negativa.

Y si de alguna manera nosotros podemos mejorar este proyecto de ley obviamente estamos siempre abiertos a brindar nuestros comentarios al respecto, yo creo que la ley se une con esta nueva intención del gobierno de probar y tener legislación de ciberseguridad en Costa Rica, a esto realmente se está poniendo presión para que se apruebe rápido, pero bueno, todavía no terminaron las deliberaciones. Entonces, en términos generales, es que, nosotros hemos tenido unos 12 años trabajando en conjunto con las organizaciones de ciberseguridad del país, realmente tenemos una relación bastante estrecha con los organismos encargados de aplicación de la ley.

Y cuando hablamos de una ley o distintas políticas, o proyectos, todo dentro del espacio de ciberseguridad que puede afectar a los ccTLD nosotros tenemos una comunicación intensa con los entes involucrados que nos ha permitido saber qué es lo que está pasando y también garantizar que ayude a ambas partes o a todas las partes implicadas. La ciberseguridad es un área clave de interés para el gobierno y para el ccTLD, en términos generales, esto conlleva algunos riesgos, como dije, porque hay veces que se están debatiendo y no sabemos exactamente cómo van a ser sancionadas, pero bueno,

vamos a seguir de cerca todo ese proceso para garantizar que realmente sea bueno para el ciberespacio y no que genere algún tipo de riesgo o peligro para los usuarios o para el ccTLD.

En términos generales, hay mucho trabajo por hacer porque Costa Rica está empezando a trabajar con la legislación sobre ciberseguridad y tenemos que aprender mucho de lo que han hecho otros ccTLD, por ejemplo, ya vi en este panel cómo manejar o cómo gestionar esta administración, esta generación de nuevas leyes, de nueva legislación, o cómo mejorar nuestro espacio de legislación de ciberseguridad para que los ccTLD salgan fortalecidos después de la sanción de la ley.

Y también tenemos la oportunidad de trabajar con las autoridades de Costa Rica y del exterior porque también tenemos la posibilidad de capacitar a nuestro personal en la última tecnología de combate al ciberdelito y también tenemos localmente otros capacitadores que pueden transferir el conocimiento para que internet continúe siendo estable y segura en Costa Rica. Gracias.

ANNALIESE WILLIAMS: Muchísimas gracias, Rosalía. ¿Alguna pregunta para Rosalía? Olga, adelante.

OLGA CAVALLI: Gracias, Annaliese, gracias a todos los presentadores porque realmente fue muy buena la presentación. Rosalía, dijeron que esta ley era bastante nueva, en la que estaban pensando en Costa Rica, y sobre

este ente, ese organismo, en el que están pensando, ¿tienen idea cómo esto encajaría dentro de la estructura burocrática del gobierno? Si va a depender directamente de la presidencia, ¿cómo va a interactuar con otros ministerios de seguridad? Quizás no, no tiene la información, pero bueno, si la tiene me gustaría conocerla.

ROSALÍA MORALES: Gracias, Olga. Sí, esta ley la impulsa el Ministerio de Tecnología, Ciencia y Telecomunicaciones, parte de la ley le da al ministerio la autoridad que tiene el Ministerio de Justicia que tienen los tribunales, por ejemplo, yo creo que le da al ministerio la posibilidad de hablar con la Interpol e intercambiar información que no tiene en este momento el ministerio, el personal o la experiencia. Entonces eso es parte de lo que se está debatiendo, es por eso que confunde un poquito los roles que deben tener cada ministerio y ese ha sido uno de los problemas por los que no avanza el proyecto de ley, pero esto tiene que ver con el Ministerio de Ciencia, Tecnología y Telecomunicaciones.

ANNALIESE WILLIAMS: Gracias. ¿Alguna otra pregunta? No veo a nadie más ni en la sala ni en Zoom. Bueno, yo creo que tenían una pregunta para Rosalía, pero quizás tendrían que hacérsela todos los miembros del panel, en general, para hablar de lo difícil que es ver cómo son las distintas iniciativas de legislación que están emergiendo y le voy a pedir entonces a todos los oradores que nos ayuden a entender cómo sus registros funcionan con esto, pero ahora vamos a nuestro último orador.

Nuestro último orador es Bárbara Povse, ella está a cargo del ccTLD de Eslovenia y presidente también de su Junta Directiva, tiene 20 años de experiencia en lo que es administración de negocios en la política de la Unión Europea y tiene mucha experiencia en los nombres de dominios respecto de privacidad y protección de datos.

BÁRBARA POVSE: Gracias, Annaliese. Buenos días a todos, gracias por esta amable presentación, sí, como podrán ver, tengo mucha experiencia, incluso recuerdo cuando todos los CC estaban fuera del radar de los legisladores, no se puede creer que directamente no había regulación y estos tiempos, sin duda, quedaron atrás. Está bien, probablemente, que yo sea la última oradora, el chiste es que el mejor producto de exportación de la Unión Europea es la legislación, así que, no sé si debo disculparme o simplemente aceptarlo.

En primer lugar, quisiera agradecer a Martha Moreira, que me ayudó a preparar esta presentación, yo voy a hablar acerca de cómo .SI y, también en parte, .PT se ocupan o enfrentan todas estas legislaciones, especialmente en el campo de la seguridad cibernética, pero también en otras áreas. Así que, gracias también, Polina, de CENTR porque yo no soy abogada, ella verificó que todos los hechos sean correctos y todos los errores que puedo llegar a cometer esos son míos, y yo me hago cargo.

Probablemente ustedes estén familiarizados con el hecho de que los países de Europa no solamente cumplen con su legislación nacional, sino que también, como todos formamos parte del mismo marco jurídico europeo, tenemos otras fuentes legales de la Unión Europea… Y si pasamos a la siguiente imagen, porque no voy a entrar en gran nivel de detalle ni voy a explicar quién hace qué en la Unión Europea y quién es responsable de qué legislación y cómo se toman las decisiones para finalmente producir directivas o reglamentaciones.

Pero podrán ver con todos estos círculos y flechas que el sistema es bastante complejo y debo admitir que yo sigo sin sentirme totalmente segura con respecto a todos los procesos en curso, por suerte no necesito conocerlos a todos, este es un trabajo muy bueno que nos entrega CENTR, especialmente el área de políticos de un pequeño equipo que trabaja dentro de CENTR, porque creo que desde la perspectiva de un registro tan chico como el nuestro nosotros nunca podríamos no solo seguir lo que está ocurriendo, sino influir. Esto quedaría fuera de la cuestión.

La siguiente imagen. Entonces esta es una lista de leyes de seguridad cibernética de la Unión Europea que son pertinentes para los CC y que ya existen. La primera directiva NIS, bueno, este fue un pequeño paso dentro de toda una serie de legislaciones relacionadas con la ciberseguridad, que luego tuvo lugar y que influyó sobre la registración de ccTLD. En ese tiempo nosotros calificábamos como proveedores de servicios esenciales; que no es lo mismo que servicios críticos,

recibimos muchas nuevas responsabilidades y ahora también tenemos el NIS2 con requerimientos adicionales.

Y en este momento estamos en la fase en la que NIS2 se transpone, traslada a las legislaciones nacionales, había distintas legislaciones en los distintos países, entonces ahora los legisladores están tratando de coordinar este trabajo, por solo mencionar, ¿cuál sería el impacto sobre nuestra área? Bueno, nosotros hablamos principalmente del artículo 21, verificación de registratarios, hay muchas cosas que no están claras allí todavía. Y luego tenemos también obligaciones en materia de informes, etc., etc.

También hay algunas pautas propuestas por NIS, acá hablamos de las medidas de seguridad para los operadores de TLD, pero también hay una sobre verificación de registratarios, estas no son normas vinculantes, sino recomendaciones. Aquí, bueno, esto todavía no se terminó, hay cierta legislación que se está desarrollando en el área de la seguridad cibernética, pero que todavía no está finalizada. Todos los días hay cambios, como dije, recibimos informes, por suerte muy completos, del personal de CENTR que incluyen los aspectos relevantes para los ccTLD y esto es extremadamente importante para nosotros.

Entonces, ¿cómo nos enfrentamos a todas estas iniciativas? Tratamos con CENTR, con la coordinación, con el grupo de trabajo sobre aspectos legales y regulatorios, tratamos de recibir información acerca de los hechos que se desarrollan y luego tratamos de influir sobre la

legislación recién cuando llega al nivel de preparación para la Unión Europea, es decir, cuando ya hay una versión preliminar tratamos de influir en aquellos campos que nos concierne y lo hacemos con algunos documentos de CENTR; que encontrarán en el sitio web de CENTR, y también participamos en varias reuniones a nivel de la Unión Europea con legisladores para tratar de generar un impacto en todas las fases del proceso.

Luego nosotros, los miembros individuales, tratamos de informar a nuestros organismos nacionales para que se puedan preparar para la nueva legislación y para que sepan cuáles son nuestras recomendaciones sugeridas con respecto a algunos cambios a realizar. Acá se menciona también los centros de análisis e información compartida de CENTR para los TLD y esto es muy importante en términos de seguridad cibernética, y hay mucho trabajo de concientización, participación y capacitación a nivel de la Unión Europea.

En esta imagen me refiero a lo que ocurre a nivel nacional, el principal mensaje es que, los ccTLD deberían ser proactivos en la medida de lo posible si es que queremos influir sobre el proceso. Tal como ya dije, nosotros tratamos de influir sobre el proceso a nivel de la Unión Europea mediante nuestros representantes nacionales y luego, llega la adopción y la sanción de legislación nacional tratamos de hablar e interactuar con los ministerios y con las legisladores, y tratamos de informarlos porque es importante que entiendan los aspectos básicos,

cuáles son las medidas y qué significan determinadas medidas a nivel del DNS.

Creo que a lo largo de los años Eslovenia es un país muy lindo, muy pequeño, nos conocemos todos, somos 2.000.000 nada más, entonces es fácil tomar las medidas y saber con quién hay que comunicarse, pero también ayuda el hecho de que nosotros como operador técnico, que trabaja de forma muy activa del lado de políticas, tratamos de reunir a los especialistas técnicos y no técnicos a nivel nacional para que hablen el mismo idioma.

La siguiente imagen, por favor. Aquí podría mencionar cuáles son los canales que utilizamos, todo tipo de canales, participamos en debates públicos, utilizamos contactos en ministerios públicos, escribimos artículos, escribimos en blogs, enviamos mensajes por correo electrónico, llamaos a la gente por teléfono cuando estamos en un proceso de consulta pública e incluso antes tratamos de hablar para influir en ese momento.

A veces tenemos bastante éxito, a veces no tanto. La implementación de CPC, que es la regulación de transfronteriza de protección al consumidor, en este caso, tuvimos muy buenos resultados, nos comunicamos muy bien con el ministerio responsable de la implementación y logramos resultados muy razonables.

No estamos teniendo resultados tan buenos con la implementación de NIS, el organismo regulador nacional está trabajando por su cuenta y

no quiere comunicarse con nadie en este momento, pero esperemos que esto cambie pronto porque creo que es sumamente importante que hablemos entre nosotros, porque como CC a nosotros nos interesa mucho proteger internet tanto como nuestro gobierno, simplemente tenemos que asegurarnos de que las reglamentaciones o la legislación que se promulgue sea aplicable, que podamos hacer lo que se nos pide y que lo que se nos pide sean las medidas adecuadas.

A veces no se entiende este tema lo suficiente. ¿Cuál es el impacto de todo esto sobre nuestro trabajo? Tratamos de mirar hacia adelante, no esperamos… Gracias. No esperamos hasta que se promulga una ley, tratamos de prepararnos con anticipación y cada vez somos mejores en cuanto a trabajar con la bola de cristal.

Seguimos el proceso desde el principio con gran ayuda de CENTR y como CENTR es una muy buena comunidad también aprendemos mucho unos de otros, nos ayudamos mutuamente y compartimos recursos, y especialmente para un registro pequeño como el nuestro esto reviste gran importancia. Nosotros, incluso antes de NIS, decidimos obtener la certificación ISO 27001 y resultó ser una muy buena decisión porque no tenemos tanto trabajo por hacer todavía con NIS1, pero sí tenemos que hacer bastante trabajo en cuanto a procedimientos de verificación de registros, estamos trabajando en eso, el cumplimiento legal es un tema clave en Europa en todos los campos, pero esto es algo difícil de lograr y estamos trabajando en eso.

¿A qué me refiero con el efecto Bruselas? Bruselas es el líder en legislación de seguridad cibernética, creo que es importante que tengamos legislación, pero que no trabajemos de manera aislada. Los nuevos requerimientos entonces hacen mucho hincapié… Perdón. Recibimos muchas nuevas obligaciones que implican un gran costo para los registros, tenemos que cambiar nuestros procedimientos, tenemos que contratar personal nuevo que pueda ocuparse de estos nuevos procedimientos, tenemos que invertir mucho en nuestra infraestructura.

Esto se está haciendo difícil, con estos nuevos requerimientos el procedimiento del registro de ccTLD es cada vez más complejo para el registratario final, ¿significa esto que se van a cansar y van a ir a algún otro lado donde sea más fácil obtener un nombre de dominio? Esto podría llegar a ser un problema ya que estaríamos compitiendo con otros CC y gTLD también, pero, por otra parte, creo que todos buscamos regenerar la confianza en internet y entonces creo que, en última instancia, encontramos el equilibrio adecuado entre sobre carga y ser demasiado relajados.

Vamos a seguir trabajando juntos porque somos un grupo de registros que comparten la misma carga, en términos generales, al menos podemos quejarnos entre nosotros, pero también es cierto que compartimos recursos y esto es muy útil. Creo que con esto termine mi presentación, ¿es esta la última imagen? Sí.

ANNALIESE WILLIAMS: Gracias, Bárbara, creo que señaló un punto muy importante con respecto a pensar hacia adelante y a ser proactivos. ¿Alguien tiene alguna pregunta para Bárbara? Veo varias preguntas, creo que esta persona estaba, primero, adelante.

UGO AKIRI: Yo era parte de .NG. Mi pregunta para Bárbara es la siguiente. Cuando usted dice que algunos países europeos están un poco retrasados, ¿significa que no están adoptando GDPR en todos los países miembros de la Unión Europea?

BÁRBARA POVSE: Gracias por su pregunta. No, no, eso no es lo que quise decir, no quise decir que algunos países están retrasados, quizás lo dije mal y es culpa mía. La legislación es la mismo, el marco jurídico es exactamente el mismo para todos los países europeos de la Unión Europea, eso es lo mismo para todos, lo que quise decir es que, hay una gran carga sobre los ccTLD europeos, a eso me quise referir. Los ccTLD europeos quizás estén presionando un poco más que otros, eso es lo que quise decir.

ANNALIESE WILLIAMS: Gracias por la aclaración. Hay una pregunta aquí y también hay una pregunta en Zoom, pero vamos, primero, a la pregunta de la persona que está aquí en la sala.

OMAR CONTRERAS: Una de las cosas que me gustaron de su presentación es la parte de colaboración, tenemos recursos limitados, tenemos que trabajar en distintos niveles y está muy bien que aprovechemos al máximo los recursos, quisiera saber si tiene alguna recomendación para ccTLD que están fuera de Europa, me refiero con respecto a tener ese mismo tipo de cooperación en América Central, en América del Sur, ¿cómo iniciaron ustedes esos canales? ¿Cómo encontraron esas áreas para al menos desarrollar juntos los recursos para después tratar de seguir avanzando? ¿Tiene algún consejo, recomendación o sugerencia?

BÁRBARA POVSE: Bueno, quizás la situación es diferente en Europa porque nosotros compartimos el mismo marco legal, entonces, si bien existe una implementación nacional que puede ser diferente, nosotros tenemos sí leyes nacionales que pueden ser diferentes, pero sigue habiendo un marco general y todos trabajamos bajo ese marco.

Cuando yo hacía la lista en las presentaciones, lo mismo pasa en Costa Rica o en Vanuatu, básicamente es la misma legislación la que está surgiendo y yo creo que lo que puede hacer una organización regional, en Europa hablamos de CENTR, pero creo que son esas organizaciones que pueden, es al menos brindar un lugar para que los hacedores de políticas se reúnan y encuentren aspectos comunes.

ANNALIESE WILLIAMS: Gracias, Bárbara. Vamos a tomar una pregunta de la sala de Zoom. Michele, por favor.

MICHELE NEYLON: Bueno, de hecho, estoy en la sala también, pero bueno.

ANNALIESE WILLIAMS: No lo había visto, perdón.

MICHELE NEYLON: Soy Michele Neylon de Blacknight. Bárbara la carga regulatoria, sé que lo están mirando desde el lado de los registros y yo lo estoy mirando del lado de los registradores, y tratando de obviamente pagar las cuentas y ganar dinero en este espacio. ¿Tienen alguna idea de si la Comisión Europea y sus amigos entienden el nivel de desventaja competitiva en la que nos ponen a todos con esta carga regulatoria? Porque si yo miro cómo los estadounidenses se están riendo de todo esto cada vez que surge algo al respecto.

La verdad resulta frustrante, entonces, ¿vemos la luz al final del túnel? ¿O seguimos enmarañados con este trabajo?

BÁRBARA POVSE: Bueno, lamento decirle que creo que no tengo buenas noticias, pero eso es lo que yo quería decir, yo lo que mencioné es a los registros y no es justo, es verdad, no solo para los registros también para los registradores, para las empresas en general. Están enfrentando estos problemas para seguir siendo competitivos en un espacio altamente

regulado y creo que no tengo una respuesta, pero sí estoy de acuerdo con usted, si le ayuda en algo.

MICHELE NEYLON: Bueno, sí, puedo tomarlo, si el registro está de acuerdo siempre me pongo contento.

ANNALIESE WILLIAMS: ¿Alguna otra pregunta para Bárbara? Bruce.

BRUCE TONKIN: Quiero hablar un poco de un marco más general. Obviamente cuando tenemos CC involucrados y, además, en la Unión Europea se está hablando de lo que hacen todos los CC en su lugar a nivel regional, pero no sé si hay grandes cambios en otras áreas donde puede haber un daño colateral, por ejemplo, cuando estamos hablando de la infraestructura crítica de seguridad, que es algo muy importante en muchos sectores, o todo lo que tiene que ver con privacidad o protección a los clientes.

Entonces, ¿este es un problema para la industria del dominio en sí mismo o hay un problema más amplio y esto encaja dentro de eso?

BÁRBARA POVSE: ¿Me está preguntando si hoy están tratando de resolver la Comisión Europea? ¿O qué?

BRUCE TONKIN: Sí, la Comisión Europea, ¿no? Si están tratando de resolver ese problema.

BÁRBARA POVSE: Yo creo que están tratando de… A ver, estoy adivinando, pero yo creo que el objetivo principal es generar confianza en internet, ese es el objetivo principal, ¿de qué manera lo hacen?

BRUCE TONKIN: Estamos hablando de economía digital, por ejemplo, generar confianza en la economía digital o en el comercio digital, ¿es esto lo que están tratando de hacer? Es interesante entonces.

BÁRBARA POVSE: No, la verdad me perdí.

BRUCE TONKIN: No, estoy tratando de ver qué es lo que impulsa toda esta reglamentación en Europa.

BÁRBARA POVSE: No estoy muy segura y creo que no se halló la persona a la que le deben preguntar esto.

BART BOSWINKEL: Annaliese, puede haber muy buenas preguntas entonces para que las vea el IGLC.

ANNALIESE WILLIAMS: Tenemos varios miembros del área de la Unión Europea, así que, también lo agrego a la lista, Bart. Hay una pregunta, tenemos a Chris y veo también que Jordan ha levantado la mano.

CHRIS DISSPAIN: Gracias, Annaliese. Para responder a lo que dijo Michele yo le puedo dar mi opinión. No creo que a ellos les importe, creo que ellos crean o están determinados, decididos a legislar lo que no lograron a través del modelo de múltiples partes interesadas y el hecho de que, esté apuntado a los ccTLD es porque ahí no tienen opción, podemos hablar de que algunos reguladores europeos dicen que esto se tiene que aplicar a todos, que nosotros sabemos que eso empezó con los ccTLD, no es así, pero ellos dicen que sí.

Ahora, el año pasado yo hice una sesión en la escuela de verano europea hablando de la fragmentación y uno de los panelistas, no voy a dar el nombre porque no sería adecuado, es una persona con cargo alto en la Comisión Europea dijo: “Sí, estamos fragmentando internet porque ustedes no hacen lo que nosotros queremos”. Entonces es este trasfondo.

ANNALIESE WILLIAMS: Gracias, Chris, creo que eso es un comentario. Ahora Jordan.

JORDAN CARTER: Gracias, Annaliese. Sí, creo que es una pregunta. Bárbara dijeron que la forma en la que la Unión Europea está sancionando la reglamentación a la velocidad, ¿esto guarda coherencia con el apoyo del público de múltiples partes interesadas?

BÁRBARA POVSE: Bueno, me están poniendo en el centro de la escena y me están señalando todos, pero la verdad...

ANNALIESE WILLIAMS: Bueno, creo que podemos hablar como grupo en otro momento, creo que es una sugerencia, lo vamos a agregar entonces para que el comité lo debata.

BÁRBARA POVSE: Gracias por salvarme.

ANNALIESE WILLIAMS: ¿Alguna otra pregunta para Bárbara o para alguno de los otros presentadores? A quienes estuvieron ahí como disertantes. Michele, ¿levantó la mano, nuevamente?

MICHELE NEYLON: Sí. Quería agradecerle a usted porque realmente fueron muy… Nos ayudaron mucho en los últimos años, nos ayudaron a tratar de

navegar a través de esta locura que surge de la Comisión Europea. Nosotros podemos tener esta ida y vuelta, ¿no? Pero, en realidad, la Comisión Europea está tratando de regularse a sí misma porque, como dijo Chris, no lo tienen en otro lugar, entonces tratan de presionar por donde pueden presionar y la verdad no me importa, pero bueno, voy a tratar de navegar en todo esto y todos nos preocupamos por NIS2, etc.

Tenemos que tener los ojos abiertos cuando estamos fuera de la Unión Europea porque todos empiezan a decir: "Uy, miren lo que están haciendo los europeos". Y bueno, la verdad es que son los estadounidenses los que se ríen de una punta a la otra, pero bueno, realmente CENTR ha sido muy útil y nos ha ayudado mucho.

BÁRBARA POVSE: Bueno, sí, si el registrador está contento el registro también.

ANNALIESE WILLIAMS: Bueno, creo que entonces podemos cerrar, escuchamos a todos los oradores hablar de que la seguridad cibernética es un área clave que preocupa a todos los gobiernos, hay mucha legislación que ya ha sido sancionada y hay muchas que están siendo debatidas para ser sancionadas. Entonces les agradecemos la oportunidad de escucharnos unos a otros, aprender unos de otros y les pido que entre todos le agradezcamos a nuestros oradores, sobre todo a Norman y Lourino porque hicieron, por primera vez, una presentación entre la ccNSO. Muchas gracias, damos por cerrada la reunión.

[FIN DE LA TRANSCRIPCIÓN]