Reporte de LACTLD sobre el IGF 2019

Berlín, Alemania

25-29 de noviembre de 2019

LACTLD
Latin American and Caribbean ccTLDs Organization

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

LACTLD
Latin American and Caribbean ccTLDs Organization

Contenidos

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Reporte de LACTLD sobre el IGF 2019

Introducción

La 14ª Reunión Anual del Foro para la Gobernanza de Internet (IGF 2019) tuvo lugar en Berlín, Alemania, del 25 al 29 de noviembre de 2019. El emblema primordial del IGF 2019 fue: *Un mundo. Una red. Una visión*.

Durante cinco días, 3679 delegados participaron presencialmente en 200 sesiones. Berlín recibió a participantes de 161 países diferentes. El 42% de ellos fueron mujeres y el 53% asistía por primera vez a un IGF.

El Reporte de LACTLD sobre el IGF 2019 presenta los principales mensajes del IGF de Berlín en torno a los tres temas clave del IGF 2019: seguridad, protección, estabilidad y resiliencia; gobernanza de datos; e inclusión digital. El informe también examina algunas de las sesiones de interés para la comunidad de los ccTLD. Destaca los principales debates y recomendaciones de políticas que se identificaron en cada una de estas sesiones.

Mensajes del IGF de Berlín

Los mensajes del IGF de Berlín se publican en el sitio web oficial del IGF proporcionado por las Naciones Unidas.

Con el fin de reflexionar sobre las discusiones generales desarrolladas durante el IGF 2019, se elaboró un conjunto consolidado de mensajes para los tres temas principales de la 14ª Reunión Anual del IGF. Estos mensajes se basan en los informes de sesiones elaborados por los organizadores y en los debates que tuvieron lugar en Berlín.

Seguridad, protección, estabilidad y resiliencia

Este tema trata sobre el papel vital de la ciberseguridad, la seguridad en línea, la estabilidad y la resiliencia de la infraestructura como requisitos previos para el crecimiento económico y un entorno digital sano y beneficioso para todos. También, aborda las perspectivas multisectoriales y multidisciplinarias para la protección tanto de los sistemas como de los usuarios, obteniendo una mejor comprensión de los aspectos multidimensionales relacionados con los riesgos, las amenazas y las diferentes formas de abordarlos.

Otro aspecto clave de este tema implica la colaboración de las partes interesadas para responder eficazmente a la creciente y rápidamente cambiante gama de amenazas para la Internet global y sus usuarios, al tiempo que se busca preservar los beneficios que todos disfrutan.

Mensajes sobre la seguridad en línea

- Internet solo alcanzará su potencial como canal de libre expresión y motor de crecimiento económico si continúa siendo un lugar seguro donde las personas se sientan protegidas. Cualquier enfoque de ciberseguridad debe tratar de preservar los beneficios que disfrutan los usuarios, al tiempo que se abordan los riesgos. Para ello, es necesario

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

adoptar enfoques holísticos que protejan a los usuarios en línea y, a la vez, fomenten o mantengan su confianza en el uso de Internet.

- La seguridad y los derechos y libertades fundamentales de las personas pueden coexistir, pero a veces es necesario hacer concesiones. Sin embargo, la prioridad de la seguridad por encima de los derechos y libertades de las personas, incluyendo la libertad de expresión y la privacidad, debe ser legítima, proporcionada y basada en el estado de derecho.
- Los debates sobre la seguridad en línea deben basarse en datos sólidos.
- Para lograr la seguridad en línea, se requiere la participación de las partes interesadas en diferentes niveles. Los actores de la industria y las partes interesadas deben explorar qué es tangible y alcanzable cuando se trata de reunir y compartir información para la prevención del abuso en línea. Juntos podrían acordar formas de actuar y cooperar sobre la base de un entendimiento compartido.

Mensajes sobre la seguridad de la infraestructura

- Si bien la tendencia actual de abordar el contenido ilícito o abusivo a partir de la cancelación, transferencia, eliminación o suspensión de los nombres de dominio parece ser una solución rápida y fácil, no ofrece una forma eficaz y sostenible para eliminar el contenido malicioso.
- Las plataformas y los proveedores en línea, al tiempo que adoptan las medidas adecuadas para suprimir o bloquear los contenidos ilegales, también deberían ponerse en contacto y cooperar con los organismos de cumplimiento de la ley para proporcionar información a fin de adoptar medidas preventivas. Los formadores de políticas y las partes responsables deberían estudiar mejor las posibilidades y limitaciones de las soluciones técnicas mediante asociaciones de colaboración entre múltiples partes interesadas.
- Más de un cuarto del tráfico de Internet funciona actualmente en IPv6. Las partes interesadas deben seguir comprometiéndose y colaborando para que esta importante transición continúe.

Mensajes sobre políticas y cooperación

- El ritmo de desarrollo de la tecnología está superando los procesos tradicionales para establecer políticas y procesos regulatorios que permitan abordar las cuestiones de seguridad de manera oportuna. Es necesario mejorar la colaboración para desarrollar e implementar soluciones de políticas, y para que los procesos de desarrollo de normas sean inclusivos y respetuosos de los derechos humanos.
- En el actual clima de crecientes tensiones entre los países en el ciberespacio –que da lugar al desarrollo de armas cibernéticas cada vez más sofisticadas, tanto defensivas

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

como ofensivas– es importante aplicar medidas eficaces de fomento de la confianza para establecer y promover la estabilidad y seguridad global en línea.

Mensajes sobre la creación de capacidades

- Los usuarios de Internet tienen la obligación de contribuir a su seguridad personal en línea. Sin embargo, sólo se puede esperar que actúen como usuarios responsables si comprenden lo que está en juego, son conscientes de los riesgos, conocen sus derechos y han aprendido a actuar de acuerdo a ellos. Los usuarios, en particular los niños, necesitan ser empoderados. La formación y la creación de capacidades en materia de ciberseguridad deberían permitir a todos los usuarios, incluidos los grupos más vulnerables y las minorías, estar más seguros en línea y ser capaces de exigir y defender sus derechos humanos.

- Existen importantes oportunidades para mejorar la seguridad del ecosistema global a través de acciones significativas que promuevan la confianza y aumenten la capacidad entre los estados nacionales, y entre los estados y otras partes interesadas.

Gobernanza de datos

Este tema se ocupa del papel de la gobernanza de datos en el fomento del crecimiento económico, la innovación, el progreso social y el desarrollo sostenible. Los debates sobre la gobernanza de los datos abordan la mejor forma de garantizar el desarrollo de marcos de protección de datos centrados en las personas a nivel nacional, regional e internacional, así como en cuestiones transfronterizas relacionadas, que respeten los derechos humanos, potencien a las personas y promuevan el desarrollo sostenible.

El tema también abarca las condiciones y los marcos éticos necesarios para facilitar la innovación basada en los datos, garantizar una competencia leal y fomentar la confianza en Internet y las tecnologías digitales.

Mensajes sobre el desarrollo y los flujos transfronterizos de datos

- Cuando los datos cruzan las fronteras, a menudo se aplican múltiples marcos jurídicos y normativos, como las normas de protección de datos personales, los requisitos de divulgación de datos y los procesos de reparación judicial. Este panorama puede generar incertidumbre en las cadenas de distribución globales basadas en los datos.

- El trabajo colaborativo en un contexto global que permita desarrollar valores y principios comúnmente acordados para los marcos regulatorios podría contribuir a fomentar la confianza en los flujos transfronterizos de datos, con los consiguientes beneficios económicos y sociales.

Mensajes sobre los datos como recurso clave de nuestra economía y sociedad

- El aumento del uso de la Internet de las cosas (IoT) en la infraestructura urbana también da lugar inevitablemente a que se produzcan, recopilen y compartan más datos. Es esencial asegurar que los servicios públicos se centren en las personas y se basen en

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

los datos, promoviendo la participación y la transparencia en el diseño de dichos servicios. El desarrollo sostenible y la protección de los derechos fundamentales de todas las personas, incluidos los grupos marginados, deberían ser los objetivos generales de la formulación de políticas.

- La falta de una adecuada gobernanza de los datos centrada en el individuo a nivel mundial y nacional limita el potencial de los datos como recurso clave para el desarrollo sostenible.

Inclusión digital

Este tema se centra en cómo la inclusión digital se sitúa en el corazón del IGF, reflejando el objetivo de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) de construir "una Sociedad de la Información centrada en las personas, inclusiva y orientada al desarrollo, en la que todos puedan crear, acceder, utilizar y compartir información y conocimientos".

Mensajes sobre el acceso inclusivo a Internet y su infraestructura

- El crecimiento de los usuarios de Internet se ha ralentizado y conectar a los que no están conectados continúa siendo un gran desafío. Al mismo tiempo, los ataques contra la conectividad a Internet se han convertido en un peligroso instrumento de la política.

Mensajes sobre la inclusión social y económica, la igualdad de género y los derechos humanos

- Los sesgos y la exclusión continúan estando profundamente arraigados en los espacios digitales. El debate sobre la inclusión de las personas marginadas debería estar en el centro de las conversaciones sobre la gobernanza de Internet y las políticas públicas, y no en los márgenes.

Mensajes sobre el contenido local y la diversidad lingüística

- La adopción de los Nombres de Dominio Internacionalizados (IDN) necesita más estímulo y apoyo por parte de todas las partes interesadas para aumentar así los beneficios que se hacen posibles al tener dominios de Internet en los idiomas y alfabetos locales.

- La aceptación universal de los IDN y de las direcciones de correo electrónico internacionalizadas no es sólo una cuestión técnica, sino también una cuestión de políticas. Los gobiernos y las entidades públicas deberían promover la aceptación universal y dar el ejemplo mediante el uso de los IDN.

- Los derechos de autor pueden ser tanto un facilitador de la producción de contenido local como una barrera para la creación y distribución de este contenido. Las licencias Creative Commons dan a los creadores de contenidos el control sobre la forma en que sus contenidos son compartidos y reutilizados.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Sesiones de interés para la comunidad de los ccTLD

IGF 2019 OF #6 ICANN: DNS, amenazas y oportunidades

Tema: Seguridad, protección,estabilidad y resiliencia
Subtema: Ciberataques / Sistema de nombres de dominio / Recursos de Internet

El Foro se centró en los Planes Estratégicos y Operativos de la ICANN para 2020-2025. Estos Planes cubren una serie de temas como la seguridad, el desarrollo del DNS, el desarrollo global y la mejora del modelo de gobernanza de múltiples partes interesadas, con un enfoque en el potencial del DNS en términos de amenazas y oportunidades. La sesión reveló un gran optimismo sobre el futuro del DNS (por ejemplo, sobre cuestiones relacionadas con el aumento de los IDN), pero también preocupación sobre el impacto del abuso en el DNS, y sobre cómo este abuso afecta a la confianza.

Si bien no se definieron recomendaciones específicas, hubo acuerdo sobre la importancia de abordar los problemas de abuso desde múltiples frentes con el propósito de aumentar la confianza futura en el uso y desarrollo del DNS.

Transcripción de la sesión

Video de la sesión

IGF 2019 OF #16 Enfoques de colaboración multistakeholder en materia de ciberseguridad

Tema: Seguridad, protección,estabilidad y resiliencia
Subtema: Creación de capacidades / Ciberataques / Mejores prácticas de ciberseguridad

Una de las principales conclusiones de la sesión fue que los desafíos de la ciberseguridad son amplios y están interrelacionados. Por lo tanto, es necesario adoptar enfoques inclusivos y de múltiples partes interesadas en las estrategias de ciberseguridad.

Durante la sesión, muchos indicaron que deberían establecerse programas y enfoques claros para ayudar a la aplicación práctica de la ciberseguridad. Además, se expresó un gran apoyo a la colaboración en materia de ciberseguridad, y al desarrollo e intercambio de capacidades.

Otro aspecto clave del debate fue la necesidad de trabajar de forma más cohesionada con los organismos encargados del cumplimiento de la ley y la necesidad de apoyar la investigación policial y el enjuiciamiento de los delitos cibernéticos.

Algunas de las principales recomendaciones y sugerencias en materia de política formuladas en la sesión fueron: el desarrollo de capacidades de los organismos de cumplimiento de la ley para la recopilación y presentación de pruebas; la sensibilización de los usuarios sobre las amenazas a la ciberseguridad; la implementación de mecanismos de denuncia de los delitos cibernéticos entre los usuarios; el fortalecimiento de la ciberseguridad para las elecciones; la promoción de la colaboración entre los expertos en ciberseguridad y las comunidades locales a fin de elaborar estrategias eficaces.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Transcripción de la sesión

Video de la sesión

IGF 2019 WS #331 ¿Debemos combatir el contenido ilícito a través del DNS?

Tema: Seguridad, protección,estabilidad y resiliencia
Subtema: Sistema de nombres de dominio / Derechos humanos / Contenido ilícito

Esta sesión fue organizada por NIC.br / CGI.br y LACTLD. El panel contó con representantes del sector privado, los gobiernos, la comunidad técnica y la sociedad civil de Europa, Asia-Pacífico, África y América Latina y el Caribe.

Al comienzo de la discusión, se planteó una distinción entre la supresión y la suspensión de un nombre de dominio. Los oradores compartieron sus puntos de vista sobre el tratamiento del contenido ilegal en el nivel del DNS.

Manal Ismail (Gobierno, Grupo Africano) sostuvo que, en algunas circunstancias, existen razones legítimas que justifican las demandas de eliminación de contenidos por parte de los gobiernos.

Polina Malaja (Comunidad Técnica, Grupo de Europa Occidental) consideró que los ccTLDs son solo actores técnicos, con la responsabilidad de operar las infraestructuras DNS de su propio TLD, así como de mantener la base de datos del registro. La oradora presentó un panorama general de las responsabilidades de los ccTLD y de las experiencias de una serie de países de Europa que han elegido diferentes enfoques para resolver los conflictos en el DNS.

Thomas Rickert (Sector privado, Grupo de Europa Occidental) afirmó que la manipulación en el DNS puede ser mal manejada por los operadores que no toman en cuenta las medidas más apropiadas para la eliminación de los contenidos. Destacó que el problema debe delimitarse correctamente a fin de dar la respuesta adecuada, reducir la visibilidad del contenido, ayudar a las víctimas y detener los escenarios de abuso.

Miguel Ignacio Estrada (Comunidad Técnica, Grupo LAC) indicó las razones por las cuales no se debería actuar en el nivel del DNS para resolver los problemas relacionados con el contenido, desde la perspectiva técnica hasta la jurídica. También, destacó que los titulares de las marcas están trabajando para proporcionar herramientas a los profesionales del derecho, con el fin de encontrar a los responsables de los contenidos ilegales en línea, en lugar de pedir a los jueces que ordenen el retiro de los nombres de dominio.

Jennifer Chung (Comunidad Técnica, Grupo de Asia y el Pacífico) advirtió que el contenido ilícito también puede encontrarse en sitios web legítimos, por lo que no hay forma de que un operador de registro lo elimine quirúrgicamente. Las opciones disponibles para un registro son la suspensión completa, la retención y/o la eliminación del nombre de dominio. No obstante, quienes tienen un registro de la dirección IP pueden seguir teniendo acceso a ese contenido ilícito. Por lo tanto, los registros no pueden utilizar sus marcos actuales para abordar esta situación.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Sobre la base de las contribuciones de los oradores, una serie de recomendaciones y sugerencias de políticas fueron propuestas durante la sesión:

- Proporcionar a los jueces y fiscales información y herramientas adecuadas para que puedan encontrar a los responsables de los contenidos.
- Ayudar a difundir los riesgos que implica la adopción de acciones en el nivel del DNS. Informar que los proveedores de alojamiento y los propietarios de los contenidos son los actores adecuados a los que se deben destinar las acciones en primer lugar.
- Definir límites claros para guiar las acciones en el nivel del DNS, así como definir algún tipo de cadena de acciones a probar en primer lugar.
- Fomentar un mayor diálogo y colaboración entre las partes interesadas para alcanzar soluciones consensuadas a los diversos problemas relacionados con este debate.

Transcripción de la sesión

Video de la sesión

IGF 2019 WS #216 Identidad en línea en el espacio multilingüe de los nombres de dominio

Tema: Inclusión digital
Subtema: Acceso / Brecha digital / Multilingüismo

El debate de la sesión demostró claramente el problema al que se enfrentan tanto los que defienden una Internet con contenido lingüístico diverso como los que defienden la Aceptación Universal (UA).

Esencialmente, hay una falla de mercado ya que no hay suficientes incentivos para que los desarrolladores, operadores o actores del DNS hagan que sus sistemas sean compatibles con UA/IDN, dada la baja demanda de tales nombres debido, a su vez, a la falta de Aceptación Universal (UA).

La sesión ilustró el problema, los mecanismos para abordarlo y el enfoque necesario en el sector público. Se identificó la necesidad de un enfoque tanto de abajo hacia arriba como de arriba hacia abajo. En último caso, la utilización de estándares sería considerado otro posible vehículo para exigir la prestación de servicios que reconozca todos los nombres de dominio.

Transcripción de la sesión

Video de la sesión

IGF LAC Space

El IGF LAC Space tuvo su cuarta edición en el IGF 2019. El encuentro fue organizado por LACTLD y reunió a más de 70 asistentes, representantes de 22 organizaciones de América Latina y el Caribe.

Los participantes de las organizaciones de la comunidad técnica y de otras partes interesadas pudieron compartir sus actualizaciones y actividades realizadas durante 2019, y también tuvieron la oportunidad de presentar sus proyectos para el próximo año.

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22

Al igual que en ediciones anteriores, el IGF LAC Space permitió conectar a los actores de América Latina y el Caribe y mejorar las actividades de colaboración y cooperación en toda la región.

Video de la sesión

Rambla República de México 6125
Montevideo, Uruguay
+598 2 604 22 22