



Reporte de LACTLD sobre el IGF 2020

Reunión virtual

Fase I, 2-6 de noviembre de 2020

Fase II, 9-17 de noviembre de 2020



lactld

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

Contenidos

Introducción	3
Sesiones relevantes para la comunidad de los ccTLD	3
Sesión principal: Confianza	3
Abuso en el DNS en la era de COVID-19: Lecciones aprendidas	4
DNS sobre HTTPS (DoH): Derechos humanos, mercados y gobernanza	5
Foro Abierto de la ICANN - Gobernanza técnica de Internet	6
Colaboración de las NRI: Políticas y normas locales de ciberseguridad	7
Manteniéndonos unidos: Infraestructura de Internet en emergencias	8
IGF 2020 Pre-Event #9 IGF LAC Space	8

Introducción

La décimo quinta edición del Foro de Gobernanza de Internet (IGF) reunió a 6136 participantes de 173 países para discutir distintos asuntos y desafíos en torno a cuatro temáticas fundamentales: datos, medio ambiente, inclusión y confianza. El IGF 2020 contó con 275 sesiones llevadas a cabo en dos fases, que se extendieron durante 12 días. Por primera vez, el Foro se realizó completamente online, en respuesta a la pandemia de COVID-19, bajo el lema general: “Internet para la resiliencia y la solidaridad humanas”.

Con el objetivo de ofrecer una visión general sobre los asuntos y posiciones claves abordados en las sesiones, la Secretaría del IGF ha consolidado una serie de mensajes para los cuatro temas clave del Foro: datos, medio ambiente, inclusión y confianza. Los Mensajes del IGF 2020 pueden ser consultados [aquí](#).

El Reporte de LACTLD sobre el IGF 2020 repasa una serie de sesiones sobre temas relevantes para la comunidad de los ccTLD, tales como: abuso en el DNS, DNS over HTTPS (DoH), políticas y regulaciones de ciberseguridad, gobernanza técnica de Internet y desafíos en torno a la confianza en la red. Además, el documento examina las discusiones regionales que se llevaron a cabo en la cuarta edición del IGF LAC Space.

Sesiones relevantes para la comunidad de los ccTLD

IGF 2020 Sesión principal: Confianza

Tema: Confianza

La sesión principal del IGF sobre la confianza facilitó un debate entre múltiples actores sobre la soberanía digital, los desafíos jurídicos transfronterizos, la fragmentación de Internet y la propuesta de un nuevo IP. Durante el debate, se subrayó la falta de coordinación y cooperación entre las partes interesadas en cuestiones jurídicas transfronterizas y la necesidad de respetar la infraestructura técnica de Internet.

Los participantes del gobierno, el sector privado, las organizaciones intergubernamentales, la sociedad civil y la comunidad técnica compartieron diferentes puntos de vista sobre las nociones de soberanía digital y soberanía de los datos, y su impacto en la infraestructura de Internet. Por una parte, el panelista del Ministerio Federal de Asuntos Económicos y Energía de Alemania afirmó que la soberanía digital se refiere a la autodeterminación en el desarrollo de la economía digital, la utilización de datos, los modelos comerciales, etc. Por otra parte, el orador de la UIT sostuvo que la noción de soberanía es pertinente porque

permite que los usuarios o ciudadanos sepan cómo se están tratando sus datos personales.

La discusión del panel también examinó la noción de la escasez de datos y el control. El panelista de Microsoft sostuvo que los datos no son un bien escaso en términos económicos y, por lo tanto, pueden compartirse entre diferentes actores con el fin de fomentar el desarrollo social y económico. En este sentido, la oradora de Research ICT Africa afirmó que actualmente los datos son convertidos artificialmente en un recurso escaso por los gobiernos y las grandes plataformas. Añadió que es necesario desarrollar un sistema transnacional que permita el movimiento transfronterizo de los flujos de datos.

La oradora del IETF aportó reflexiones clave a la discusión de la sesión. Sostuvo que la soberanía de los datos introduce restricciones y complejidad en la arquitectura de Internet. La Presidenta del IETF explicó que Internet fue diseñada para facilitar la interconexión global y para ignorar explícitamente las fronteras nacionales. Añadió que el diseño de las tecnologías troncales de Internet no se ajusta a ninguna jurisdicción en particular, sino que tiene por objeto mejorar el rendimiento y la seguridad de la red, así como facilitar su gestión y configuración. La panelista de la comunidad técnica afirmó que es muy importante mantener unido el tejido de Internet y respetar su arquitectura técnica.

[Grabación de la sesión](#)

IGF 2020 WS #317 Abuso en el DNS en la era de COVID-19: Lecciones aprendidas

Tema: Confianza

Cuestiones: Mejores prácticas de ciberseguridad / Abuso en el DNS / Seguridad del DNS

La sesión examinó los datos más relevantes sobre los niveles de abuso registrados en los últimos meses. Los panelistas de la comunidad técnica y del sector privado compartieron opiniones comunes, ejemplos de iniciativas actuales para estudiar y vigilar el abuso en el DNS, ideas para la colaboración futura y posibles pasos a seguir.

Los panelistas coincidieron en que no ha habido un aumento en los niveles de abuso en el DNS durante la pandemia. Explicaron que, si bien se han detectado incrementos en los registros de nombres de dominio relacionados con el coronavirus, muchos de ellos fueron con fines especulativos y/o no maliciosos. Según los panelistas, el aumento de los registros de nombres de dominio asociados a un tema específico es una tendencia que suele verse como resultado de temas populares y acontecimientos importantes que ganan la atención y la repercusión de los medios de comunicación. El orador de la ICANN señaló que,

además de examinar los datos, es importante reunir información detallada sobre los dominios que se consideran “de riesgo” para determinar los niveles reales de abuso. Por lo tanto, añadió que a pesar de que se monitorearon miles de registros por día, tan solo decenas de estos dominios estaban relacionados con casos de abuso en el DNS.

Los oradores analizaron también las actividades de colaboración durante la pandemia. Constataron que los actores del ecosistema del DNS han actuado conjuntamente y en colaboración para vigilar los niveles de abuso que pudieran estar relacionados con el COVID-19.

Durante la sesión, la representante del sector privado subrayó que los registros y registradores no están en la posición adecuada para mitigar el abuso de contenido. También explicó que la industria ha organizado diversas iniciativas fuera de la ICANN con el objetivo de abordar de manera eficaz y adecuada el abuso, tales como: el *Framework to Address Abuse*, los recursos y documentos de Internet & Jurisdiction Policy Network, y otras alianzas y coaliciones de la industria en torno a categorías específicas de abuso.

Finalmente, los oradores compartieron sus ideas sobre los posibles pasos a seguir. En general, se destacó la importancia de fortalecer la colaboración entre las partes interesadas y de hacer participar a toda la industria en estos esfuerzos. La panelista del sector privado declaró que seguirán consolidando los instrumentos con los que han venido trabajando y fortaleciendo sus relaciones con la industria.

[Grabación de la sesión](#)

IGF 2020 WS #73 DNS sobre HTTPS (DoH): Derechos humanos, mercados y gobernanza

Tema: Datos

Cuestiones: Competencia / Derechos Humanos / Estándares Técnicos

La discusión sobre DoH analizó los principales desafíos y preocupaciones relacionados con la implementación y el despliegue del protocolo, la concentración del mercado, la centralización de los datos del DNS, su posible impacto en el cumplimiento de la reglamentación nacional y los efectos extraterritoriales de las políticas. Además, los panelistas conversaron sobre la forma en que DoH puede proteger los derechos fundamentales de los usuarios (privacidad, libertad de expresión, libertad de acceso a la información) y eludir la censura.

Los expositores de los distintos sectores ofrecieron sus miradas sobre el asunto. Por un lado, uno de los panelistas de la comunidad técnica explicó que si bien DoH no altera el mecanismo básico de consulta/respuesta del DNS, su

implementación y despliegue podría tener efectos variados para los distintos actores. En esta línea, se planteó la necesidad de evaluar y monitorear el impacto que DoH puede tener sobre las propiedades críticas de Internet, tales como la gestión descentralizada de la red, su arquitectura abierta e interoperable, su resiliencia, entre otras.

Por otro lado, la expositora de la sociedad civil argumentó que los datos del DNS no encriptados han sido filtrados, controlados y regulados a través de distintas técnicas a los largo del tiempo. Por lo tanto, sostuvo que el cifrado de estos datos no solo protege la privacidad y el anonimato de los usuarios, sino que es un avance técnico necesario para eludir la censura y proteger derechos fundamentales, tales como la libertad de expresión y la libertad de acceso a la información. La expositora de la sociedad civil agregó que DoH deberá ser implementado con consideraciones normativas y reglamentarias fundamentales y las preocupaciones de los distintos actores deberán ser abordadas a través de un enfoque de las múltiples partes interesadas.

Durante la última parte de la sesión, los expositores participaron en una discusión abierta sobre la soberanía de los datos, la interacción del GDPR con los datos del DNS, la concentración de proveedores de DNS cifrados, y la influencia extraterritorial de las políticas domésticas. Finalmente, destacaron la importancia de continuar el diálogo entre los distintos sectores con el fin de abordar integralmente los desafíos y preocupaciones en torno a DoH.

[Grabación de la sesión](#)

IGF 2020 OF #44 Foro Abierto de la ICANN - Gobernanza técnica de Internet

Tema: Confianza

Cuestiones: Abuso en el DNS / Seguridad del DNS / Seguridad de enrutamiento

Los miembros de la Junta Directiva de la ICANN y de la organización de la ICANN debatieron la noción de gobernanza técnica de Internet y analizaron la función que la ICANN está desempeñando para garantizar que Internet siga evolucionando de manera segura, estable e interoperable.

El Presidente y CEO de ICANN, Göran Marby, diferenció la gobernanza de Internet de la gobernanza técnica de Internet. En términos generales, sostuvo que la primera está directamente vinculada a los asuntos de acceso y uso de la red. En cambio, la segunda se concentra especialmente en el funcionamiento de Internet.

En este sentido, Göran Marby informó que la ICANN está trabajando en la gobernanza técnica de Internet con el objetivo de mejorar la comprensión de los fundamentos técnicos del funcionamiento de Internet entre los legisladores, los reguladores y otras partes interesadas no técnicas. De este modo, busca prevenir los efectos imprevistos y perjudiciales de las nuevas políticas y regulaciones sobre el funcionamiento técnico de la red. En otras palabras, la ICANN tiene la intención de informar sobre las consecuencias técnicas de determinadas políticas a fin de mantener una Internet estable, segura y resiliente. Göran Marby añadió que la ICANN está dirigiendo su atención a los debates que se están llevando a cabo en tres espacios principales: las iniciativas de las organizaciones intergubernamentales, los órganos de estandarización y las propuestas de regulación a nivel nacional o regional.

Durante el Foro Abierto, los oradores examinaron diversos proyectos e iniciativas que la ICANN ha llevado a cabo con el fin de proporcionar información objetiva e imparcial sobre el sistema de identificadores únicos de Internet. Asimismo, el Director Técnico de la ICANN, David Conrad, discutió el impacto que nuevas tecnologías específicas (como 5G, el nuevo IP, Digital Object Architecture, Blockchain) podrían tener en el funcionamiento técnico de Internet.

[Grabación de la sesión](#)

IGF 2020 Sesión de colaboración de las NRI: Políticas y normas locales de ciberseguridad

Tema: Confianza

Durante la sesión, se abordaron los marcos de ciberseguridad aplicados por los distintos países y los mecanismos de cooperación establecidos en los planos local, regional y global. El debate también abarcó las cuestiones de ciberseguridad más importantes entre las iniciativas nacionales y regionales de gobernanza de Internet.

Los panelistas describieron varias iniciativas clave para fortalecer la cooperación en materia de ciberseguridad. También formularon recomendaciones pertinentes al respecto. En primer lugar, se destacó la necesidad de sensibilizar a los diversos actores sobre las cuestiones de ciberseguridad. En segundo lugar, los oradores señalaron la necesidad de crear una cultura de ciberseguridad dentro de los países y las comunidades. En tercer lugar, se enfatizó la importancia de fortalecer y mejorar la educación y la creación de capacidades en relación con estas cuestiones. De acuerdo con los panelistas, estas medidas son fundamentales para promover los mecanismos y políticas nacionales de ciberseguridad.

[Grabación de la sesión](#)

IGF 2020 WS #338 Manteniéndonos unidos: Infraestructura de Internet en emergencias

Tema: Medio ambiente

Cuestiones: Impacto de las TIC en el medio ambiente / Ciudades sustentables / Ciudades inteligentes

Los panelistas abordaron la resiliencia de la infraestructura global de Internet en situaciones de emergencia. Sobre la base de las experiencias presentadas en la discusión, los oradores destacaron la importancia de las TIC en la respuesta y la mitigación de diferentes tipos de crisis y desastres.

Durante la sesión, el panel consideró la necesidad de inversiones y planes nacionales que permitan a los diferentes actores interesados estar preparados y aumentar la cooperación en situaciones de emergencia. Esos planes deberán tener en cuenta los diferentes escenarios de desastre y deberán permitir una respuesta rápida para las poblaciones afectadas. Los panelistas también destacaron la necesidad de crear una infraestructura descentralizada y resiliente para garantizar un acceso significativo y eficaz a Internet durante las crisis.

[Grabación de la sesión](#)

IGF 2020 Pre-Event #9 IGF LAC Space

La cuarta edición del IGF LAC Space reunió a 17 organizaciones y a más de 50 participantes en una sesión de intercambio regional coordinada por LACTLD. Durante este encuentro, las organizaciones compartieron los proyectos, iniciativas e investigaciones que han desarrollado en el último año y sus planes para 2021. El IGF LAC Space contó con representación del sector privado, la sociedad civil, la comunidad técnica y la academia.

Muchos de los presentadores conversaron acerca del trabajo que han desarrollado desde distintos enfoques para ampliar la inclusión digital en la región de América Latina y el Caribe.

También, las organizaciones participantes informaron acerca de los estudios, investigaciones y papers que se han producido en el último año con el objetivo de informar los procesos de toma de decisiones y el desarrollo de regulaciones en materia de Internet en la región. Los expositores de distintos sectores coincidieron en que las decisiones sobre políticas y regulaciones deben estar adecuadamente informadas con los aportes de las distintas partes interesadas. En este sentido, se advirtió sobre la aprobación de nuevas regulaciones en países de América Latina que impactan de forma negativa el desarrollo de Internet y de la economía digital en la región.

Miguel Ignacio Estrada, General Manager de LACTLD, informó a la comunidad sobre las actividades, proyectos y capacitaciones que los ccTLD de la región han estado llevando a cabo. También, compartió las últimas novedades sobre la Nube Anycast de LACTLD. Comentó que esta iniciativa ha ido creciendo con la incorporación de nuevos clientes (14 actualmente) y nodos, y con la [firma](#) de un memorando de entendimiento entre LACTLD y LAC-IX para expandir la Nube Anycast en los IXP de la región. Además, Miguel Ignacio Estrada conversó sobre el Observatorio del DNS y sobre el Foro de Contenido Ilegal de LACTLD, una iniciativa orientada a fomentar la capacitación y colaboración con los jueces, fiscales y agencias de cumplimiento de la ley de América Latina y el Caribe.

[Grabación de la sesión](#)