Miércoles 1 de agosto de 2018; 14:30-16:00 h.

Sesión 7

Desafíos en la Gestión de Identificadores de Internet

Primera sección

Fueron desarrollados cuatro temas, cada uno por un especialista, quien en 7 minutos planteó la introducción de cada tema además de sus desafíos y problemáticas en el siguiente orden: Bloqueos a sitios/redes, por Raquel Gatto (ISOC); Preparación ante desastres, por Lito Ibarra (SVNET); Privacidad bajo el enfoque de GDPR y su impacto en el DNS por Rodrigo de la Parra (ICANN); y Seguridad de enrutamiento por Guillermo Cicileo (LACNIC).

Bloqueo a sitios / redes: Raquel Gatto, ISOC

- El concepto de bloqueo en Internet es una interrupción total o parcial de las comunicaciones electrónicas, mismo que puede ocurrir en países, grupos de personas o de servicios.
- Internet Society presentó un estudio que contempla las principales técnicas para realizar bloqueos: bloqueo basado en el protocolo y en la IP, bloqueo basado en inspección profunda de paquetes (DPI), bloqueo basado en las URL, bloqueo basado en la plataforma y bloqueo basado en el DNS.
- Los bloqueos no siempre son eficientes, ya que no siempre cumplen el objetivo de interrumpir los servicios y generan efectos colaterales dañinos para el ecosistema, tanto a nivel de derechos humanos como en cuestiones económicas y en aspectos técnicos para las redes.
- Un caso emblemático fue el intento de bloqueo a WhatsApp, que no funcionó de manera eficiente y tuvo repercusiones en países de la región.

Preparación ante desastres: Lito Ibarra (SVNET)

- Durante LACIGF se han discutido diversos aspectos de la capa de usuarios, incluyendo los esfuerzos para conectar a más personas a Internet.
- No obstante, en la base de todo, la infraestructura de las redes se mantiene presente, misma que se encuentra sujeta a desastres. De tal suerte que la promoción de mayores aplicaciones y servicios basados en Internet vuelve a los usuarios más dependientes del acceso a Internet.
- Una de las cuestiones relacionadas con los desastres naturales es la protección de la infraestructura crítica que nos permite mantenernos conectados. Desafortunadamente, no todos los desastres naturales pueden predecirse.
- Los sistemas que se encuentran en riesgo son los servidores que resuelven los nombres de dominio, los puntos de intercambio de tráfico, los centros de datos, los proveedores

de conectividad locales e internacionales, así como la infraestructura diversa (cables, fibras, enlaces, enrutadores, switches...)
- A pesar de que existen diversas medidas de mitigación, algunas de estas no son adoptadas hasta que ocurre algún desastre natural.

Privacidad bajo el enfoque de GDPR y su impacto en el DNS: Rodrigo de la Parra (ICANN)
- Las medidas de privacidad y protección de datos de la Unión Europea han formado parte de las discusiones de la comunidad de ICANN desde hace tiempo. En esta ocasión, el tema se toca en el contexto de sus implicaciones para la gobernanza de Internet.
- La GDPR fue emitida por la Unión Europea y entró en vigor el 25 de mayo de 2018; es aplicable a empresas que procesan datos personales de sujetos que residen en la Unión Europea. Su incumplimiento implica multas de grandes montos.
- La GDPR afecta al Sistema de Nombres de Dominio en al menos dos áreas:
    - En relación con las partes contratadas, ya que recopilan, muestran y procesan datos personales. Entre estos actores se encuentran los registros y registradores.
    - A nivel interno, ICANN recopila algunos datos personales y los procesa para servicios internos.
- Una de las soluciones propuestas por la comunidad de ICANN fue la Especificación Temporal, que proporciona un modelo interino unificado, de modo que las disposiciones contenidas en la GDPR sean cumplidas y al mismo tiempo se garantice el funcionamiento de servicios de registro como WHOIS.
    - Además, la comunidad de múltiples partes interesadas de ICANN se dará a la tarea de definir una política que atienda los cambios generados por la entrada en vigor de la GDPR.

Seguridad de enrutamiento: Guillermo Cicileo (LACNIC)
- El enrutamiento en Internet es uno de los pilares para su funcionamiento, con base en BGP. Sin embargo, debido a que fueron diseñados hace tiempo, hay diversas consideraciones de seguridad que no fueron tomadas en cuenta.
- Ha habido diversas propuestas para solucionar las preocupaciones relacionadas con la seguridad en el enrutamiento, como RPKI. Sin embargo, la adopción de tales medidas es aún baja, por lo que uno de las intenciones es promover su adopción entre los actores relevantes.
- También es posible adherirse al programa MANRS, a fin de aumentar las medidas de seguridad entre los proveedores de acceso a Internet.

Segunda sección:

Las problemáticas y desafíos de cada tema fueron compartidos con los asistentes a la sesión por medio de las pantallas del salón. Posteriormente, los asistentes fueron separados en cuatro grupos (cada uno con un moderador y un relator) para mantener 30 minutos de debate constructivo y abierto sobre las problemáticas, desafíos y buenas prácticas de cada tema. Los relatores por cada tema fueron: Alexandra Dans (ICANN) para el tema de Bloqueos a sitios/redes; Shernon Osepa (ISOC) para el tema de Preparación ante desastres; Gabriela Ramirez (.AR) para el tema de Privacidad bajo el enfoque de GDPR y su impacto en el DNS; y Carolina Caeiro (LACNIC) para el tema de Seguridad de enrutamiento.

Las preguntas para detonar la discusión fueron las siguientes:

Bloqueos a sitios / redes:

- ¿Qué usuarios y servicios de Internet se ven afectados por las técnicas de bloqueo de Internet?
- ¿Cuáles son los efectos en los derechos humanos, en la economía y en la estabilidad de la red más comunes?
- ¿Cuáles son los roles de los distintos actores en el proceso de bloqueos de Internet: gobiernos, usuarios, comunidad técnica, sector privado?
- ¿Cuáles son los procesos y sus características en bloqueos?

Preparación ante desastres:

- ¿Qué medidas de mitigación se pueden tomar?
- ¿Quiénes deben interesarse por la prevención de daños?
- ¿Cuál es el papel de cada parte interesada (sociedad civil, gobierno, empresa privada, academia, comunidad técnica)?
- ¿Cuáles componentes del sistema de conectividad deben ser protegidos?
- ¿De dónde deben provenir los recursos para desarrollar medidas de prevención o mitigación?
- ¿Es un trabajo a nivel nacional o internacional?
- ¿Debe incluirse este tema en Gobernanza de Internet?

Privacidad bajo el enfoque de GDPR:

- En su opinión ¿cómo debe lograrse un equilibrio entre objetivos de privacidad/protección de datos personales y objetivos de seguridad y de estabilidad operativa?
- ¿Cuáles han sido las lecciones aprendidas en torno al impacto de una regulación regional en aspectos globales de Internet?
- El Modelo de Múltiples Partes Interesadas y el reto de la reacción eficiente ante eventos externos.

Seguridad de enrutamiento:

- ¿Cuáles son los problemas que pueden afectar al usuario final si el sistema de ruteo falla?
- ¿Qué medidas existen para mitigar estos problemas?
- ¿Cómo lograr que los ISP adopten tales medidas?
    - Validación: trabajo fuerte con los NOG, IXP, etc.
    - Adopción de RPKI:
        - Capacitación de los operadores.
        - Mayor difusión en el ecosistema de Internet.
        - Adhesión a MNRS (reputación de los ISP).
    - Adopción y seguimiento de estándares por parte de los operadores.

Tercera sección:
El público fue reunido nuevamente, a fin de que los relatores compartieran los resultados de los debates en cada grupo.

Bloqueos a sitios/redes: Alexandra Dans, ICANN

- Fueron señaladas diversas razones para impulsar bloqueos, incluyendo ejemplos concretos:
    - En Uruguay se intentó ejecutar un bloqueo por razones de juego. El juego es legal en el país, pero se encuentra regulado.
    - Hubo diversos casos señalados en Venezuela, además de algunas soluciones para intentar saltar los bloqueos, incluyendo usos de DNS alternativos.
- También se discutieron las perspectivas éticas del bloqueo, resaltando que existen motivos legítimos, como la lucha en contra de la pornografía infantil.
- Surgieron algunas preguntas, incluyendo aspectos legítimos para ordenar bloqueos, particularmente en cuanto a la legitimidad de las autoridades que son competentes para ordenarlos. En caso de que tal legitimidad no exista, los bloqueos pueden ser legales pero no serían éticos.

Preparación ante desastres: Shernon Osepa, ISOC

- Una de las experiencias compartidas fue la de México, luego del terremoto de septiembre de 2017: muchos usuarios intentaron hacer uso de servicios basados en Internet, superando la capacidad de la infraestructura. Algunas opiniones sugirieron la difusión de consejos acerca de uso de Internet después de desastres.
- En el caso de Guatemala, es susceptible a desastres provocados por volcanes, por lo que la prevención y monitoreo cobra especial relevancia.
- Para Haití, la coordinación local entre los operadores y el gobierno cobró especial relevancia en casos de desastre.
- En cuanto a la prevención de daños, fue mencionada la importancia de proponer soluciones holísticas, a fin de incorporar las preocupaciones y mejores prácticas de todas las partes interesadas.
- Además, los participantes coincidieron en que la prevención y recuperación en casos de desastres es un tema importante para la comunidad de gobernanza de Internet.

Privacidad bajo el enfoque de GDPR y su impacto en el DNS: Gabriela Ramirez, .AR

- En cuanto al equilibrio entre privacidad y seguridad, los participantes señalaron que no existe un antagonismo entre tales características, por lo que la información que sea recolectada debe ser pertinente, a fin de evitar abusos en tales casos.
- También fue mencionada las diferencias entre los ccTLD y los gTLD, mismos que mantienen una relación diferente con ICANN, por lo que las obligaciones de cada actor son diferentes.
- Las legislaciones locales en materia de protección de datos fueron identificadas como un elemento importante en la discusión.
- La GDPR fue señalada como una oportunidad para que la comunidad revise sus mecanismos de recolección, tratamiento y protección de datos personales, a fin de salvaguardar los intereses de los usuarios finales.

Seguridad de enrutamiento: Carolina Caeiro, LACNIC

- Los participantes mostraron diversos ejemplos que ocurrieron en la comunidad con respecto a ataques a ruteo.
- Además, fue señalado que algunos ataques de ruteo no son percibidos por los usuarios finales.

- En cuanto a las medidas de prevención y refuerzo de seguridad en el enrutamiento, fueron señaladas algunas como RPKI y BGPsec, incluyendo aspectos concretos como la necesidad de que las conexiones de BGP incorporen contraseñas para cada enrutador.
- La iniciativa de MANRS de Internet Society fue señalada como una de las medidas de prevención para reforzar la seguridad del ruteo.
- Además resaltó la necesidad de cooperación entre los operadores no solo a nivel nacional, sino también entre países.
- La capacitación fue identificada como un elemento clave, no solamente para operadores, sino para diversos actores de la comunidad de Internet.

Relator:
Israel Rosas, Outreach Manager LAC, Internet Society