# Relatoría LACIGF 12

**Título de la sesión:** TEMA INTERSECTORIAL – SECTOR COMUNIDAD TÉCNICA: Enfoque cooperativo para afrontar retos de seguridad en Internet

**Resumen de la sesión:**

La sesión fue moderada por **Ernesto Majó (LACNIC, Uruguay)** y **Ernesto Bojórquez (LACTLD, Mexico). Ernesto Majó** comenzó con una breve introducción conceptual sobre el tema que nos convoca, empieza mencionando que el concepto de seguridad hoy en día es mucho más amplio, y llega a tomar distintas dimensiones, entre ellas la estabilidad y resiliencia de Internet, las capacidades humanas, y la infraestructura. Él cree que la dimensión humana es un factor imprescindible, al igual que la colaboración que también lo considera como un factor esencial para entender los desafíos del campo. Al mismo tiempo mostró una infografía del ecosistema de Internet para dar visibilidad a la complejidad y a los diversos actores que participan, cada uno con distintas responsabilidades. También mencionó que para lograr un Internet más seguro nuestro alcance es acotado debido a que la naturaleza de Internet se encuentra enmarcada en el concepto central de la cooperación, debemos resolver en conjunto las problemáticas y trabajar en forma mancomunada para encontrar las soluciones.

Posteriormente a la introducción se invitó al público a trabajar en cuatro grupos de trabajo, según actores participantes.

- Comunidad Técnica;
- Sociedad Civil;
- Sector Empresarial;
- Sector Gubernamental.

Cada grupo debía contribuir respondiendo a dos consignas:

- ¿Cuales son las iniciativas o protocolos para identificar los retos de seguridad?
- Llevar temas críticos y herramientas o protocolos que desarrollamos.

Después, cada grupo hice una pequeña presentación sobre el debate planteado.

En la presentación del grupo de la comunidad técnica a cargo de **Sebastián Bellagamba (Internet Society, Uruguay)**, él comentó algunos de los temas que identificaron desde su organización, entre ellos conectividad, confianza en Internet y seguridad.

Los retos asociados a estos temas, se pueden dividir en tres partes:

1. En principio lo asociado al PGP y seguridad en Internet, y cómo asegurar protocolos por default en la transferencia de paquetes para mayor seguridad;
2. Por otro lado el tema del despliegue IoT, y cómo lidiar con el desconocimiento en seguridad de redes de los fabricantes de estos productos;
3. Por último, lo que refiere a la fragmentación de Internet y su impacto, que puede resultar tanto positivo, como negativo.

Sobre el último punto en particular, Bellagamba mencionó que ISOC realizó un estudio sobre la consolidación en los segmentos de Internet, entre ellos el más discutido fue el de la capa de servicios. Hoy en día la cantidad de servicios es innumerable, dado que el costo de innovación se ve abaratado por los proveedores de nube en comparación con otras capas.

En colectivo fueron listados los desafíos que creyeran pertinentes:

- Vulnerabilidad de domínios DNS;
- Enrutamiento;
- Falta de coordinación entre comunidad técnica;
- Asegurar la integridad de la información;
- Regulación;
- MANRS (¿Como llevar nodos a instancias nacionales y regionales?);
- Imposibilidad de transabilidad de implementación de IPv4;
- Necesidad de trabajar en la creación de capacidades.

También presentaron un listado de herramientas y proyectos identificadas por la comunidad técnica para contribuir con la seguridad:

- OTA (Over The Air): la programación por aire se refiere a varios métodos para distribuir software nuevo, ajustes de configuración e incluso actualizar claves de cifrado para dispositivos como teléfonos celulares, decodificadores o equipos de comunicación de voz seguros;
- RPKI: emisión de material criptográfico que permita a los miembros de LACNIC demostrar digitalmente que poseen el derecho de uso de direcciones IPv4 e IPv6;
- CSIRTs: significa Computer Security Incident Response Team;
- BGP (Border Gateway Protocol): en telecomunicaciones, BGP es un protocolo mediante el cual se intercambia información de encaminamiento o ruteo entre sistemas autónomos.

**Andrés Sastre (ASIET, Uruguay)** hizo la presentación por el sector privado. En su grupo de trabajo fueron identificados los siguientes retos:

- Falla de mecanismos de diálogo entre público y privado;
- Altas exigencias por parte del estado;
- Falta de innovación por parte de las empresas;
- Falta de confianza y mal uso de la navegación segura;
- Falta de disponibilidad de productos en la red.

Algunas soluciones propuestas por eso grupo fueron:

- Exigencia de mínimos, por parte de la industria, en términos amplios;
- Educación digital, para contrarrestar la desconfianza.

**Julián Casasbuenas (Association for Progressive Communications - APC y Colnodo, Colombia)** presentó la discusión hecha en el grupo de trabajo de la sociedad civil. Inicialmente, identificaron algunos retos de seguridad en la sociedad civil:

1. Apropiación Digital / Educación en temas de seguridad digital y protección de sus datos: Se identifica un gran desconocimiento de la sociedad en general en temas de seguridad. Se recomienda iniciar en la educación primaria para formar desde la primera infancia en seguridad digital, invitando a la escuela en participar;

2. Incidir en políticas públicas desde sociedad civil, ser más proactivos que reactivos. Trabajo con las múltiples partes interesadas para la construcción de regulaciones y políticas públicas y que puedan ser compartidas con toda la sociedad para recibir también sus comentarios;
3. Inversión en seguridad y construcción participativa;
4. Establecer proporcionalidad en temas de seguridad y vigilancia en los países de LAC.

Algunas iniciativas propuestas por el grupo de trabajo:

1. Programas de protección en seguridad.
2. Alfabetización digital desde gobiernos y todos los sectores con mucha atención en la educación básica;
3. Programas sostenibles con continuidad;
4. Compartir experiencias y materiales, usando plataformas que integramos.

**Alejandra Erramuspe (AGESIC, Uruguay)** y **Juan Cayoja Cortez (UMSA, Bolivia)** fueron los responsables por presentar la discusión de sector gubernamental. El sector se dividió en 2 grupos. Un grupo por un lado propuso generar medidas y disposiciones legales, que permitan la formación de nuevos especialistas y se produzca una cultura de seguridad. Por el otro lado, el segundo grupo mencionó la necesidad de establecer marcos jurídicos, a partir de conocer las experiencias de distintos países.

Al finalizar las conclusiones de cada grupo, el moderador principal Ernesto Bojórquez, hizo la siguiente pregunta al público: ¿Cómo creen que los diferentes sectores podrían colaborar con enfrentar los retos planteados?

A continuación varios participantes se acercaron al micrófono para realizar su intervención. Se compartieron experiencias de países como Perú, Uruguay y Colombia. También se mencionó la importancia y la responsabilidad de los gobiernos por mantener la continuidad en las políticas públicas, más allá de los cambios de gobierno.

**Outputs y otros links relevantes:**
Sesión completa en: https://www.youtube.com/watch?v=wlipzllXLxo

**Por:** Raysa Alanes (Las De Sistemas, Argentina) y Juliana Novaes (Artículo 19, Brasil)

**Revisado por:** David Paredes Abanto (DIDEPTI SRL, Perú)

**Coordinación y edición:** Nathalia Sautchuk Patrício (NIC.br, Brasil) y Guilherme Alves (Youth Observatory, Brasil)