INSTITUTO FEDERAL DE TELECOMUNICACIONES

OFICINA DEL COMISIONADO
JAVIER JUÁREZ MOJICA
IFT/100/PLENO/OC-JJM/016/2018

Ciudad de México, a 3 de agosto de 2018.

DAVID GORRA FLOTA
SECRETARIO TÉCNICO DEL PLENO
P R E S E N T E

En cumplimiento a lo dispuesto en el artículo 23, fracción II, de la Ley Federal de Telecomunicaciones y Radiodifusión, y en el artículo 15, fracción I, del Estatuto Orgánico del Instituto Federal de Telecomunicaciones, me permito enviar para conocimiento del Pleno de este Instituto el informe sobre mi participación en el encuentro "Internet Engineering Task Force, (IEFT 102)", realizado por Internet Society (ISOC), que tuvo lugar del 14 al 20 de julio del año en curso en Montreal, Canadá.

Se anexa el informe de actividades correspondientes al evento mencionado.

Sin otro particular, reciba un cordial saludo.

1036

Instituto Federal de Telecomunicaciones
RECIBIDO
con anexo
03 AGO. 2018
AREA STP
NOMBRE Y HORA Juan 14:00 hrs.

ATENTAMENTE

JAVIER JUÁREZ MOJICA
COMISIONADO

Insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tel. (55) 5015 4000

INSTITUTO FEDERAL DE TELECOMUNICACIONES

OFICINA DEL COMISIONADO
JAVIER JUÁREZ MOJICA

Ciudad de México, a 03 de agosto de 2018.

PLENO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES
PRESENTE

Informe que presenta el Comisionado Javier Juárez Mojica, respecto a su participación en representación del Instituto Federal de Telecomunicaciones en el encuentro "Internet Engineering Task Force" en Montreal, Canadá, durante los días del 15 al 18 de julio del 2018.

A partir de la invitación realizada por la organización Internet Society (ISOC), se asistió a la Meeting Internet Engineering Task Force (IEFT 102).

La asistencia corresponde al programa de POLICYMAKERS, desarrollado por ISOC para el IETF, el cual tiene como objetivo acercar a los expertos en políticas públicas de países en desarrollo y los participantes técnicos del IETF, en un medioambiente propicio para el intercambio de información, presentación de soluciones, entre otros.

Así mismo, el programa permite a los miembros del IETF conocer las preocupaciones y prioridades en materia de Internet de los participantes que representan a los países en desarrollo.

Dicho programa se centra en acortar la brecha entre la comunidad técnica y los responsables de la formulación de las políticas públicas. Con la misión de producir documentos técnicos de alta calidad y de ingeniería relevante que influya en la forma de diseñar, usar y administrar el Internet de tal manera que su desarrollo alcance un mayor potencial.

Con ello, se busca que, en conjunto con especialistas voluntarios, operadores, investigadores y vendedores, colaboren para desarrollar y promover estándares que han soportado la evolución del Internet.

Insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tel. (55) 5015 4000

En el citado evento se dio una breve introducción al contexto histórico de cómo surgió el internet y como se ha desarrollado, incluyendo discusiones técnicas sobre los siguientes rubros:

- ✓ DNS (Domain Name System);
- ✓ BGP (Border Gateway Protocol);
- ✓ Redes Comunitarias;
- ✓ IXP;
- ✓ ENRUTAMIENTO;
- ✓ DIRECCIONAMIENTO;
- ✓ TUNNELING, entre otros.

Por otra parte, la forma de trabajar y de elaborar estándares por parte del IETF, resulta interesante, ya que se trata de un foro abierto a cualquier persona interesada, con la apertura de participación y propuesta de elaboración de documentos o recomendaciones que puedan contribuir a la mejora del funcionamiento del Internet, con tan solo suscribirse a una lista de distribución que corresponda al grupo de trabajo de su interés.

En este contexto, resulta interesante mencionar que para aprobación de los estándares no hay votaciones convencionales, se utilizan el concepto "consenso amplio", ("Rough consensus" en inglés); la mecánica consiste en que cuando el Presidente del grupo de trabajo considera que algún asunto polémico o recomendación está suficientemente discutida, somete a aprobación de los asistentes si están de acuerdo con la versión final de dicho documento, siendo dicha manifestación a través de un sonido ("MMMMHH"), mecanismo que permite a los participantes manifestarse anónimamente.

A manera de reflexión, en general se trata de un mecanismo usado en la toma de decisiones por consenso para indicar el "sentido del grupo" con respecto a un asunto en particular bajo consideración. Se ha definido como la "visión dominante" de un grupo según lo determinado por su presidente; resultando un mecanismo interesante para los Comités con los que cuenta el Instituto, brindando una apertura de manifestación con un mecanismo de confidencialidad.

Insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tel. (55) 5015 4000

Durante el encuentro, se participó en sesiones de grupos de trabajo sobre los siguientes temas:

- ✓ 6man (IPv6 Maintenance)
- ✓ ace (Authentication an Authorization for Constrained Environments
- ✓ detnet (Deterministic Networking)
- ✓ gaia (Global Access to the Internet for All Research Group
- ✓ Dnsop (Domain Name System Operations

También, en esta edición del IETF, se abordó el tema de la importancia de transitar al IPv6, sensibilizando a los asistentes sobre el inminente agotamiento de las direcciones de IPv4, así como las consecuencias negativas de no migrar a dicho protocolo. Un ejemplo interesante sucedió en Bélgica, actual líder de transición en IPv6, siendo el detonador más importante el requerimiento legal de identificar unívocamente cualquier comunicación de internet, lo cual no sería posible con el protocolo IPv4, esto fue señalado como uno de argumentos de peso para la adopción de IPv6 en aquel país.

Por ello, es importante que el IFT, continúe con la promoción del micro sitio e incluso considerar otras medidas que puedan ser adoptadas.

En países como España y Bélgica, se han creado grupos de trabajo multidisciplinarios (Task Force Groups), cuya principal finalidad es elaborar recomendaciones que coadyuven a transitar a IPv6.

El Internet de las Cosas (**IoT por sus siglas en inglés**), fue otro de los temas actuales abordados en el IETF 102, particularmente en el rubro de seguridad de estos millones de dispositivos que se conectan a través de internet.

Si consideramos que uno de los principales propósitos del IETF es el correcto funcionamiento del Internet, la seguridad en el Internet de las cosas (con dispositivos que podrían generar ataques masivos a la red), es una de las áreas de interés en este foro.

Es por ello, desde el punto de vista de los consumidores, es un tema sumamente relevante, ya que se preguntan ¿Cómo garantizar la privacidad y seguridad del IoT? En este rubro los reguladores juegan un rol central sin embargo debe de abordarse con mesura.

Lo anterior, encaminado a que los gobiernos deben observar lo que sucede en materia de IoT, sin embargo, ser prudentes y no regular algo que aún no ha terminado de surgir.

En este contexto se compartió la experiencia de Canadá, del grupo denominado "Canadian Multistakeholder Process", integrado por un grupo de participantes con el fin de desarrollar recomendaciones para un conjunto de normas y políticas para asegurar el Internet de las Cosas en Canadá.

Así mismo se compartió un documento denominado "Seguridad de la IoT para formuladores de políticas", que contiene las consideraciones clave a la hora de abordar la seguridad en materia de IoT, siendo éstas que los sistemas IoT están interconectados y son complejos; que la seguridad interna es diferente a la externa, siendo ambas sumamente importantes; que la seguridad es un proceso continuo; que es primordial investigar e informar sobre vulnerabilidades y que las plataformas son importantes jugadores en el mercado.

También se abordan los desafíos de seguridad en IoT:

- Los incentivos económicos aún no favorecen a los dispositivos de mayor seguridad.

- Los nuevos jugadores en el ecosistema de IoT pueden tener poca o nula experiencia previa en seguridad de Internet.

- Los problemas de seguridad de IoT tienen un alcance global debido a la integración de la cadena de valor en la manufacturación y comercialización de los productos y, por lo tanto, los componentes pueden estar bajo el control de diferentes actores en diferentes jurisdicciones.

- El consumidor tiene, en general, un conocimiento limitado sobre seguridad del internet.

- La dificultad al detectar incidentes de seguridad (por ejemplo, un dispositivo remoto de monitoreo de audio y video para el cuidado de bebés puede continuar funcionando bien, a pesar de haber sido vulnerado y ser parte de un *botnet* realizando ataques DDoS o haber sido modificado para transmitir sonido e imágenes a terceras partes no autorizadas).

Y las recomendaciones de política pública:

- Fomentar una cultura de seguridad entre las partes interesadas del IoT en todas las etapas del ciclo de vida del producto.

- El uso de la política pública para impulsar la seguridad en los dispositivos IoT como un diferenciador competitivo.

- Mejorar las prácticas de compras públicas para IoT.

- Fomentar la cultura de seguridad de internet en los consumidores.

- Promover un papel más importante para las asociaciones de protección al consumidor.

- Asociarse con la industria de los seguros.

- Fomentar la tecnología y soluciones neutrales de proveedores, no basarse en estándares técnicos específicos, proveedores o productos, sino centrarse en los resultados deseables como una mayor seguridad, privacidad y interoperabilidad.

Dicho documento se encuentra disponible en la siguiente liga electrónica: https://www.internetsociety.org/wp-content/uploads/2018/04/IoT-Security-for-Policymakers_20180419-EN.pdf.

En resumen, la participación en dicho evento permitió intercambiar experiencias y puntos de vista con reguladores y actores relevantes en el ámbito internacional, lo que contribuye a la adquisición de información relevante para el desarrollo de las actividades del IFT, además de fortalecer los lazos de cooperación institucional deseables para implementar las mejores prácticas internacionales.

Este informe se acompaña con el programa de actividades del evento referido.

ATENTAMENTE

JAVIER JUÁREZ MOJICA
COMISIONADO

Insurgentes sur 1143,
Col. Nochebuena, C.P. 03720
Delegación Benito Juárez,
México, D.F.
Tel. (55) 5015 4000