|  |  |  |
| --- | --- | --- |
| itu_logo | **Unión Internacional de Telecomunicaciones**  **Oficina de Normalización de las Telecomunicaciones** |  |

Ginebra, 26 de mayo de 2016

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Ref.: | | **Addéndum 1 a la**  **Carta Colectiva TSB 12/11** |  | |
| Tel.: | | +41 22 730 5858 | A: | |
| Fax:  Correo-e: | | +41 22 730 5853  [tsbsg11@itu.int](mailto:tsbsg11@itu.int) | * – A las Administraciones de los Estados Miembros de la Unión; * – A los Miembros del Sector UIT‑T; * – A los Asociados de la CE 11 del UIT-T; y * – A las Instituciones Académicas de la UIT | |
| Asunto: | **Talleres del UIT-T sobre "Seguridad del SS7" (29 de junio de 2016) y "Lucha contra la falsificación aplicando soluciones de conformidad e interoperabilidad" (28 de junio de 2016) durante la reunión de la Comisión de Estudio 11 del UIT-T  (27 de junio – 6 de julio de 2016)** | | |

Muy Señor mío/Muy Señora mía:

El presente addéndum contiene información adicional sobre eventos pertinentes organizados en la Sede de la UIT en Ginebra durante la reunión de la Comisión de Estudio 11 del 27 de junio al 6 de julio de 2016.

Cúmpleme señalar a su atención los eventos siguientes:

# 1 Taller del UIT-T sobre "[Seguridad del SS7](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx)", 29 de junio de 2016 (09.00-12.30)

Introducción

El Sistema de Señalización número 7 (SS7) es un conjunto de protocolos de señalización telefónica desarrollado por el UIT-T desde la década de 1970, que se utiliza para establecer y cortar la mayoría de las llamadas telefónicas en el mundo.

Las normas SS7 se aplican ampliamente en redes telefónicas públicas conmutadas (RTPC), muy conocidas como Recomendaciones de la serie UIT-T Q.700. Las redes inteligentes normalizadas por la UIT también están relacionadas con el SS7 (UIT-T Q.1200-Q.1699). Con el crecimiento de las telecomunicaciones móviles, la ETSI ha desarrollado los protocolos MAP y SAP, que también se basan en el SS7 y son adecuadas para redes móviles terrestres públicas (RMTP), como las redes GSM. Además, el IETF publicó una serie de RFC llamada SIGTRAN, que permite utilizar el SS7 en redes IP.

El SS7 fue concebido para ser gestionado por operadores en la inteligencia de que cualquiera que estuviera conectado a una red SS7 podía considerarse fiable. El entorno de red actual y, en particular, las interconexiones por Internet, las redes basadas en el SS7 se vuelven vulnerables y pueden ser atacadas. La prensa ha señalado vulnerabilidades y problemas de seguridad relacionados con el SS7 que permiten determinar la ubicación del usuario e interceptar las comunicaciones telefónicas. Algunos operadores también lo han confirmado.

La CE 11 del UIT-T está investigando actualmente las cuestiones de seguridad del SS7 y en este evento se tratará de determinar posibles medidas para mejorar los mecanismos de seguridad del SS7.

Objetivos

Los objetivos del taller son:

• compartir información sobre cuestiones de seguridad del SS7;

• analizar las normas actuales del SS7 y determinar las que están afectadas;

• debatir cómo mejorar la seguridad de las normas SS7;

• debatir las propuestas de mejora de la seguridad de las redes basadas en el SS7 en beneficio de usuarios y operadores;

• debatir la cooperación con otros organismos de normalización y organizaciones sobre cuestiones de seguridad del SS7.

Destinatarios

Están invitados miembros y no miembros de la UIT. Se apreciará en particular la participación de operadores, vendedores, expertos en seguridad, instituciones de investigación e instituciones académicas, organismos de normalización y otras organizaciones similares.

La lista de normas SS7 (no exhaustiva)

Recomendaciones del UIT-T

− Serie UIT-T Q.700 (MTP, SCCP, TCAP, TUP, ISUP)

− UIT-T Q.1200-Q.1699 (Redes inteligentes)

− UIT-T Q.1912.5 (Interfuncionamiento entre SIP-I e ISUP)

Especificaciones ETSI/3GPP

− 3GPP TS 09.02 (Mobile Application Part, MAP)

− 3GPP TS 09.78, 3GPP TS 29.078 (CAMEL Application Part, CAP)

IETF RFC

− RFC 4960, Stream Control Transmission Protocol (SCTP)

− RFC 5133, ISDN User Adaptation (IUA)

− RFC 4165, Message Transfer Part 2 (MTP) User Peer-to-Peer Adaptation Layer (M2PA)

− RFC 3331, Message Transfer Part 2 User Adaptation Layer (M2UA)

− RFC 4666, Message Transfer Part 3 User Adaptation Layer (M3UA)

− RFC 3868, Signalling Connection Control Part (SCCP) User Adaptation (SUA)

− RFC 3807, V5 User Adaptation (V5UA)

− RFC 4129, DPNSS/DASS2 User Adaptation (DUA)

**Sitio Web:** <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/201606/Pages/default.aspx>

## 2 Taller de la UIT sobre "[Lucha contra la falsificación aplicando soluciones de conformidad e ‎interoperabilidad](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx)", 28 de junio de 2016 (1400-1800)

Introducción

En la [Resolución 188](http://www.itu.int/pub/S-CONF-PLEN-2015/en) (Busán, 2014) de la Conferencia de Plenipotenciarios sobre la "Lucha contra la falsificación de dispositivos de telecomunicaciones/tecnologías de la información y la comunicación" se resuelve encargar a los Directores de las tres Oficinas que presten asistencia a los Estados Miembros respecto de sus inquietudes en cuanto a los dispositivos de telecomunicaciones/TIC falsificados compartiendo información a escala regional o mundial, incluyendo sistemas de evaluación de la conformidad.

Asimismo, en el taller de la UIT sobre "[Lucha contra dispositivos TIC falsificados y de baja calidad](http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx)" que se celebró en noviembre de 2014, se identificó el alcance de los problemas y los efectos negativos de la falsificación, a saber, la pérdida de impuestos, regalías y otros ingresos, la disminución de las ventas, los precios y las operaciones, la erosión de la marca, el fondo de comercio y la reputación de la marca, la reducción de los incentivos a la innovación y la inversión, la disminución de la tasa de empleo y el crecimiento económico, las perturbaciones de la red y las dificultades de compatibilidad, resultantes de la ínfima calidad de la prestación y la recepción de los servicios; y los riesgos para la salud, la seguridad y el medio ambiente.

De cara al futuro, deben tomarse medidas para luchar contra los productos TIC falsificados. Por consiguiente, la [Cuestión 8 (C8) de la CE 11 del UIT-T](http://www.itu.int/en/ITU-T/studygroups/2013-2016/11/Pages/q8.aspx) está dirigiendo actualmente estudios para determinar todas las posibles soluciones técnicas que permitan luchar contra la falsificación de dispositivos TIC. La C8 ha publicado un [informe técnico sobre dispositivos TIC falsificados‎](http://www.itu.int/pub/T-TUT-CCICT) y se han creado varios nuevos temas de trabajo, en particular un proyecto de nueva Recomendación "[Solución marco para luchar contra la falsificación de dispositivos de TIC](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)".

Asimismo, en la UIT y todo el mundo, ha habido debates sobre si los programas de conformidad e interoperabilidad podrían ser una de las soluciones técnicas para luchar contra dispositivos TIC falsificados.

Objetivos

Los objetivos del taller son:

• sensibilizar sobre los estudios realizados actualmente en la C8 de la CE 11 del UIT-T, en particular para fomentar el desarrollo de la Recomendación técnica "[Solución marco para luchar contra la falsificación de dispositivos de TIC](http://web.itu.int/ITU-T/workprog/wp_item.aspx?isn=10502)";

• determinar si los programas de conformidad e interoperabilidad pueden ayudar o no a luchar contra los dispositivos TIC falsificados;

• comprender las nuevas tendencias y los nuevos mecanismos de falsificación, alteración y/o duplicación de identificadores únicos de dispositivos TIC;

• comprender los mecanismos destinados a asegurar la gestión de la cadena de suministro (fabricación, importación, distribución y comercialización) para garantizar la trazabilidad, la seguridad y la privacidad y confianza de las personas, los productos y las redes;

• seguir sensibilizando acerca del problema de la falsificación de los dispositivos de TIC, así como de los peligros que entraña;

• recabar opiniones, propuestas e ideas de expertos de la UIT y de todo el mundo para seguir realizando estudios a este respecto en el próximo periodo de estudios.

Destinatarios

Están invitados miembros y no miembros de la UIT. Se acogerá con agrado, en particular, la participación de proveedores y fabricantes, instituciones de investigación y académicas, laboratorios, organismos reguladores, operadores, ONG, autoridades aduaneras y organismos de seguridad, organismos de normalización y de evaluación de la conformidad, y otras organizaciones similares.

**Sitio web:** <http://www.itu.int/en/ITU-T/Workshops-and-Seminars/20160628/Pages/default.aspx>

Les deseo una reunión agradable y fructífera.

Les saluda muy atentamente,‎

Chaesub Lee  
Director de la Oficina de  
Normalización de las Telecomunicaciones