**CCP.I/REC. 31 (XXXVII-20)[1]**

**DIRECTRICES Y RECOMENDACIONES DE LA UIT CONTRA EL USO DE DISPOSITIVOS ILEGALES**

La 37 Reunión del Comité Consultivo Permanente I: Telecomunicaciones/Tecnologías de la Información y la comunicación (CCP.I),

**CONSIDERANDO:**

a) Que la Comisión Interamericana de Telecomunicaciones (CITEL), reconociendo la seriedad y las repercusiones sociales del robo de terminales móviles, emitió, en el marco de la XIX Reunión del CCP.I en septiembre de 2011, la Resolución CCP.I/RES.189, «MEDIDAS REGIONALES CONTRA EL HURTO DE EQUIPOS TERMINALES MÓVILES», en las que se insta a los Estados Miembros, entre otras cosas, a que consideren incluir en sus marcos reglamentarios la prohibición de la activación y el uso de los IMEI o del número de serie electrónico del fabricante de los dispositivos reportados como robados, perdidos o de origen ilegal en las bases de datos regionales o internacionales,

b) Que a pesar de los esfuerzos y del avance realizados por los Estados Miembros a nivel interno en la lucha contra este flagelo, ha aumentado el tráfico transfronterizo ilegal de dispositivos falsificados, manipulados y robados y de sus repuestos,

c) Que las ventas y la circulación notablemente crecientes en los mercados de dispositivos de telecomunicaciones/TIC falsificados y manipulados tienen un impacto negativo en los gobiernos, fabricantes, proveedores, operadores y consumidores a través de: la pérdida de ingresos, erosión del valor de la marca/derechos de propiedad intelectual y reputación, interrupciones en la red, mala calidad del servicio (QoS) y peligro potencial para la salud y la seguridad públicas, así como los desechos electrónicos en el ambiente;

d) Que los dispositivos de telecomunicaciones/TIC falsificados y alterados pueden afectar negativamente la seguridad y privacidad de los usuarios;

e) Que el plan de trabajo y las actividades relacionadas de la CITEL, a través de la Relatoría 1.5 del CCP.I sobre conformidad, control de fraudes y dispositivos móviles ilegales o irregulares, incluye objetivos a fin de proporcionar a los Estados Miembros los marcos, las mejores prácticas y recomendaciones relacionados con las diferentes cuestiones que deben abordarse para combatir mejor estos problemas;

f) Que el UIT-T, con base en los estudios del Sector de Normalización de las Telecomunicaciones de la UIT para combatir los dispositivos falsificados de telecomunicaciones/tecnologías de la información y la comunicación, y la Resolución 97 – Lucha contra el robo de dispositivos móviles de telecomunicaciones, elaboró recomendaciones sobre estos temas a través de la Comisión de Estudio 11, Cuestión 15;

g) Que la Organización de los Estados Americanos, por medio de la AG/RES. 2935 (XLIX-O/19) *ESFUERZOS HEMISFÉRICOS PARA COMBATIR EL USO DE EQUIPOS TERMINALES MÓVILES HURTADOS, EXTRAVIADOS O ADULTERADOS*, invita a los Estados Miembros a tomar medidas contra

[1] CCP.I-TIC/doc. 5008/20 rev. 3

el uso de dispositivos robados en colaboración con la industria y al fortalecimiento de sus marcos reglamentarios.

**RECONOCIENDO:**

a) Los esfuerzos y avances realizados por los Estados Miembros, la industria (los fabricantes y operadores móviles), las fuerzas del orden, las autoridades de seguridad pública, las autoridades judiciales y otras autoridades pertinentes en el combate contra la falsificación de dispositivos, el hurto de dispositivos móviles y la alteración o duplicación de los identificadores de dispositivos TIC móviles.

b) La continuidad y el crecimiento en el uso de dispositivos falsificados, robados y alterados.

c) La necesidad de que los Estados Miembros fortalezcan el combate contra estos temas críticos de seguridad pública.

**RECOMIENDA A LOS ESTADOS MIEMBROS:**

1. Iniciar una revisión de las políticas de telecomunicaciones en el país y establecer/actualizar un marco reglamentario que incorpore las medidas necesarias que autoricen a los gobiernos a identificar y actuar contra los dispositivos móviles ilegales, falsificados y robados siguiendo las directrices y recomendaciones de la UIT.

2. Iniciar un programa de registro de dispositivos mediante la implementación de soluciones técnicas disponibles para este fin, tal como se hace referencia en la Recomendación UIT-T Q.5050 *«Solución marco para contrarrestar la falsificación de dispositivos TIC».*

3. Elaborar medidas para bloquear los dispositivos reportados como perdidos/robados en la base de datos internacional y reforzar las medidas nacionales e internacionales contra los terminales ilegales con base en la Recomendación UIT-T Q.5051 "Marco para luchar contra la utilización de dispositivos móviles robados".

4. Estudiar y divulgar el Informe Técnico UIT-T *QTR-RLB-IMEI - «Confiabilidad del identificador IMEI»* para comprender las vulnerabilidades clave de los IMEI, incluida la reprogramación de IMEI en dispositivos móviles, los desafíos para hacer que el IMEI que no sean reprogramables, los efectos de la alteración de IMEI en los usuarios móviles, propietarios de las marcas, fabricantes, proveedores de servicios, reguladores, gobiernos, las fuerzas del orden y la seguridad nacional.

5. Implementar estrategias y/o adoptar procesos para la detección y el bloqueo de dispositivos móviles con identificadores alterados o duplicados, o incluso inválidos, con base en la Recomendación UIT-T Q.5052 «*Abordaje de los dispositivos móviles con identificadores únicos duplicados*».

6. Implementar y promover soluciones técnicas para que los consumidores puedan verificar la legalidad y conformidad de sus dispositivos antes de comprarlos, según se hace referencia en la Recomendación UIT-T Q.5050 «Solución marco para contrarrestar la falsificación de dispositivos TIC» y la Recomendación UIT-T Q.5051 «Marco para luchar contra la utilización de dispositivos móviles robados».

7. Estudiar los enfoques disponibles para la autenticación de dispositivos con base en UIT-T Q.5052 «Abordaje de los dispositivos móviles con identificadores únicos duplicados», que propone mecanismos para eliminar el uso de dispositivos fraudulentos en las redes móviles.

8. Estudiar y explorar la posibilidad de implementar una plataforma técnica centralizada basada en la nube para el abordaje de los dispositivos falsificados, robados e ilegales con servicio en múltiples países, teniendo en cuenta múltiples desafíos potenciales como los aspectos técnicos, la privacidad, el control, la transferencia de datos, la jurisdicción, etc.