ITU Publicaciones
Periodo de estudios 2018-2021

Unión Internacional de Telecomunicaciones
Sector de Desarrollo

Comisión de Estudio 2 Cuestión 4

Asistencia a los países en desarrollo para la aplicación de programas de conformidad e interoperabilidad y la lucha contra la falsificación de equipos de TIC y el robo de dispositivos móviles

Informe de resultados sobre la
Cuestión 4/2 del UIT-D

Asistencia a los países en desarrollo para la aplicación de programas de conformidad e interoperabilidad y la lucha contra la falsificación de equipos de TIC y el robo de dispositivos móviles

Periodo de estudios 2018-2021

Asistencia a los países en desarrollo para la aplicación de programas de conformidad e interoperabilidad y la lucha contra la falsificación de equipos de TIC y el robo de dispositivos móviles: Informe de resultados sobre la Cuestión 4/2 del UIT-D para el periodo de estudios 2018 2021

ISBN 978-92-61-34133-6 (versión electrónica)
ISBN 978-92-61-34143-5 (versión EPUB)
ISBN 978-92-61-34153-4 (versión Mobi)

Cita recomendada: Asistencia a los países en desarrollo para la aplicación de programas de conformidad e interoperabilidad y la lucha contra la falsificación de equipos de TIC y el robo de dispositivos móviles: Informe de resultados sobre la Cuestión 4/2 del UIT-D para el periodo de estudios 2018-2021. Ginebra: Unión Internacional de Telecomunicaciones, 2021. Licencia: CC BY NC-SA 3.0 IGO.

Fotografía de la portada: Shutterstock

Agradecimientos

Las Comisiones de Estudio del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) brindan una plataforma neutral en la que expertos de gobiernos, empresas, organizaciones de telecomunicaciones e instituciones académicas de todo el mundo pueden reunirse y crear herramientas y recursos prácticos para abordar cuestiones de desarrollo. A tal efecto, las dos Comisiones de Estudio del UIT-D se encargan de elaborar Informes, Directrices y Recomendaciones partiendo de las contribuciones recibidas de los Miembros. Las Cuestiones de estudio se determinan cada cuatro años en el marco de la Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT). Los miembros de la UIT, reunidos en la CMDT-17, que se celebró en Buenos Aires en octubre de 2017, decidieron que la Comisión de Estudio 2 se ocupara de siete Cuestiones relacionadas con los "servicios y aplicaciones de las tecnologías de la información y la comunicación en pro del desarrollo sostenible" durante el periodo de estudios 2018-2021.

El presente informe se preparó en respuesta a la Cuestión 4/2: **Asistencia a los países en desarrollo para la aplicación de programas de conformidad e interoperabilidad y la lucha contra la falsificación de equipos de TIC y el robo de dispositivos móviles**, bajo la dirección y coordinación generales del equipo directivo de la Comisión de Estudio 2 del UIT-D, encabezado por el Sr. Ahmad Reza Sharafat (República Islámica del Irán), en calidad de Presidente, con el apoyo de los siguientes Vicepresidentes: Sr. Nasser Al Marzouqi (Emiratos Árabes Unidos)(dimitió en 2018); Sr. Abdelaziz Alzarooni (Emiratos Árabes Unidos); Sr. Filipe Miguel Antunes Batista (Portugal)(dimitió en 2019); Sra. Nora Abdalla Hassan Basher (Sudán); Sra. Maria Bolshakova (Federación de Rusia); Sra. Celina Delgado Castellón (Nicaragua); Sr. Yakov Gass (Federación de Rusia)(dimitió en 2020); Sr. Ananda Raj Khanal (República de Nepal); Sr. Roland Yaw Kudozia (Ghana); Sr. Tolibjon Oltinovich Mirzakulov (Uzbekistán); Sra. Alina Modan (Rumania); Sr. Henry Chukwudumeme Nkemadu (Nigeria); Sra. Ke Wang (China); y Sr. Dominique Würges (Francia).

El informe fue redactado bajo la dirección del Relator para la Cuestión 4/2, Sr. Cheikh Tidjani Oudaa (Mauritania), en colaboración con los siguientes Vicerrelatores: Sr. Ahmadou Dit Adi Cisse (Malí); Sra. Amel Khiar (Argelia); Sr. Joseph Onaya (Kenya); Sr. Brillant Harivony Rakotoratsimanjefy (Madagascar); y Sr. Serigne Abdou Lahatt Sylla (Senegal).

Merecen un agradecimiento especial los coordinadores de los capítulos por su dedicación, su apoyo y su competencia.

El presente informe se ha elaborado con el apoyo de los coordinadores de la BDT, los editores, el equipo de producción de publicaciones y la secretaría de las Comisiones de Estudio del UIT-D.

Índice

Lista de cuadros y figuras

Cuadros

Figuras

Resumen ejecutivo

Dependencia y confianza mundial en los dispositivos de TIC

Los dispositivos de tecnologías de la información y la comunicación (TIC) son las puertas de acceso esenciales al mundo digital. La coordinación y el cumplimiento de las normas a escala mundial son indispensables para garantizar la interoperabilidad de las redes y la interconexión de usuarios y máquinas.

La implementación de programas de conformidad e interoperabilidad (C+I) y de técnicas avanzadas para combatir la proliferación de equipos de TIC falsificados y el robo de dispositivos móviles avanza en todos los países, aunque algunos progresan más rápidamente que otros.

El Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) ha estado ayudando a los Estados Miembros a evaluar los problemas técnicos y económicos relacionados con la necesidad de garantizar la conformidad e interoperabilidad de los dispositivos de TIC, centrándose en la asistencia, la capacitación y el intercambio de prácticas óptimas de los Estados Miembros de la UIT. El UIT-D ha colaborado estrechamente en estos asuntos con el Sector de Radiocomunicaciones de la UIT (UIT-R) y el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) con el fin de crear sinergias en estos esfuerzos y de lograr así una mayor repercusión.

Además, en una sociedad cada vez más conectada a través de dispositivos de TIC, el uso de los marcos de C+I sigue siendo un tema importante ampliamente debatido por creadores, fabricantes, importadores, operadores y usuarios. El papel de los organismos reguladores a este respecto resulta fundamental para lograr un equilibrio de los niveles de seguridad y control necesarios.

Por último, otra cuestión importante para el futuro de la C+I es la aparición de nuevas tecnologías en todos los sectores impulsadas por la Internet de las Cosas (IoT), y las normas que deben tenerse en cuenta cuando los países en desarrollo están implementando o revisando los marcos de C+I.

En este contexto, en el presente informe se analizan las prácticas más idóneas para lograr soluciones óptimas.

Trabajo de fondo en el ámbito de la C+I

Durante los anteriores periodos de estudio, la UIT se centró en la importante cuestión de la asistencia en materia de conformidad e interoperabilidad para los países en desarrollo. Se obtuvieron varios productos finales importantes que siguen siendo pertinentes para el trabajo del UIT-D en relación con la Cuestión 4/2. El anterior informe sobre la Cuestión 4/2 puede consultarse en la dirección https://www.itu.int/pub/D-STG-SG02.04.1-2017 y las actividades adicionales de la UIT-D para la prestación de asistencia a los países en desarrollo, como la base de datos del marco nacional y regional de C+I, las evaluaciones regionales y los eventos de capacitación, pueden consultarse en https://itu.int/go/CI_Development.

Capítulo 1 – Productos de tecnologías de la información y la comunicación que permiten el logro de los Objetivos de Desarrollo Sostenible

1.1 Importancia de los productos de TIC para la sociedad

La transformación digital está permitiendo un cambio rápido en todas las industrias y en todos los aspectos de nuestras vidas. Las tres fuerzas fundamentales de las tecnologías de la Información y la Comunicación (TIC), la movilidad, la banda ancha y la nube están reconfigurando las cadenas de valor, se están digitalizando los modelos de negocio y se están superando las distancias. Así está apareciendo una nueva economía de servicios en la que cada vez más las personas pueden, por ejemplo, compartir bienes y servicios en lugar de comprarlos y poseerlos; una ilustración de cómo la era digital está permitiendo nuevos modelos de negocio innovadores y cambiando las vidas[1].

Los principales beneficios de las TIC son un incremento del acceso, la conectividad y las eficiencias para las personas, las comunidades y las economías[2]:

- *Acceso* a la información y a los servicios: Gracias a los dispositivos e infraestructuras de TIC y al uso de tecnologías como los teléfonos móviles, las redes de telecomunicaciones celulares (como 3G y LTE), Internet y la banda ancha, las TIC pueden mejorar el acceso universal a la información y a los servicios para las personas de todo el mundo, en zonas tanto rurales como urbanas.
- *Conectividad* entre individuos y organizaciones: La conectividad instantánea o casi instantánea entre individuos, organizaciones y redes puede aumentar la productividad y la innovación en múltiples sectores y comunidades, y facilitar la comunicación en tiempo real necesaria para la rápida ampliación de servicios esenciales.
- *Aumento de la eficacia* gracias a la mejora de la productividad y la eficiencia de los recursos.
- *Adopción* de normas ecológicas mediante la conformidad para reducir eficazmente el cambio climático.
- *Capacidad* de las TIC para desbloquear y aprovechar las *ganancias de productividad* al mejorar el acceso a la información y la comunicación entre las personas (reduciendo así los recursos desperdiciados en desplazamientos y en la recogida manual de datos) y al proporcionar la infraestructura necesaria para la recogida y el análisis de grandes conjuntos de datos (macrodatos).

---

1 Como afirma Hans Vestberg, Presidente y Director General de Ericsson en su prefacio a ICT & SDGs – Final Report: How Information and communications technology can accelerate action on the Sustainable Development Goals. The Earth Institute, Columbia University, and Ericsson.

2 Huawei. 2017 ICT Sustainable Development Goals Benchmark. Huawei, 2017.

1.2 Dispositivos de TIC: Elementos de referencia para la columna vertebral de la economía social

Es necesario un marco estratégico con el fin de aplicar políticas coherentes y reforzar las iniciativas de desarrollo basadas en las TIC. Las TIC deben integrarse en todos los aspectos de la política pública y la actividad económica. Para lograrlo, será necesario:

- Formular políticas públicas y normativas que permitan el pleno aprovechamiento de las TIC.
- Ampliar y actualizar rápidamente la infraestructura de las TIC.
- Promover las asociaciones público-privadas para incubar empresas de TIC de nueva creación que proporcionen servicios apropiados a nivel local.
- Resolver los problemas de interoperabilidad de las TIC.
- Desarrollar la capacidad para gestionar los sistemas de TIC.
- Velar por que la política y la reglamentación se adapten a la rápida innovación e implantación de las TIC.

1.3 Conectar y proteger a los usuarios de las TIC y las redes mediante la conformidad con normas reconocidas

La inversión en infraestructura e innovación es un motor fundamental del crecimiento económico y el desarrollo. El progreso tecnológico también es clave para encontrar soluciones duraderas a los retos económicos y medioambientales, como la creación de empleo y el fomento de la eficiencia energética. El fomento de las industrias sostenibles y la inversión en investigación científica e innovación son formas importantes de facilitar el desarrollo sostenible[3].

ODS 9: Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación

Metas:

9.1 – Desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, incluidas infraestructuras regionales y transfronterizas, para apoyar el desarrollo económico y el bienestar humano, haciendo especial hincapié en el acceso asequible y equitativo para todos.

9.a – Facilitar el desarrollo de infraestructuras sostenibles y resilientes en los países en desarrollo mediante un mayor apoyo financiero, tecnológico y técnico a los países africanos, los países menos adelantados, los países en desarrollo sin litoral y los pequeños Estados insulares en desarrollo.

9.b – Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo, incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas.

9.c – Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

[3] Programa de las Naciones Unidas para el Desarrollo (PNUD). Objetivos de Desarrollo Sostenible. ODS 9: Industria, innovación e infraestructura.

Para proteger a los usuarios y redes de TIC, tenemos que centrarnos en:

- Calidad.
- Seguridad.
- Interoperabilidad.
- Entorno del espectro libre de interferencias.
- Normativa nacional.
- Sostenibilidad.
- Fiabilidad.
- Resiliencia.
- Asequibilidad (a través de las economías de escala promovidas por la conformidad y la interoperabilidad, o C+I).

Para ello, debemos tener en consideración las cuestiones relacionadas con los equipos y sistemas de TIC, que incluirían:

- Requisitos y normas técnicos.
- Evaluación de la conformidad.
- Control de los equipos.
- Seguimiento posterior del mercado.
- Promoción de los acuerdos de reconocimiento mutuo.

Por consiguiente, se requieren **métodos innovadores** para evaluar la C+I, que incluirían:

- Laboratorios de prueba nuevos o compartidos.
- Servicios de laboratorio virtual.
- Acuerdos de reconocimiento mutuo (ARM) que reflejen los requisitos y las limitaciones locales y regionales.
- Seguimiento posterior del mercado.
- Soluciones de pruebas inteligentes.
- Armonización de la normativa.

Tareas:

- Sensibilización.
- Establecimiento de una plataforma de creación de contactos sobre C+I para los miembros del UIT-D.
- Promoción de la colaboración, la investigación y el intercambio de experiencias sobre los diversos aspectos abarcados por la Cuestión.
- Representación de los miembros del UIT-D en otros foros que tratan de la C+I (por ejemplo, las reuniones del grupo ISO/CASCO STAR).
- Elaboración de un cuestionario para recopilar informes por países y realizar el seguimiento de los avances obtenidos en materia de C+I.
- Formulación de directrices.
- Publicación de recomendaciones.

1.4 Repercusión de la pandemia de la COVID-19 sobre los tipos de procedimientos de aprobación

La pandemia de la COVID-19 ha tenido –y sigue teniendo– repercusiones importantes en el comercio internacional y en la evaluación de la conformidad de los productos, incluidos los dispositivos de TIC. Las actividades de homologación se han visto gravemente afectadas por el cierre de fronteras y las dificultades de acceso a las instalaciones (como los laboratorios para la realización de pruebas físicas y los expertos sobre el terreno). Esto ha dado lugar a la necesidad de encontrar formas innovadoras de certificar la conformidad y la calidad de los productos. Los organismos reguladores, los fabricantes y los operadores han estado desarrollando soluciones ad hoc para mantener las empresas en funcionamiento y evitar las interrupciones de la cadena comercial. Ha llegado el momento de aprovechar el potencial de las tecnologías digitales para ofrecer soluciones de evaluación de la conformidad.

Capítulo 2 – Conformidad e interoperabilidad

2.1 Introducción

La evaluación de la conformidad garantiza que los equipos de TIC cumplen las especificaciones técnicas y las normas. La conformidad ayuda a vendedores y usuarios a evaluar cómo funcionará el equipo cuando se integre en una red con otros dispositivos para proporcionar un servicio de red. Las pruebas de interoperabilidad miden si dos o más productos implementan correctamente las especificaciones técnicas necesarias para garantizar una integración satisfactoria compatible con determinados protocolos de comunicación.

Las pruebas de C+I son importantes para determinar las características de los equipos de una red de TIC que podrían no cumplir con las normas reconocidas del sector y, por tanto, afectar a la calidad del servicio de red prestado. La disponibilidad de productos avanzados de alta calidad para uso comercial contribuye al despliegue generalizado de las tecnologías de red y los servicios de red asociados.

2.2 Examen de las cuestiones/prioridades esenciales en distintos países y regiones

Los problemas en el ámbito de la C+I son debidos a diferentes preocupaciones y dificultades que incluyen, entre otras[4]:

- comportamiento de los servicios de señalización de la red inteligente existente (problemas de interoperabilidad) cuando se sustituyen equipos, señalización en redes móviles (acceso, núcleo, SMS);
- falta de conformidad e interoperabilidad entre equipos de varios fabricantes;
- interfaces o protocolos no normalizados en equipos de fabricantes distintos;
- diferentes revisiones de software en equipos de un mismo fabricante, lo que da lugar a un protocolo de inicio de sesión (SIP) incompatible clientes;
- conformidad de los adaptadores multimedios (STB) fabricados por diferentes fabricantes de dispositivos intermedios de televisión por protocolo de Internet (TVIP);
- ancho de banda, y más concretamente capacidad de trasmisión de voz, datos y vídeo cuando los usuarios sobrecargan el tráfico en las redes existentes;
- logro de la interoperabilidad en redes complejas mediante la integración de redes y dispositivos;
- servicios ofrecidos por algunos proveedores que no proporcionan la infraestructura y los equipos de apoyo para permitir la interoperabilidad con otros operadores;
- metodología para la adopción de normas;
- gestión de los CDR para la facturación;
- implantación de nuevas funcionalidades y servicios en todas las plataformas;

[4] UIT-D. Informe Final sobre la Cuestión 4/2 de la Comisión de Estudio 2 del UIT-D para el periodo de estudios 2014-2017. Asistencia a los países en desarrollo para la ejecución de programas de compatibilidad e interoperatividad. UIT, 2017.

- existencia de diferentes modelos de cobro;
- nueva tecnología no interoperable con los equipos existentes;
- falta de instalaciones y centros de prueba;
- falta de personal formado para realizar tareas de C+I;
- problemas de soporte de la RDSI;
- problemas de los terminales de usuario con diferentes sistemas;
- problemas de Interoperabilidad entre los servicios y los equipos terminales que utilizan los clientes;
- vendedores que utilizan interfaces patentadas y no normalizadas;
- costos;
- la falta de capacidad humana y de oportunidades de formación;
- sistemas institucionales débiles;
- falta de sensibilización respecto de la normalización;
- desafíos de interoperabilidad.

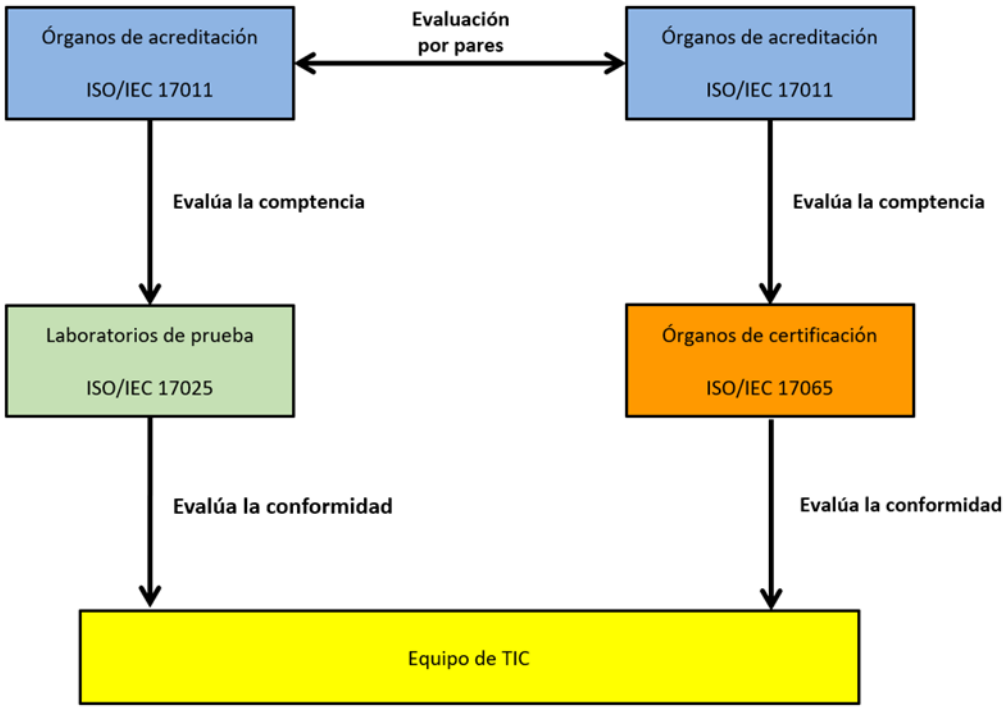
Actividades de evaluación de la conformidad

Las actividades de evaluación de la conformidad incluyen:

- designación/reconocimiento de los órganos de acreditación;
- designación/reconocimiento de los órganos de certificación;
- designación/reconocimiento de los laboratorios de prueba;
- inscripción/certificación.

En la **Figura 1** se muestran las actividades de evaluación de la conformidad.

Figura 1: Actividades de evaluación de la conformidad



2.3 Requisitos técnicos y normas

Los proveedores y operadores de servicios especifican las normas y los requisitos de los equipos y sistemas que utilizan para prestar servicios a sus clientes. Los organismos reguladores nacionales dictan reglamentos, normas y especificaciones para los equipos y sistemas desplegados en sus territorios. Los usuarios, los proveedores de servicios y los organismos reguladores nacionales exigen que se demuestre que los equipos y sistemas se ajustan a las normas y especificaciones adecuadas y que pueden interoperar según lo especificado.[5]

Para fomentar el desarrollo de normas, guías y recomendaciones internacionales, el Comité de Obstáculos Técnicos al Comercio (TBT) de la Organización Mundial del Comercio (OMC) estableció seis principios:[6]

- Transparencia.
- Apertura.
- Imparcialidad y consenso.
- Pertinencia y efectividad.
- Coherencia.
- La dimensión del desarrollo.

La importancia de las normas

La conformidad con las normas técnicas:

- Resulta esencial para la interoperabilidad de los equipos y las redes.
- Reduce el riesgo de dependencia exclusiva de una tecnología o un proveedor concretos.
- Garantiza el cumplimiento de los objetivos legítimos, incluidos los relativos a la seguridad y la no interferencia.
- Contribuye a la integración regional.
- Contribuye a la agregación de mercados, la competitividad y el comercio.

Nuevos procedimientos

Los nuevos procedimientos incluyen una combinación de:

- Las declaraciones de conformidad de los fabricantes, las pruebas de conformidad realizadas por empresas comerciales de pruebas y la vigilancia del mercado.
- Normas mundiales y ARM sobre normas y homologaciones entre países o entre grupos de países.

2.4 Acuerdos de reconocimiento mutuo/acuerdos de evaluación de la conformidad

2.4.1 ¿Qué es una disposición/acuerdo de reconocimiento mutuo?

Un acuerdo de reconocimiento mutuo sobre evaluación de la conformidad (en adelante ARM) es un arreglo/acuerdo voluntario (sobre procedimientos y procesos) entre las partes

[5] UIT. Establecimiento de regímes de conformidad e interfuncionamiento: Directrices completas.
[6] OMC. Comité de Obstáculos Técnicos al Comercio. Documento G/TBT/9. Noviembre de 2000.

(entidades privadas o públicas) sobre el reconocimiento de los resultados de la evaluación de la conformidad.

Un *acuerdo* de reconocimiento mutuo constituye un compromiso jurídico formal de las partes para reconocer los resultados de la evaluación de la conformidad de los equipos de telecomunicaciones. Trata de los requisitos reglamentarios y a continuación se denomina "ARM reglamentario". Este tipo de acuerdos suelen ser bilaterales, regionales o multilaterales, celebrados por dos o más gobiernos.

Un *arreglo* de reconocimiento mutuo es un arreglo voluntario entre las partes para reconocer los resultados de la evaluación de la conformidad de los equipos de telecomunicaciones. Trata de requisitos no reglamentarios y en adelante se denomina "ARM no reglamentario". Un ejemplo de arreglo de reconocimiento mutuo es el compromiso asumido por los organismos de acreditación de reconocer mutuamente los resultados de la evaluación de la conformidad por parte de los organismos de evaluación de la conformidad acreditados.

Las partes de un ARM están obligadas a poner en marcha procesos y procedimientos para aplicar el ARM en beneficio mutuo. Esto se aplica tanto a los ARM reglamentarios como a los ARM no reglamentarios.

Un ARM no socava la autoridad reguladora dentro de la jurisdicción de las partes del acuerdo/arreglo. El ARM debe especificar los distintos organismos que participan en su aplicación:

- *Parte*: Entidad que ha aceptado participar en el ARM.
- *Autoridad de designación*: Autoridad gubernamental u organismo competente reconocido nombrado por la parte con el fin de designar un organismo de evaluación de la conformidad para evaluar la conformidad en virtud del ARM.
- *Organismo de acreditación*: Organismo encargado de evaluar y reconocer las competencias específicas de los laboratorios de prueba y/o de los organismos de certificación de acuerdo con las normas internacionales.
- *Organismo de evaluación de la conformidad*: Organismo designado para evaluar la conformidad con los requisitos de telecomunicaciones de otra parte en virtud del ARM (puede ser un tercero o un laboratorio de pruebas del proveedor o un organismo de certificación).
- *Comisión mixta*: Comisión creada por las partes con el fin de gestionar la redacción e implementación del ARM, realizar los ajustes que sean necesarios y tratar cualquier otro asunto relacionado con el buen funcionamiento del ARM, incluyendo futuros cambios y ajustes.
- *Autoridad reguladora*: Entidad con autoridad legal responsable de las telecomunicaciones.

2.4.2 Papel de los ARM en el régimen de C+I

Los ARM sirven para:

- Reconocer la competencia de terceros para llevar a cabo los procesos nacionales de reglamentación y homologación.
- Evitar el coste de la realización de pruebas por duplicado y fomentar la transparencia.
- Facilitar el acceso a los mercados extranjeros.
- Recortar el tiempo de acceso al mercado y los costes de producción.
- Combatir las prácticas predatorias y los obstáculos a la entrada en el mercado.
- Racionalizar los procedimientos y métodos, y así reducir considerablemente los costes de los productores que venden en múltiples mercados.

Objetivo final: "una prueba, hecha una vez, válida en todo el mundo".

2.5 Infraestructura virtual[7]

2.5.1 Pruebas virtuales

En el sector de las TIC, los servicios se prestan cada vez más de forma virtual, a través de Internet. Esta nueva realidad también se aplica a nuevos mecanismos de evaluación de la conectividad de los equipos de TIC por las redes IP y está alineada con los requisitos de las nuevas redes convergentes.

Los laboratorios virtuales pueden ofrecer servicios de pruebas oportunos, asequibles y sostenibles a los países en desarrollo que carecen de capacidades para realizar pruebas propias.

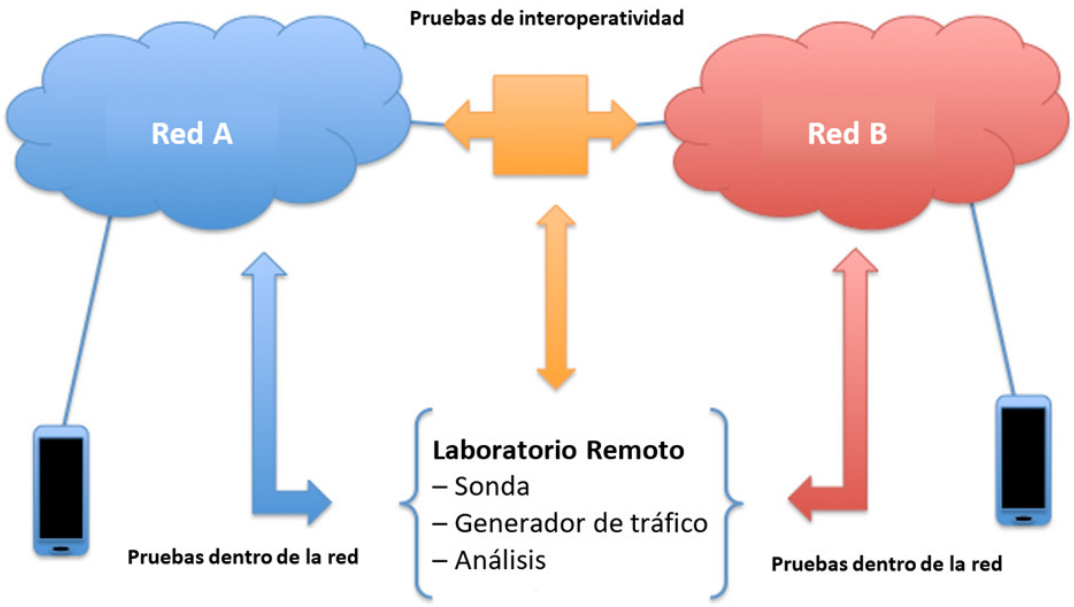
A continuación se presentan dos soluciones de pruebas virtuales: las pruebas de interoperabilidad a distancia y las pruebas de homologación a distancia.

2.5.2 Pruebas de interoperabilidad a distancia

Objetivo: *Evaluar la interoperabilidad de las redes de operadores en diferentes países/regiones*

La experiencia en todo el mundo ha confirmado la necesidad de procedimientos de realización de pruebas y de certificación normalizados de los productos y sistemas basados en las TIC para evitar numerosos problemas que afectan al usuario y a los operadores.

Figura 2: Pruebas de interoperabilidad a distancia



La falta de interoperabilidad puede causar una multitud de problemas, entre ellos:

- reducción de la velocidad de comunicación;

[7] UIT-D. Informe Final sobre la Cuestión 4/2 de la Comisión de Estudio 2 del UIT-D para el periodo de estudios 2014-2017. Op. cit.

- baja fiabilidad de la comunicación;
- acortamiento de la vida útil de los dispositivos y equipos;
- alto consumo de energía;
- interferencia de un servicio sobre otro (especialmente en los sistemas inalámbricos);
- equipos de baja calidad, que dificultan la evolución y la compatibilidad con las nuevas tecnologías y protocolos;
- incompatibilidades de los equipos que provocan atascos en las comunicaciones (a menudo muy difíciles de diagnosticar);
- fluctuaciones en la calidad de funcionamiento de la red debido a la falta de procedimientos para controlar los cambios en los equipos y el software;
- problemas en la interconexión de equipos de diferentes fabricantes y entre redes de diferentes países.

Los objetivos concretos de las pruebas a distancia pueden ser: el desarrollo de productos, la certificación de la autoridad reguladora, las pruebas de preconformidad e interoperabilidad de los productos de TIC, la evaluación de la conformidad de los dispositivos móviles y los protocolos IP, y el servicio sobre el terreno.

Destinatarios: operadores de telecomunicaciones, fabricantes y usuarios de equipos (diversidad de necesidades – clientes, operadores, asociaciones, organismos reguladores, etc.).

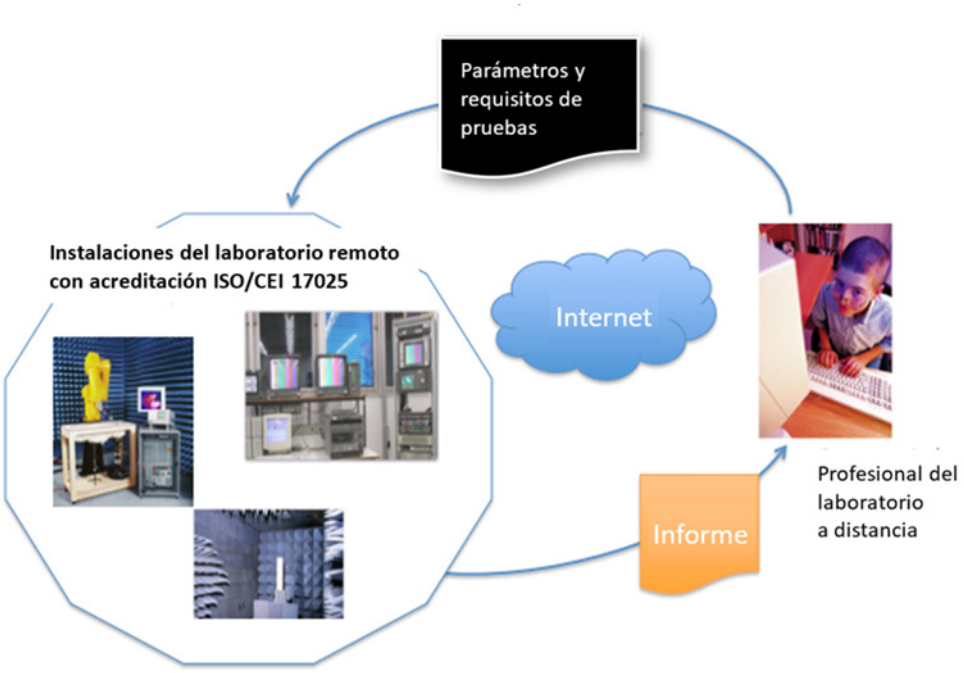
Es deseable una cooperación estrecha y fuerte con los grandes fabricantes de sistemas de pruebas y medidas, para garantizar una actualización rápida de la infraestructura cuando sea necesario.

2.5.3 Pruebas de homologación a distancia

Objetivo: *Proporcionar acceso a la infraestructura física de pruebas a distancia para la homologación*

Las pruebas de homologación a distancia permiten el desarrollo en laboratorio, y las pruebas de preconformidad, de conformidad y de interoperabilidad de muestras de productos de TIC por medios remotos o virtuales utilizando la infraestructura de otros laboratorios. Las muestras serán suministradas por otras entidades (participación comunitaria).

Figura 3: Pruebas de homologación a distancia



El nivel de los servicios de laboratorio prestados puede adaptarse a través de varias fases:

- Fase 1: Formación a distancia.
- Fase 2: Realización de pruebas en las muestras con transmisión de vídeo de cada paso y envío de datos para la composición de informes.
- Fase 3: El laboratorio local participa cada vez más en las pruebas de ciertos tipos de productos, en particular los productos de la red central (para lograr el máximo beneficio en cuanto a las necesidades de la infraestructura central).
- Fase 4: Se facilita infraestructura para la realización de pruebas a distancia (inversión en una infraestructura adecuada de medición de pruebas).
- Fase 5: Consultoría y formación para pasar a la adquisición de una infraestructura de pruebas local (si se considera oportuno).

Requisitos: normas aplicables, realización de pruebas, filtrado, etc.

2.6 Vigilancia del mercado

El objetivo de la vigilancia del mercado sobre los equipos de telecomunicaciones desplegados es garantizar que los productos introducidos en el mercado no causen interferencias electromagnéticas, dañen la red pública de telecomunicaciones, pongan en peligro la salud o la seguridad pública o perjudiquen el interés público de cualquier otro modo. En la práctica, la vigilancia del mercado abarca todas las medidas (incluidas la prohibición, la retirada o la recuperación) necesarias para detener la circulación de los productos que no cumplen los requisitos establecidos en la legislación y la normativa pertinentes, garantizar la conformidad de los productos e imponer sanciones. La vigilancia del mercado es fundamental para el buen funcionamiento del mercado de las telecomunicaciones. Es esencial para proteger al consumidor y al trabajador contra los riesgos que presentan los productos no conformes. Además, la vigilancia del mercado ayuda a proteger a las empresas responsables contra la competencia desleal de operadores económicos sin escrúpulos que hacen caso omiso de las normas o ahorran en calidad. Muchos organismos reguladores del mundo cuentan con

prescripciones jurídicas específicas relativas a la organización de la vigilancia del mercado. Los reglamentos suelen establecer las obligaciones claras para las autoridades de vigilancia del mercado y estipulan que deben tener las potestades, recursos y conocimientos necesarios para desempeñar adecuadamente sus funciones. Deben establecerse procedimientos para el seguimiento de las reclamaciones, el seguimiento de los accidentes, la comprobación de la adopción de medidas correctoras y la recopilación de conocimientos científicos y técnicos relacionados con las cuestiones de seguridad.

2.6.1 Principales partes interesadas

Las principales partes interesadas son:

- Gobiernos/organismos reguladores.
- Organismos de acreditación (AB).
- Organismos de evaluación de la conformidad (CAB).
- Fabricantes, importadores, vendedores y proveedores de servicios.

2.6.2 Consultas sobre inteligencia y experiencia en la vigilancia del mercado

Las actividades incluyen:

- Compartir información y consultar con otros países que han establecido programas de vigilancia del mercado y de observancia de la ley, en particular dentro de la región, donde existe un lenguaje común y quizás una gestión del espectro y una asignación de frecuencias comunes para los servicios.
- Enviar avisos o advertencias previas a los socios en relación con los problemas de conformidad de las tecnologías y los productos que puedan desplegarse en una fase temprana en un país o región concretos, alertando a los socios de posibles problemas de conformidad cuando los productos o las tecnologías se desplieguen de forma más amplia y permitiendo orientar los esfuerzos de inspección y auditoría con mayor precisión.

2.7 Evaluación de la conformidad de las nuevas tecnologías

Si no se preparan a tiempo, la conformidad y la interoperabilidad supondrán un grave problema para los países en desarrollo, ya que los servicios y las aplicaciones de las TIC se utilizan en todos los aspectos de la vida de las personas y la proliferación de las nuevas tecnologías (IoT, 5G, etc.) es una realidad.

El escenario previsto donde todas las cosas están conectadas está creando una mayor demanda de C+I. Los países en desarrollo están buscando maneras innovadoras de resolver las diferentes necesidades que aparecen, por ejemplo:

- Estableciendo requisitos técnicos comunes.
- Definiendo las referencias técnicas principales (normas) a nivel internacional.
- Elaborando políticas para unos marcos de C+I sólidos que fomenten la colaboración en un entorno de TIC de múltiples partes interesadas (es decir, mediante la creación de mecanismos como la aceptación de las declaraciones de proveedores y los acuerdos de reconocimiento mutuo).

2.7.1 Nuevos desafíos tecnológicos

Estos desafíos incluyen:

- Repercusiones de los problemas de interoperabilidad en los esfuerzos de ampliación:
  - sensibilización a escala del organismo regulador;
  - precepción de la reglamentación como barrera de entrada.
- Sensibilización y percepción de la C+I por parte de los conceptores:
  - coste monetario;
  - coste humano y de seguridad.
- Financiación y recursos limitados para los proyectos/productos:
  - costes de certificación;
  - los mercados aún se encuentran en una fase inicial.

2.7.2 Pruebas de preconformidad

La realización de pruebas de preconformidad requiere:

- Conocimiento de la C+I:
  - pertinente para el diseño de producto concreto;
  - en cada fase del recorrido de un producto hasta el mercado.
- Sensibilización respecto de los efectos de la C+I:
  - apreciación de los costes (monetarios, de tiempo, técnicos) para una empresa de nueva creación;
  - la reglamentación como una ventaja y no como un obstáculo.

2.7.3 Repercusiones esperadas[8]

La C+I puede mejorar las perspectivas de éxito al:

- facilitar una mezcla de productos inteligente;
- incorporar la C+I desde el principio;
- conocer qué personas y qué recursos se necesitarán, y cuándo.

Puede ayudar a los organismos reguladores a propiciar la aparición de productos y empresas al:

- propiciar los ARM transversales;
- promover una participación informada de los empresarios.

[8] UIT. Sesión temática para la Cuestión 4/2. 16 de octubre de 2019.

Capítulo 3 – Lucha contra la proliferación de dispositivos falsificados, de baja calidad y manipulados

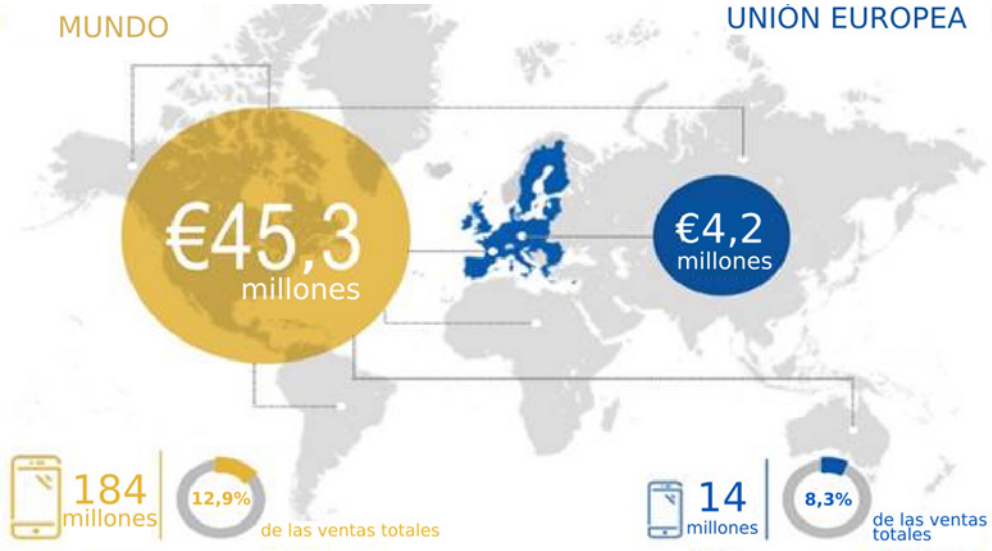
En la actualidad, el mercado de las TIC y el comercio de dispositivos móviles falsificados es un problema socioeconómico mundial con repercusiones negativas para la innovación, la inversión, el crecimiento económico, la salud y el empleo. También existe el peligro de que los recursos se desvíen a la delincuencia organizada.

La Conferencia Mundial de Desarrollo de las Telecomunicaciones de 2017 (CMDT-17), en su Resolución 79 (Rev. Buenos Aires, 2017), identificó la lucha contra la proliferación de equipos y dispositivos falsificados como una prioridad en el marco de la Cuestión 4/2. En este capítulo se describen los problemas causados por los dispositivos de telecomunicaciones/TIC falsificados y se ofrecen directrices para identificar y combatir su uso.

3.1 Problemas y cuestiones

La falsificación de equipos de telecomunicaciones/TIC, en especial de teléfonos móviles, constituye un desafío para los usuarios, fabricantes y gobiernos de todo el mundo, y también para la innovación, la inversión y el crecimiento económico. Según los cálculos de la Oficina de Propiedad Intelectual de la Unión Europea (EUIPO), las pérdidas de ingresos en concepto de ventas de teléfonos inteligentes ascendieron a 45 300 millones de euros en 2015.[9]

Figura 4: Pérdida de ventas debida a los teléfonos inteligentes falsificados: UE y mundo



[9] EUIPO. Study on fake smartphones. Octubre de 2018.

Por parte de los usuarios, los incentivos que impulsan la proliferación de terminales falsificados incluyen:

- los dispositivos falsificados y manipulados pueden ser más asequibles que los auténticos y ofrecer acceso a las redes;
- estos dispositivos ofrecen a los usuarios funcionalidades interesantes tales como múltiples tarjetas SIM, televisión, radio FM y varios servicios de Internet móvil (chat, videollamadas, navegación por la web, transferencias de dinero, etc.) a un bajo coste.

El impacto negativo de los terminales falsificados sobre la salud humana, sobre la calidad de las redes y servicios y las finanzas se debe a una serie de factores, entre los que se encuentran los siguientes (lista no exhaustiva):

- dispositivos poco fiables que suponen una amenaza para la salud y el medio ambiente debido a sus componentes peligrosos (por ejemplo, plomo o cadmio), a su elevada tasa de absorción específica (SAR) o a sus baterías, que entrañan un riesgo de explosión;
- degradación de la calidad del servicio (QoS), incluyendo problemas de accesibilidad de voz, caída de llamadas, problemas de movilidad (traspaso) y menor velocidad;
- pérdidas financieras para los fabricantes de terminales auténticos (pérdida de ventas, impacto negativo en el precio);
- pérdidas fiscales (ingresos aduaneros e impuestos);
- violaciones de los derechos de autor y de las patentes, competencia desleal;
- pérdida de garantía y soporte técnico;
- interrupciones en la calidad de funcionamiento de la red de telecomunicaciones, como por ejemplo la pérdida de control sobre la potencia.

En cuanto al rendimiento de la red, un informe de Qualcomm[10] demostró las repercusiones negativas que entrañan los equipos falsificados para las redes:

- reducción de la capacidad de la red: La capacidad de datos de la evolución a largo plazo (LTE) se ha reducido en un 23 por ciento, la capacidad de datos del acceso a paquetes de alta velocidad (HSPA) en un 6 por ciento, y la capacidad de voz del sistema universal de telecomunicaciones móviles (UMTS) en un 27 por ciento;
- reducción de la compatibilidad con las funciones más recientes de LTE, como LTE-CA (agregación de portadoras), MIMO (entrada múltiple y salida múltiple) 4x4 y 256 QAM (modulación de amplitud en cuadratura), lo que repercute negativamente en la experiencia general del usuario;
- el aumento de las necesidades de cómputo de emplazamiento de la red, lo cual entraña gastos de capital y de explotación, lo que repercute negativamente en la rentabilidad para los operadores de telefonía móvil.

Entre los problemas vinculados a los dispositivos falsificados con IMEI no válida figuran los siguientes:

- Dificultades para identificar y bloquear dispositivos móviles falsificados, ya que muchos tienen códigos IMEI de aspecto legítimo. Los falsificadores suelen utilizar en sus productos rangos de números IMEI que se corresponden con los de los fabricantes de dispositivos legítimos, lo que dificulta la diferenciación entre productos legítimos y falsificados.
- Amenazas a la seguridad pública. Estos dispositivos podrían facilitar las actividades delictivas y el terrorismo.
- Los trastornos causados por el bloqueo de los dispositivos falsificados vendidos suelen penalizar a los usuarios, en lugar de a quienes comercian con productos falsos.

[10] Qualcomm. Combating mobile counterfeiting and theft. Octubre de 2018.

3.2 Definiciones

- **Terminal**: Equipo conectado a una red de telecomunicaciones para proporcionar acceso a uno o más servicios específicos (Recomendación UIT-R V.662-3).[11]
- **IMEI** (*International Mobile Equipment Identity* – Identidad internacional del equipo móvil): Código único asignado a cada terminal móvil IMT-2000 por el fabricante y utilizado para identificar al terminal IMT-2000 ante la red a efectos de validación del equipo terminal o tareas similares.
- **EIR** (*Equipment Identity Register* – Registro de identidad de equipo): Registro al que se puede asignar la identidad del equipo del usuario con fines de inscripción. La naturaleza, la finalidad y el uso de esta información es un tema que hay que seguir estudiando.
- **Lista blanca**: Registro de los dispositivos autorizados para su uso en un país (incluidos los dispositivos que se han importado o fabricado legalmente en ese país).
- **Lista negra**: Registro de dispositivos a los que se les debe denegar el servicio en la red de telecomunicaciones.

3.3 Directrices

Es importante que todas las partes interesadas (es decir, los gobiernos, los fabricantes, los operadores de redes y los consumidores) colaboren en la lucha contra la proliferación de equipos de telecomunicaciones/TIC falsificados.

Figura 5: Responsabilidad en la lucha para combatir las falsificaciones

La colaboración es fundamental para la creación de un marco normativo y técnico para luchar contra la proliferación de productos falsificados. Para ello:

- Los gobiernos y los organismos reguladores deben elaborar marcos normativos que apliquen procedimientos normalizados y desplieguen una plataforma tecnológica para hacer cumplir la normativa; organizar campañas de sensibilización, en particular sobre los riesgos para los usuarios de dispositivos falsificados, como los riesgos para la salud y la mala calidad de servicio; y promover la vigilancia del mercado para evitar el comercio en el mercado negro de dispositivos.
- Los gobiernos deberían considerar la posibilidad de reducir los impuestos y las tasas sobre los dispositivos de TIC importados legítimamente. Esto también puede reducir el coste de propiedad.
- A nivel nacional, los organismos reguladores deberían colaborar con los fabricantes y los operadores de red a fin de determinar cuál es el alcance del uso de dispositivos falsificados en el mercado local.

[11] Sector de Radiocomunicaciones de la UIT (UIT-R). Recomendación ITU-R V.662-3 (05/2000). Términos y definiciones.

- Los servicios aduaneros y de seguridad deben contar con los recursos necesarios para poder combatir el tráfico ilícito y verificar la legitimidad de los identificadores de los dispositivos en el punto de importación.
- Los fabricantes e importadores deben registrar todos los equipos importados y fabricados localmente y respetar los procedimientos de homologación establecidos por el organismo regulador.
- Los fabricantes deben mejorar la seguridad de los códigos IMEI cumpliendo con los principios de diseño técnico para la implementación de la seguridad del IMEI y participando en el proceso de la Asociación GSM (GSMA) para presentar informes y corregir las vulnerabilidades de seguridad del IMEI.
- Los operadores pueden contribuir a la lucha contra la proliferación de dispositivos falsificados: proporcionando datos de la red de dispositivos al organismo regulador y a las partes interesadas del gobierno; creando una base de datos EIR para apoyar la funcionalidad de la lista negra y la lista blanca de IMEI con el fin de denegar el acceso a los dispositivos falsificados; e informando por SMS a los abonados de la situación de sus dispositivos, si fuera necesario.
- Los clientes pueden contribuir verificando la legitimidad de los dispositivos que tienen previsto comprar remitiéndose a los servicios de verificación que ofrecen otras partes interesadas; registrando los dispositivos importados individualmente; y denunciando los dispositivos falsificados a las autoridades.
- Debe establecerse un sistema de evaluación de la conformidad, así como una base de datos centralizada a nivel nacional que contenga toda la información sobre los productos (identificadores, especificaciones técnicas, ciclos de vida de los productos, etc.) para contribuir a una vigilancia eficaz del mercado.

La experiencia de países como Rwanda (véase la sección 3.4.4) sugiere que, a nivel regional:

- Es importante celebrar acuerdos de reconocimiento mutuo entre países para la evaluación de la conformidad y la vigilancia del mercado.
- Un sistema de control centralizado de los equipos podría reducir en gran medida el número de dispositivos falsificados y de baja calidad que entran en el mercado.
- Los centros de pruebas reconocidos a nivel regional podrían ayudar notablemente a aplicar la evaluación de la conformidad mediante la certificación y las declaraciones de conformidad de los proveedores.

3.4 Experiencia nacional (estudios de caso)

Las contribuciones de los Estados Miembros y de las partes interesadas han sido fundamentales para la elaboración de este informe. Las contribuciones se basan en la experiencia nacional, los datos y las prácticas existentes en la lucha contra la proliferación de dispositivos falsificados.

Todos los que han contribuido están de acuerdo en la necesidad de establecer marcos políticos, jurídicos y reglamentarios aplicables.

Algunos contribuyentes proponen utilizar soluciones técnicas existentes, como son las normas internacionales y las técnicas de vigilancia del mercado, y crear bases de datos y plataformas centralizadas para bloquear los dispositivos falsificados.

Además, varios contribuyentes proponen ampliar los esfuerzos a nivel regional y subregional, con el fin de poner en común las diferentes técnicas de lucha contra la falsificación de dispositivos.

3.4.1 Madagascar

En Madagascar, el 25% de los dispositivos activos en las redes móviles son productos falsificados[12]. Aunque estos dispositivos aportan ciertas ventajas, por ser asequibles, ofrecer acceso a servicios universales y reducir la brecha digital, estas ventajas se ven superadas por los diversos riesgos que suponen para la salud humana (por ejemplo, niveles de emisión peligrosos), para los operadores (QoS, interferencias, etc.) y para la economía del país.

Para evitar que el desarrollo digital tenga repercusiones perjudiciales para la salud humana y la economía, Madagascar ha adoptado medidas destinadas a:

- Aumentar la sensibilización de los usuarios respecto de los peligros de los dispositivos falsificados.
- Acabar con los mercados negros y hacer cumplir las medidas aduaneras.
- Prohibir los terminales falsificados y velar por la certificación de los equipos de TIC importados.
- Utilizar una plataforma para analizar e identificar los códigos IMEI y bloquear los dispositivos falsificados a partir del 30 de junio de 2019.

3.4.2 Guinea

En la contribución del Gobierno de Guinea se hace hincapié en las inquietudes ligadas a la certificación de los equipos e infraestructuras de telecomunicaciones, así como a la interoperabilidad de los servicios de telecomunicación[13]. Desde 2015, el gobierno ha promulgado leyes de telecomunicaciones que han reestructurado el sector. Las reformas han aportado beneficios como el aumento del parque telefónico, la mejora de la calidad del servicio, el incremento de la contribución del sector al producto interior bruto y el control del mercado digital y del sector de la certificación.

El gobierno ha impuesto normas muy estrictas para la certificación de los equipos de telecomunicaciones, con contramedidas y sanciones para frenar las infracciones. El Organismo Regulador de Correos y Telecomunicaciones (ARPT) evalúa los equipos terminales para comprobar su conformidad con los requisitos básicos, solicitando documentaciones administrativas y técnicas muy detalladas antes de expedir los certificados de conformidad. Las medidas adoptadas en Guinea incluyen:

- Seguimiento riguroso y continuo de la labor de la UIT en el ámbito de la normalización.
- Intervención de varios actores, en particular: el ARPT, aduanas, autoridades fiscales, ministerios, etc.
- Aprobación de los equipos de telecomunicaciones, concedida para un período de cinco años renovable.
- Implantación práctica del sistema de etiquetado para los equipos aprobados.
- Incautación de equipos o desmantelamiento de instalaciones implicados en la falsificación, a expensas del infractor.
- Confiscación del equipo falsificado, dictada por el tribunal competente.
- Sanciones en caso de no inscripción: toda persona que posea equipos terminales o equipos radioeléctricos en el sentido de la ley con miras a su venta o distribución, gratuita u onerosa, o que venda dichos equipos, así como toda persona que conecte dichos equipos

[12] CE 2 del UIT-D, Documento 2/45 de Madagascar.
[13] CE 2 del UIT-D, Documento SG2RGQ/9(Rev.1) de Guinea.

a una red pública de telecomunicaciones/TIC infringiendo el régimen de certificación o sin autorización previa, se expone a una multa de entre 10 y 200 millones GNF.
- Duplicación de las multas en caso de reincidencia.

3.4.3 Senegal

Además de luchar eficazmente contra la piratería, la falsificación y el robo de dispositivos de telecomunicaciones/TIC, y de tomar medidas para adaptarse a los cambios en el entorno legal, el Gobierno de Senegal ha emprendido importantes iniciativas en colaboración con las comunidades continentales e intercontinentales, las multinacionales, los reguladores de telecomunicaciones y TIC y los proveedores de servicios de Internet (ISP) para luchar contra esta moderna lacra, que es un obstáculo para la innovación tecnológica, la creación de empleo y riqueza y la inversión extranjera directa[14].

Senegal ha puesto en marcha medidas de carácter legislativo y reglamentario y ha dado otros pasos para mejorar la protección de la propiedad individual, entre ellos:

- Un marco legislativo basado en una serie de leyes.
- Un marco reglamentario basado en una serie de decretos.
- La brigada nacional de lucha contra la piratería y la falsificación.
- El Organismo de la Propiedad Industrial y la Innovación Tecnológica del Senegal.
- El Organismo Regulador de Telecomunicaciones y Correos (ARTP).
- Las aduanas del Senegal.
- La participación de fabricantes y distribuidores nacionales y multinacionales de teléfonos, tabletas, teléfonos inteligentes y decodificadores.

3.4.4 Rwanda

Consciente del peligro que suponen los dispositivos falsificados para el consumidor, la industria y la economía, el Gobierno de Rwanda ha elaborado una estrategia para combatir la proliferación de dispositivos falsificados y ha establecido una hoja de ruta a nivel regional, junto con los Estados Miembros pertenecientes a la Comunidad de África Oriental (CAO)[15]. Las propuestas del gobierno incluyen:

- Acuerdos mutuos entre los Estados miembros de la CAO: Revisión de los instrumentos jurídicos y reglamentarios de los Estados miembros con vistas a la celebración de acuerdos de reconocimiento mutuo para la evaluación de la conformidad y la mejora de la vigilancia del mercado.
- Un sistema de seguimiento centralizado: Establecer un sistema de control en tiempo real basado en el bloqueo de la tarjeta SIM EIR, la preautorización del IMEI, la autorización del IMEI y la alerta EIR como el mejor enfoque para luchar contra la proliferación de dispositivos ilegales a nivel regional.
- Centros regionales de realización de pruebas: La creación de centros regionales de realización de pruebas acreditados facilitaría la evaluación de la conformidad en los Estados miembros de la CAO mediante la certificación con la declaración de conformidad del proveedor. Esto reducirá el coste de la certificación para las plantas de ensamblaje regionales y reducirá el coste del producto final. El establecimiento de acuerdos mutuos entre países facilitará la creación de laboratorios especializados en diferentes países.

[14] CE 2 del UIT-D, Documento SG2RGQ/66(Rev.1) de Senegal [en francés].
[15] CE 2 del UIT-D, Documento SG2RGQ/69 de Rwanda.

3.4.5 Zimbabwe

Todos los operadores de red móvil de Zimbabwe tienen la capacidad de detectar los dispositivos falsificados con IMEI duplicados existentes en sus redes. Sin embargo, dada la importancia de los dispositivos falsificados para los ingresos del operador – estos dispositivos representan la mayoría de los usuarios de la red –, la desconexión real es poco frecuente.[16] No obstante, en Zimbabwe se han tomado las siguientes medidas para combatir la proliferación de dispositivos falsificados y el robo de dispositivos móviles:

- Prohibición de utilizar cualquier dispositivo que no cumpla los requisitos de homologación.
- Obligación para los abonados a la red móvil de registrar las tarjetas SIM recién adquiridas en el operador de red móvil (ORM) antes de que la tarjeta pueda activarse en la red.
- Adquisición de una base de datos de registro de abonados para garantizar que todas las tarjetas SIM activadas en el país estén correctamente registradas, lo que también facilita la detección de dispositivos falsificados y teléfonos móviles falsos.
- Comprobación y certificación de todos los nuevos dispositivos de TIC a nivel regional por un laboratorio de pruebas independiente gestionado por la Autoridad Independiente de Comunicaciones de Sudáfrica (ICASA).

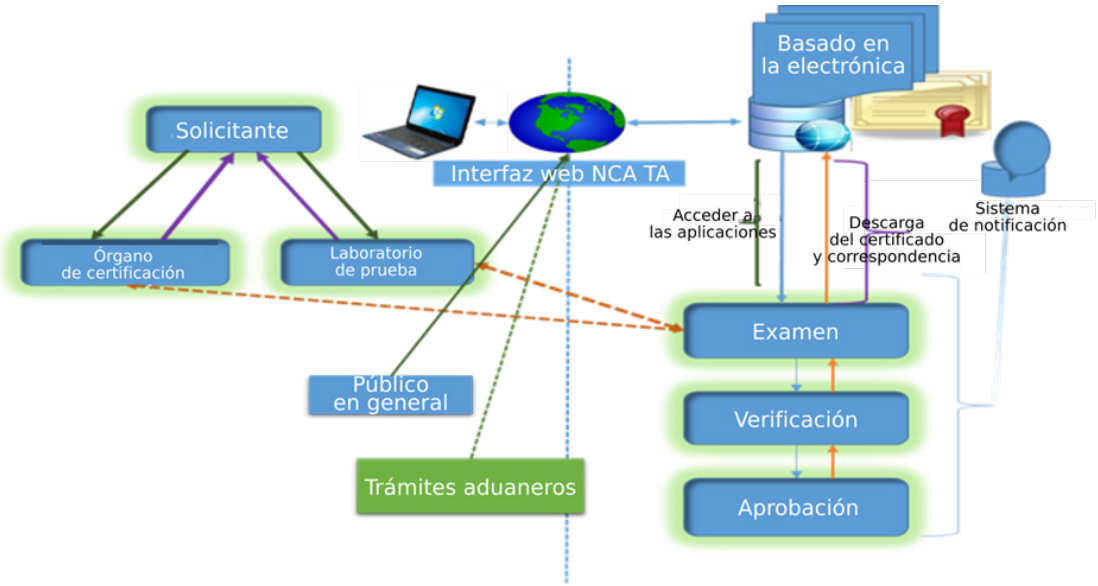
3.4.6 Ghana

En Ghana, la homologación se utiliza para proteger los dispositivos, usuarios y redes de telecomunicación/TIC.[17] Para ello, la Autoridad Nacional de Comunicaciones (NCA) ha creado un régimen de homologación para certificar y probar los equipos de comunicación con el fin de garantizar el cumplimiento de las normas internacionales:

- Aplicación de un procedimiento de homologación basado en documentación técnica que contenga informes de pruebas y requisitos de conformidad relativos a la protección de los consumidores, la protección del medio ambiente, la perturbación de la red, la integridad y la interoperabilidad, así como disposiciones para garantizar la conformidad con el Plan Nacional de Atribución de Frecuencias.
- Atribución del certificado de homologación (TAC) y de la marca NCA, con los detalles del equipo publicados en el sitio web de la NCA.
- Implantación de un sistema de concesión de licencias de venta, integrado en el régimen de homologación, para racionalizar las actividades de los concesionarios de equipos electrónicos y de comunicación y garantizar que sólo se utilicen dispositivos de TIC homologados.
- Disposiciones para fortalecer la vigilancia del mercado a escala nacional.
- Establecimiento de laboratorios de ensayo para las mediciones relativas a la tasa de absorción específica (SAR), el campo electromagnético (CEM), la televisión digital terrenal (TDT) y la radiofrecuencia y la señalización (RF&Sig).

[16] CE 2 del UIT-D, Documento SG2RGQ/85 de Zimbabwe.
[17] CE 2 del UIT-D, Documento SG2RGQ/82 de Ghana.

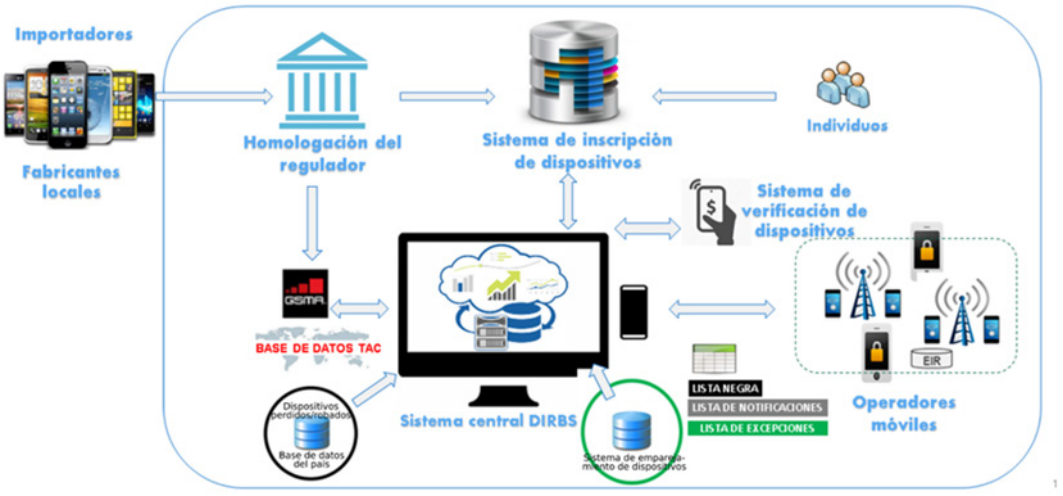
Figura 6: Proceso de homologación



3.4.7 Pakistán

La Autoridad de Telecomunicaciones del Paquistán (PTA), en colaboración con Qualcomm, ha puesto en marcha el Sistema de identificación, registro y bloqueo de dispositivos (DIRBS), una plataforma de tecnología de código abierto que permite garantizar que solo se utilizan dispositivos aprobados y legales en las redes móviles del país[18]. El DIRBS: posibilita la identificación de todos los dispositivos; capta la base instalada de los dispositivos; realiza un seguimiento de todas las activaciones de nuevos dispositivos; se ocupa de los dispositivos ilegales y falsificados; se ocupa del robo de móviles, y contempla excepciones/amnistía.

Figura 7: Sistema de identificación, registro y bloqueo de dispositivos (DIRBS)



[18] Para más información sobre el DIRBS, sírvase consultar el sitio web de la Pakistan Telecommunication Authority (PTA) y el de la Pakistan Federal Board of revenue (FBR).

3.4.8 La Asociación GSM

La GSMA mantiene la Base de Datos Internacional Mobile Equipment Identity, que es una base de datos central mundial que contiene información básica sobre el IMEI de millones de dispositivos móviles en uso en todo el mundo.[19]

La GSMA ofrece un servicio de "comprobación de dispositivos" a los comerciantes de dispositivos, a los recicladores y a las aseguradoras, así como a las fuerzas del orden (en algunos mercados, los consumidores también pueden acceder al servicio directamente). Permite a los usuarios averiguar al instante si un dispositivo ha sido denunciado como perdido o robado a través del registro del estado del dispositivo, tal y como informan a la GSMA sus miembros operadores de redes móviles de todo el mundo.

La GSMA quiere conectar al mayor número posible de ORM a la base de datos de IMEI.

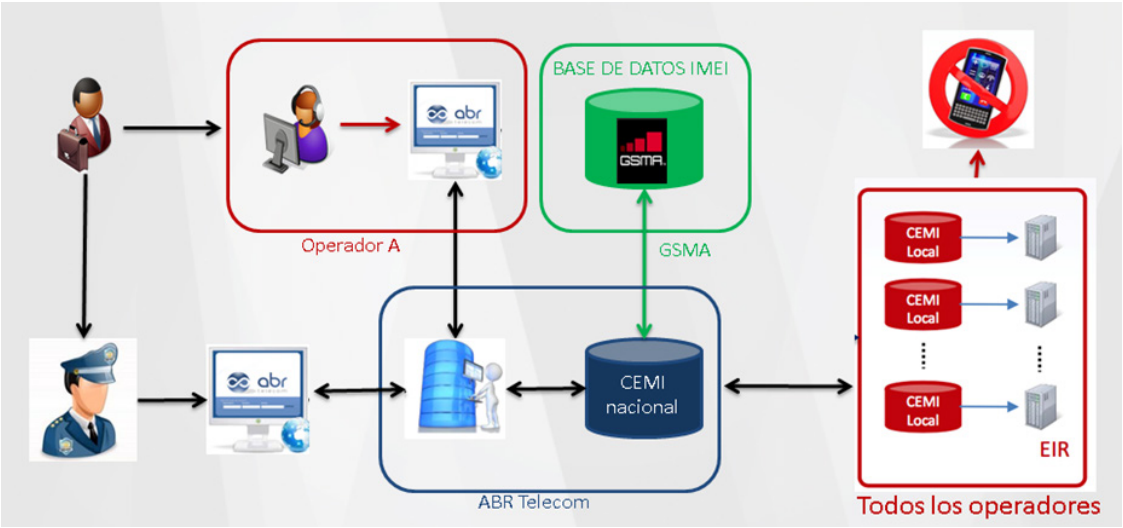
En septiembre de 2016, la Asociación GSM se alió con la Organización Mundial de Aduanas (OMA) para luchar contra la falsificación y el comercio fraudulento de móviles. La integración de la base de datos de IMEI permitirá realizar comprobaciones cruzadas y filtrar los dispositivos falsificados identificados por su IMEI en el punto de importación.

3.4.9 Brasil

Para combatir el uso de identificadores únicos robados, falsificados y no certificados, el Gobierno de Brasil ha puesto en marcha la iniciativa Celular Legal, coordinada por la *Agência Nacional de Telecomunicações* (ANATEL) y en la que participan todas las partes interesadas.[20] Las medidas aplicadas en el marco de esta iniciativa se organizan en torno a dos módulos:

- El módulo CEMI (*Cadastro de Estações Móveis Impedidas*) permite a los operadores de telefonía móvil y a la policía bloquear los dispositivos robados a petición del usuario.

Figura 8: Flujo de trabajo del CEMI



[19] CE 2 del UIT-D, Documento SG2RGQ/80 de la Asociación GSM (GSMA).
[20] João Zanon, Combating to the use of stolen and counterfeit ICT devices, Taller del UIT-D sobre *Lucha contra la falsificación de dispositivos de TIC*, 4 de octubre de 2018.

- El módulo SIGA (*Sistema Integrado de Gestão de Aparelhos*) se utiliza para identificar y bloquear dispositivos vinculados a otros tipos de fraude: manipulación, clonación, dispositivos no certificados, identificadores únicos irregulares, etc. *Celular Legal* dispone de una herramienta en línea que permite comprobar el estado de un dispositivo a partir de su código IMEI.[21]

3.4.10 Omán

De los dispositivos móviles registrados en la red nacional de Omán, casi 2 millones poseen códigos IMEI no válidos. Algunos números IMEI se han repetido casi 10 veces, porque más de 10 dispositivos poseen el mismo IMEI.[22] Esto crea un problema técnico en cuanto al registro de estos dispositivos en las redes locales y aumenta la carga financiera de los consumidores en general, al socavar la confianza en estos productos.

Los reguladores quieren asegurarse de que todos los dispositivos de TIC comercializados por los distribuidores e importadores se ajustan plenamente a las órdenes y decisiones pertinentes emitidas por el organismo regulador. Para ello, el organismo de inspección de la Autoridad Reguladora de las Telecomunicaciones (TRA) se encarga de garantizar la compatibilidad y el cumplimiento de las normas y especificaciones técnicas aplicables a los equipos de TIC vendidos en el mercado nacional.

La TRA ha creado un teléfono de ayuda en colaboración con los operadores locales para que los clientes puedan verificar los códigos IMEI. Aun así, la organización se enfrenta a dificultades, como la falta de acceso a una base de datos internacional de códigos IMEI, ya que el acceso completo a la base de datos de la GSMA no se concede a los organismos reguladores, sino únicamente a los fabricantes y operadores de un país determinado.

3.4.11 Normas y recomendaciones internacionales

- ISO 12931:2012: Criterios de calidad de funcionamiento para las soluciones de autentificación utilizadas en la lucha contra la falsificación de bienes materiales.
- ISO 16678:2014: Directrices para la identificación interoperable de objetos y sistemas de autenticación conexos con el fin de impedir la falsificación y el comercio ilícito.
- UIT-T Q.5050 (03/2019): Lucha contra la falsificación y el robo de dispositivos de TIC.
- UIT-T Y.4808 (08/2020)**:** Marco arquitectónico de entidad digital para luchar contra la falsificación en la IoT.

[21] Agência Nacional de Telecomunicações (ANATEL). Celular Legal.
[22] CE 2 del UIT-D, Documento 2/326 de Omán.

Capítulo 4 – Robo de dispositivos móviles

4.1 Introducción

El incremento del uso de dispositivos móviles en todo el mundo ha ido acompañado de un aumento del uso de dispositivos robados, a nivel tanto nacional como transfronterizo. Se necesitan iniciativas mundiales para mantener fuera de las redes a los dispositivos robados en todo el mundo.

La magnitud del daño que el uso de dispositivos fraudulentos está causando en todo el ecosistema ha hecho que los gobiernos y las industrias se interesen cada vez más por la búsqueda de remedios. Los gobiernos están aplicando normativas que abordan una amplia gama de cuestiones, entre ellas:

- el robo de teléfonos móviles;
- los riesgos para la seguridad;
- la pérdida de ingresos fiscales;
- la privacidad del consumidor;
- la calidad de la red;
- los derechos de propiedad intelectual.

Desde hace muchos años, la GSMA lidera las iniciativas del sector que implican el intercambio de datos para bloquear el acceso a las redes de dispositivos móviles robados o perdidos en todo el mundo. Utilizando el código único IMEI, la GSMA gestiona una lista negra de dispositivos sospechosos (es decir, los denunciados como perdidos o robados), que se pone a disposición de los operadores de todo el mundo.[23]

4.2 Problemas y cuestiones

El robo de dispositivos es un problema global que requiere una coordinación y una acción transfronterizas para que el robo resulte económicamente poco atractivo. Aunque las iniciativas de la industria han tenido un efecto positivo, es necesario realizar más esfuerzos, ya que la mayoría de las actividades realizadas hasta la fecha se han basado en normas mundiales de libre aplicación y algunos países aún no han coordinado sus esfuerzos con las prácticas mundiales de la industria. En este sentido, los países necesitan tener un enfoque unificado para la coordinación mundial con los esfuerzos de la industria. La falta de acción socava la eficacia de algunas de las medidas aplicadas.

Los requisitos para hacer frente al robo de dispositivos son los siguientes.

Normativa y medidas de aplicación

- Elaborar un marco reglamentario.

[23] CE 2 del UIT-D, Documento SG2RGQ/80 de la GSMA

- Implementar procedimientos operativos normalizados.
- Instalar y administrar una plataforma técnica para velar por la aplicación de la normativa.
- Realizar campañas de sensibilización.

Plataforma técnica

- Clasificar los dispositivos existentes:
  - analizar los datos del dispositivo a partir de la información de la red;
  - clasificar los dispositivos por IMEI (válido/inválido, único/duplicado)
- Permitir a los dispositivos existentes:
  - emparejar los códigos IMEI fraudulentos existentes con los códigos de identidad del abonado móvil internacional (IMSI) y el número de directorio del abonado internacional de la estación móvil (MSISDN).
- Registrar nuevos dispositivos:
  - exigir la homologación de tipo con identificadores de dispositivo únicos;
  - registrar los dispositivos importados y producidos localmente únicamente con identificadores válidos y únicos.
- Detectar la falsificación de códigos IMEI:
  - analizar los datos de red;
  - identificar dispositivos con códigos IMEI fraudulentos.
- Permitir el bloqueo de red:
  - controlar el acceso de los dispositivos no conformes/no registrados mediante el control de la red.

Implementación del sistema técnico[24]

- Conveniencia para todas las partes interesadas, en especial los consumidores.
- Un sistema autónomo que alivie la necesidad de integración e interoperabilidad de la red móvil que conllevan para los operadores costes innecesarios, limitaciones de la capacidad y cargas sobre los recursos.
- No se requiere una vinculación estricta entre el dispositivo y el cliente.
- Flexibilidad/configurabilidad para adaptarse a las normativas nacionales sin necesidad de personalización.

4.2.1 Delitos y fraudes relacionados con los dispositivos

Los delitos y fraudes relacionados con los dispositivos tienen repercusiones negativas sobre varios grupos de partes interesadas:

- Consumidores: Riesgo de perjuicio en relación con el robo, la pérdida de propiedades y la pérdida de información personal.
- Gobiernos: Mayor criminalidad, menores ingresos fiscales.

[24] Mohammad Raheel Kamal. An Open Source CEIR to Combat Counterfeit and Stolen ICT Devices. *Tercer Taller Regional de la Comisión de Estudio 11 del UIT-T para África sobre " Dispositivos de TIC falsificados, retos en materia de pruebas de conformidad e interoperabilidad en África"*, Túnez, 30 de septiembre de 2019.

- Comerciantes: Compra involuntaria de bienes robados, problemas de calidad de funcionamiento de la red.
- Aseguradoras: Aumento de los costes de seguro, transferencia de la titularidad de los bienes robados.
- Operadores: Pérdida de abonados, pérdida de subsidios, costes de suscripción de seguros.
- Autoridades encargadas de velar por el cumplimiento de la ley: Crimen organizado, pérdida de recursos.

4.2.2 Funciones y responsabilidades de las partes interesadas

Varias partes interesadas pueden desempeñar un papel importante en la lucha contra el robo de dispositivos.

Los **gobiernos** pueden elaborar un marco normativo, aplicar procedimientos operativos normalizados, desplegar y gestionar tecnología destinada a hacer cumplir la normativa, y realizar campañas de sensibilización;

Los **fabricantes/importadores** pueden obtener la aprobación del tipo de dispositivo por parte del gobierno/organismo regulador, registrar todos los dispositivos que se van a importar y registrar todos los dispositivos fabricados localmente.

Los **operadores** pueden proporcionar al gobierno datos de red relacionados con los dispositivos, garantizar la compatibilidad con el Registro de Identidad de Equipos (EIR), admitir la creación de listas negras de códigos IMEI válidos/no válidos y permitir excepciones, y notificar a los abonados el estado de sus dispositivos, a través de un SMS si fuera necesario.

Los **consumidores** Los consumidores pueden verificar el estado de sus dispositivos (a través de un SMS, una aplicación o una interfaz web), registrar los dispositivos importados individualmente, denunciar el robo de dispositivos a las autoridades y presentar pruebas (facturas) de los dispositivos auténticos, si fuera necesario.

4.2.3 Herramientas indispensables para combatir el robo de dispositivos

La lucha contra el robo de dispositivos se puede llevar a cabo a nivel de la red y del dispositivo.

Protección basada en el dispositivo:

- Capacidad para borrar contactos y fotos y bloquear los pagos mediante el móvil.
- Función de reinicio de fábrica para borrar todos los datos.
- Función de borrado a distancia.

Protección basada en la red:

- Bloqueo del acceso a la red del teléfono robado.

Comprobación de la situación del dispositivo:

- Comprobar la situación del dispositivo antes del reciclado.
- Hacer que el robo de un teléfono no sea rentable.

4.3 Directrices

Implicación de múltiples partes interesadas

Los usuarios pueden denunciar el robo de dispositivos a sus operadores de red, activar las funciones antirrobo en sus dispositivos y, en los países en los que los operadores están conectados a la lista negra de IMEI de la GSMA para los operadores, se puede animar a los usuarios a comprobar el estado del IMEI de los dispositivos usados que tienen previsto comprar.[25]

Los operadores de redes móviles pueden bloquear los dispositivos robados en sus redes y conectarse a la lista negra de IMEI de la GSMA para operadores a fin de compartir y recopilar datos de la lista negra y animar a sus proveedores de dispositivos a proteger adecuadamente la integridad de las implementaciones de IMEI en sus productos.

Los fabricantes de dispositivos/propietarios de marcas pueden garantizar la integridad de los códigos IMEI en todos sus productos, diseñar dispositivos más seguros (es decir, imposibilitar la reprogramación de los códigos IMEI) e implementar la funcionalidad de desactivación *kill switch* para permitir a los usuarios desactivar a distancia los dispositivos perdidos y robados.

Los operadores de tiendas de aplicaciones pueden obtener los códigos IMEI de los dispositivos robados a través de la GSMA y utilizarlos para denegar el acceso a la tienda de aplicaciones a los dispositivos que hayan sido denunciados como robados.

Todas las partes interesadas (gobiernos, fabricantes, operadores de redes y consumidores) deben colaborar en la lucha contra el robo de dispositivos móviles, en particular mediante:

- Compromiso y participación de las fuerzas del orden.
- Vigilancia de los canales de distribución para hacer frente al tráfico de dispositivos robados.
- Apoyo legislativo y judicial a las iniciativas antirrobo.
- Atención centrada en los dispositivos, mínimos inconvenientes para los usuarios.
- Un énfasis renovado en los esfuerzos colectivos, con todos los países desempeñando su papel.
- Medidas para apoyar las capacidades existentes en lugar de replicarlas o socavarlas.
- Medición e información de la eficacia de los enfoques adoptados.
- Análisis de las medidas adoptadas para determinar lo que funciona y lo que no.
- Adopción de tecnologías y soluciones emergentes para colmar las lagunas.

Gobiernos y organismos reguladores deben colaborar para asegurarse de que:

- Los operadores despliegan EIR para bloquear los dispositivos robados en las redes locales.
- Se cumplen las directrices de prácticas óptimas para el bloqueo de dispositivos y el intercambio de datos.
- Los EIR de los operadores se conectan a la base de datos de IMEI para garantizar el bloqueo internacional.
- Se refuerzan los niveles de seguridad del IMEI y se notifican y resuelven los problemas.

---

[25] James Moran (GSMA). Combating device crime together – Best practice to combat mobile device theft. *Taller de la UIT sobre "Enfoques globales para luchar contra la falsificación y el robo de dispositivos de TIC"*, Ginebra, 23 de julio de 2018.

- Los códigos IMEI son comprobados por los agentes de la ley, los funcionarios de aduanas, los minoristas y los consumidores.
- Se toman medidas contra los delincuentes (manipulación de IMEI, robo y tráfico).
- Se tomen medidas para educar a los consumidores y promover las capacidades de los interruptores de seguridad (*kill switch*).
- Se acuerdan sistemas de medición para seguir el progreso de estos esfuerzos y se instaura la obligación de presentar informes.

4.4 Experiencias nacionales (estudios de caso)

4.4.1 República Centroafricana

En el marco de su política de desarrollo de las infraestructuras de TIC, el Gobierno de la República Centroafricana ha abierto el mercado de las TIC a cuatro operadores de telefonía móvil y un operador de telefonía fija para garantizar la máxima cobertura del territorio nacional y ofrecer servicios de calidad a la población.[26]

Los fallos en la aplicación de esta política por parte del Organismo Regulador de las Comunicaciones Electrónicas y Correos (ARCEP) han provocado un desarrollo no regulado de las infraestructuras, dificultades en el control de la conformidad y la interoperabilidad de los equipos de TIC y un aumento de las falsificaciones y los robos de terminales móviles. Las inversiones y los ingresos del sector se han resentido.

Para hacer frente a estos problemas, el Gobierno de la República Centroafricana:

- Adoptó y promulgó la Ley de Comunicaciones Electrónicas y sus textos de aplicación.
- Adoptó y promulgó la ley de creación del Organismo Regulador de las Comunicaciones Electrónicas y Correos (ARCEP).
- Redactó el proyecto de ley sobre ciberdelincuencia y ciberseguridad.
- Creó un centro de control de tráfico, antifraude y localización de terminales móviles.
- Creó la Secretaría Permanente para la Gobernanza de las Comunicaciones Electrónicas con el fin de garantizar la vigilancia tecnológica.
- Completó el proyecto de red medular de infraestructura de fibra óptica internacional que conecta la capital, Bangui, con la República del Congo y Camerún.
- Ejecutó el proyecto de digitalización nacional *Centrafrique digital 2025*.
- Implementó un plan estratégico nacional para el desarrollo de infraestructuras de banda ancha de muy alta velocidad.
- Creó una agencia nacional de TIC y un centro nacional de datos.

La República Centroafricana recomienda que la UIT preste asistencia y apoyo para ayudar a los países a crear capacidad en relación con los programas de conformidad e interoperabilidad, y para hacer frente a los productos falsificados y al robo de equipos móviles.

4.4.2 México

Para luchar contra el robo de equipos terminales móviles, el Instituto Federal de Telecomunicaciones (IFT), organismo regulador nacional de las telecomunicaciones y la

[26] CE 2 del UIT-D, Documento SG2RGQ/144 de la República Centroafricana.

radiodifusión de México, ha establecido obligaciones reglamentarias. Se han puesto en marcha varias iniciativas a nivel nacional e internacional para controlar los códigos IMEI.[27]

En el plano internacional, el Gobierno de México, a través de sus ministerios y departamentos, ha firmado convenios bilaterales y regionales para intercambiar información sobre los códigos IMEI de los dispositivos robados o perdidos y prohibir su reutilización. Se ha concluido un acuerdo con la GSMA para implementar el sistema de verificación de dispositivos IMEI, que permite a los usuarios de dispositivos móviles consultar la base de datos de números IMEI de la GSMA en tiempo real.

En el plano nacional, el IFT publicó en el Diario Oficial una disposición técnica (IFT-011-2017) con directrices de colaboración en materia de seguridad y justicia, relativas a la suspensión del servicio para los dispositivos o equipos terminales móviles denunciados como robados o extraviados. El IFT reforzó esta colaboración con la aplicación de disposiciones técnicas que incluían especificaciones para los terminales móviles conectados a las redes de telecomunicaciones y el control de la conformidad:

- Evaluación de la conformidad.
- Actualización del certificado de conformidad.
- Base de datos de códigos IMEI de dispositivos aprobados.
- Control de la conformidad mediante requisitos de certificación.

El IFT verifica el cumplimiento de los requisitos de la citada disposición técnica siguiendo los métodos de prueba descritos en la misma.

4.4.3 Universidad de Ciencia y Tecnología del Irán

Para prevenir el fraude y combatir la venta y el uso de dispositivos ilegales, incluidos los teléfonos robados y los teléfonos por los que no se han pagado tasas aduaneras, la República Islámica del Irán elaboró en 2017 un plan de registro de teléfonos móviles.[28]

Cuando el dispositivo se enciende para acceder a un servicio, se evalúa; si la información requerida no está disponible en la lista legal, el dispositivo se identificará como ilegal y se añadirá a una lista negra.

Según el sistema de comercio global de la República Islámica del Irán, los teléfonos importados se registran en las fronteras aduaneras y se asigna a cada terminal un código de activación único. La Universidad de Ciencia y Tecnología del Irán ha desarrollado el sistema HAMTA, una base de datos en línea que permite la activación del dispositivo con un código único y ofrece a los usuarios dos funciones principales:

- informar del estado de los teléfonos móviles actualmente activos en el país, confirmar la autenticidad de un teléfono móvil y verificar que la unidad es legal y está activada;
- activar teléfonos nuevos y legalmente importados.

Los datos de los equipos registrados en el sistema HAMTA se transmiten al Organismo Regulador de las Comunicaciones de la República Islámica del Irán y a los operadores de telefonía móvil. Sólo los dispositivos registrados y autentificados por el sistema HAMTA se consideran legales y pueden acceder a los servicios prestados por los operadores; todos los demás están en la lista negra.

[27] CE 2 del UIT-D, Documento 2/166 de México.
[28] CE 2 del UIT-D, Documento 2/83 de la República Islámica del Irán.

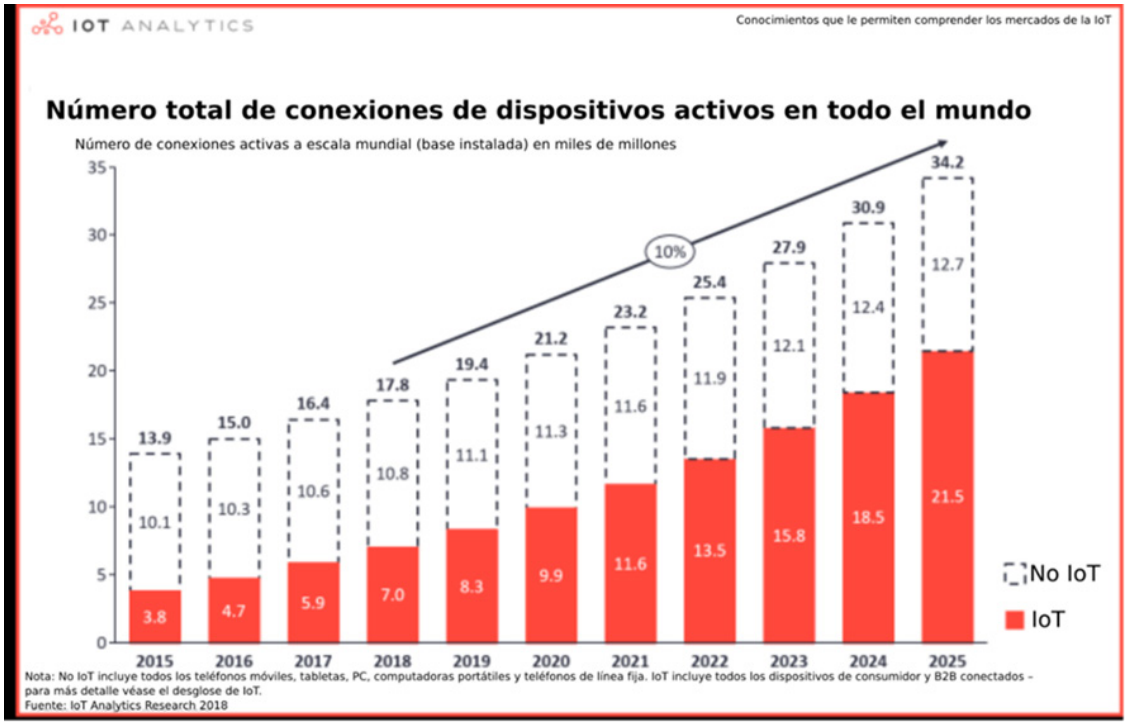
Capítulo 5 – La Internet de las cosas y la C+I

5.1 Introducción

La UIT define Internet de las cosas (IoT) como "una infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperabilidad de tecnologías de la información y la comunicación (TIC) presentes y futuras. [29],[30]

Las tecnologías IoT se encuentran en diferentes sectores industriales y afectan a la vida cotidiana de las personas a través de plataformas que procesan los datos generados por miles de millones de dispositivos conectados. Un estudio realizado por IoT Analytics indica que el número total de conexiones de dispositivos activos en todo el mundo aumentará de forma espectacular. En 2020, de los 21 200 millones de conexiones de dispositivos activos en todo el mundo, 9 900 millones son conexiones de IoT. Esta cifra puede aumentar a 21 500 millones en 2025.[31]

Figura 9: Número de conexiones de dispositivos activos en todo el mundo



[29] Recomendación UIT-T Y.2060 (06/2012): Visión general de la Internet de las cosas.
[30] Recomendación UIT-T Y.2069 (07/2012): Términos y definiciones para la Internet de las cosas.
[31] IoT Analytics, State of the IoT 2018: Number of IoT devices now at 7B – Market accelerating. Agosto de 2018.

5.2 Efectos de la IoT sobre la C+I y la preparación de las TIC

Para satisfacer las necesidades específicas de la IoT, hay que resolver ciertos problemas y desafíos, como la calidad, la fiabilidad, la cobertura y el bajo consumo de energía.

5.2.1 Desafíos de la IoT

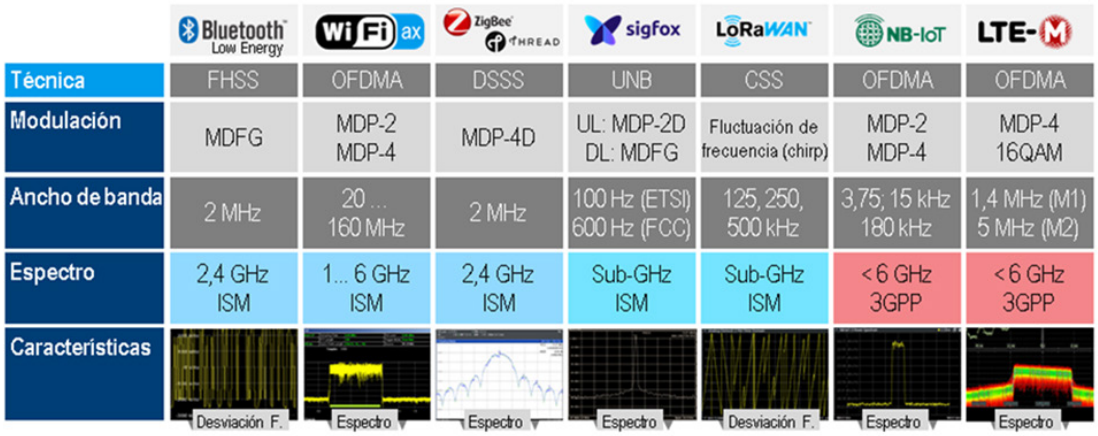
No basta con tener buenos sensores de recogida de datos; también es necesario garantizar una buena conectividad para transmitir los datos e implementar una plataforma para analizarlos y procesarlos.

Entre los muchos retos asociados a la IoT, destacan los siguientes.

La elección de la tecnología: Clave del éxito de la IoT

En el futuro, las aplicaciones de IoT que requieran cobertura y movilidad totales se centrarán en la tecnología celular, como las tecnologías LTE-M y NB-IoT basadas en 4G y 5G. Otras, como Sigfox o LoRaWAN, harán uso de tecnologías de baja potencia que operan en las bandas sin licencia. La mayoría de las aplicaciones utilizarán tecnologías inalámbricas de corto o medio alcance, como Bluetooth®, WLAN/Wi-Fi y Zigbee. Las tecnologías inalámbricas de IoT se muestran en la **Figura 10**.[32]

Figura 10: Tecnologías inalámbricas de IoT



Diseño que responde a las necesidades de IoT, es decir, calidad, fiabilidad, cobertura ampliada, latencia, etc.

El diseño también debe responder a las expectativas de los usuarios, especialmente en el ámbito de la confidencialidad y la protección de los datos personales, y generar confianza mediante el empleo de normas de seguridad en el ecosistema de IoT.

[32] Joerg Koepp (Rohde & Schwarz, Alemania), "Ensuring reliable and secure communication in a hyper-connected world", *Cuestión 4/2 del UIT-D, Taller sobre conformidad e interoperabilidad de las TIC: desafíos para los países en Desarrollo*, Ginebra, 16 de octubre de 2019.

La necesidad de certificación de las plataformas y dispositivos de IoT

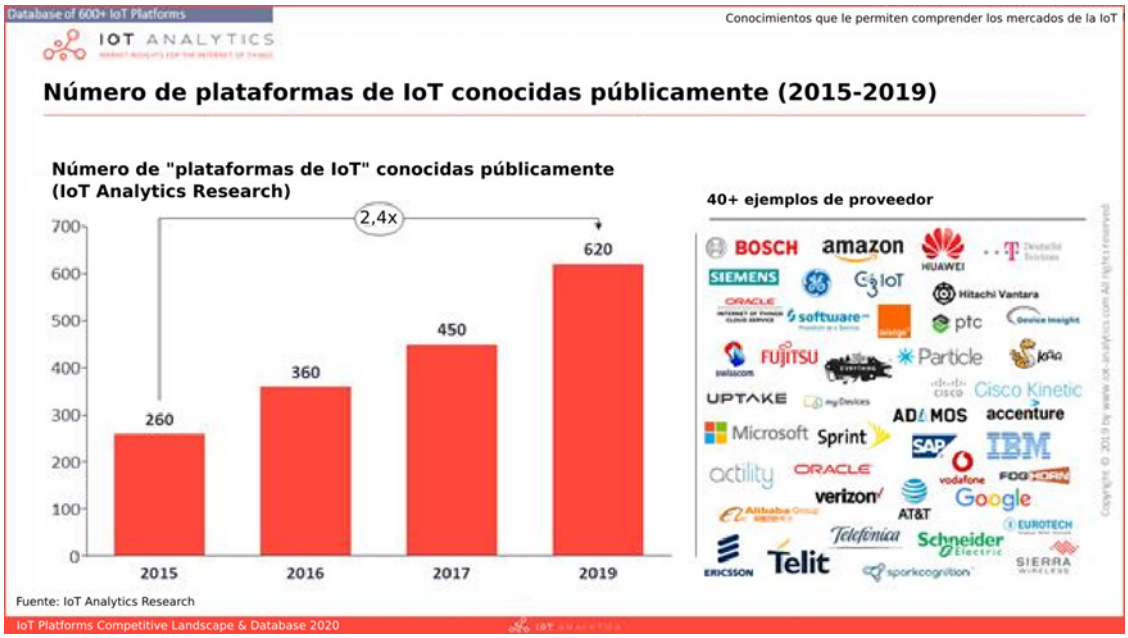
Las plataformas y los dispositivos deben certificarse evaluando su conformidad respecto de las normas y los reglamentos internacionales.

5.2.2 Limitaciones de la IoT

La IoT se basa esencialmente en el objeto (sensor), la red (conectividad), los datos y las aplicaciones de explotación. Las limitaciones resultantes incluyen:

- **Múltiples plataformas de IoT**: Las estadísticas generadas por IoT Analytics muestran que en 2019 hubo **620** plataformas IoT y más de 40 proveedores (véase la **Figura 11**).[33]

Figura 11: Número de plataformas de IoT conocidas públicamente



- **Múltiples protocolos de IoT**: Existen múltiples protocolos de intercambio de datos, dependiendo de las organizaciones de normalización (SDO) y de los fabricantes de productos IoT. Cada norma de IoT tiene su propio marco normativo, lo que deja a los profesionales de TI la posibilidad de elegir entre una multitud de opciones (véase la **Figura 12**).[34]

[33] IoT Analytics, IoT Platform Companies Landscape 2019/2020: 620 IoT Platforms globally. Diciembre de 2019.

[34] Alianza para la Innovación de la IoT (AIOTI), IoT LSP Standard Framework Concepts, Release 2.9, 2019.

Figura 12: Panorama de las organizaciones de normalización y alianzas de la IoT (dominios vertical y horizontal)

Fuente: AIOTI WG3 (IoT Standardisation) – Release 2.9

En la actualidad, la IoT dista mucho de estar normalizada, existiendo un amplio abanico de normas y soluciones incompatibles.[35] Dada la proliferación de plataformas y protocolos de IoT que facilitan la comunicación con los objetos, las normas técnicas aplicables a esta tecnología han evolucionado en diversos contextos a partir de diversas aplicaciones y partes interesadas, con requisitos y objetivos diferentes. Por consiguiente, un importante desafío es el que consiste en garantizar la interoperabilidad, la escalabilidad, la solidez de las normas internacionales y la seguridad de extremo a extremo. (véase la **Figura 13**).

Figura 13: Necesidad de sistemas de certificación adaptados

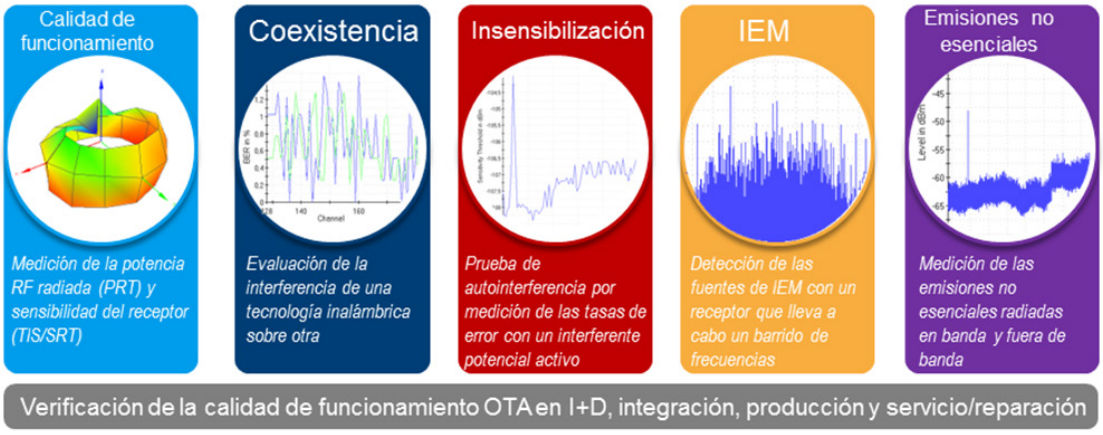
5.2.3 Ejemplo: Prueba de IoT de Rohde & Schwarz

Para Rohde & Schwarz, las mediciones por vía aérea (OTA) ayudan a garantizar la calidad de funcionamiento y el cumplimiento de la normativa. Las pruebas se centran en la calidad de funcionamiento, la coexistencia, las pruebas de interferencias, las interferencias

[35] UIT. Documento del UIT-T SG20-TD1722, *Seminario web de la UIT sobre el tema "Acelerar la transformación de las ciudades mediante las normas"*, 25 de junio de 2020.

electromagnéticas (IEM) y la medición de las emisiones no esenciales radiadas en banda y fuera de banda (véase la **Figura 14).**[36]

Figura 14: Mediciones OTA



5.2.4 Organizaciones de normalización

La adopción de un enfoque unificado para los sistemas de IoT como medio para fomentar el desarrollo de la industria ha incitado a las SDO a trabajar para crear una arquitectura normalizada que garantice la interoperabilidad de sistemas, aplicaciones, dispositivos y sensores.

Unión Internacional de Telecomunicaciones

El UIT-T ha desarrollado las Recomendaciones de la serie Y, que abarcan la infraestructura mundial de la información, los aspectos del protocolo internet, las redes de próxima generación, la IoT y ciudades inteligentes Internet de las cosas y ciudades y comunidades inteligentes. La Comisión de Estudio 20 (CE 20) del UIT-T ha estado trabajando en normas internacionales para promover la interoperabilidad entre las infraestructuras digitales y las aplicaciones de la IoT.

En marzo de 2020, la UIT publicó la Recomendación UIT-T Y.4459[37], en la que se presentaba una arquitectura de entidad digital. Esta la define un conjunto mínimo de componentes arquitectónicos y servicios necesarios para proporcionar información genérica e interoperabilidad de los servicios. Facilitará la interoperabilidad de la identificación, la descripción, la representación, el acceso, el almacenamiento y la seguridad de los dispositivos de IoT. Este marco arquitectónico propicia el uso de una interfaz común de seguridad y gestión entre distintas aplicaciones de IoT.

Para la realización de pruebas de C+I, la Comisión de Estudio 11 (CE 11) del UIT-T y el Comité de Dirección sobre Evaluaciones de Conformidad del UIT-T están trabajando junto con la CE 20 en un modelo de red para las pruebas de IoT.[38]

---

36 Joerg Koepp (Rohde & Schwarz, Alemania). Op. cit.

37 Recomendación UIT-T Y.4459 (12/2020): Marco de arquitectura de entidad digital para la interoperabilidad de Internet de las cosas.

38 Kofi Ntim Yeboah-Kordieh (Ghana), ITU-T SG11 Work Updates and Activities, *Cuestión 4/2 del UIT-D, Taller sobre conformidad e interoperabilidad de las TIC: desafíos para los países en desarrollo*, Ginebra 16 de octubre de 2019.

La Organización Internacional de Normalización y la Comisión Electrotécnica Internacional

En 2018, la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI) publicaron la norma ISO/IEC 30141, una arquitectura de referencia normalizada armonizadora para la IoT, descrita como "el complejo conjunto de miles de millones de dispositivos inteligentes conectados a través de Internet".[39]

En 2019, la ISO y la CEI publicaron la norma ISO/IEC 21823-1,[40] que proporciona una visión general de la interoperabilidad en lo que respecta a los sistemas de IoT.

Instituto de Ingenieros Eléctricos y Electrónicos (IEEE)

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó la norma 2413-2019, "IEEE Standard for an Architectural Framework for the Internet of Things (IoT)".[41] La norma P2413.1 proporciona un plan arquitectónico para la implementación de la ciudad inteligente aprovechando la interacción e interoperabilidad entre los diferentes componentes y dominios de la ciudad inteligente.[42] Esta norma se basa en el marco arquitectónico establecido para la IoT en el proyecto de norma IEEE P2413, que se basa a su vez en la norma internacional ISO/IEC/IEEE 42010.

5.3 Reglamentación y políticas para la IoT y las TIC

Los organismos reguladores deben ser conscientes de las repercusiones de la C+I en la IoT. Aunque los laboratorios de pruebas contribuyen a garantizar la calidad de funcionamiento, la conformidad y la interoperabilidad de los productos, la normativa también es necesaria.

En la actualidad, el despliegue de las tecnologías de la IoT por parte de entidades públicas y privadas se lleva a cabo en diferentes sectores, como la sanidad, las telecomunicaciones, la educación, la agricultura, las finanzas y los medios de comunicación, así como en las ciudades inteligentes. Por lo tanto, el establecimiento de un entorno normativo intersectorial, adaptado a la IoT, es de suma importancia y requiere una reglamentación de quinta generación (o sea, una reglamentación basada en la colaboración).

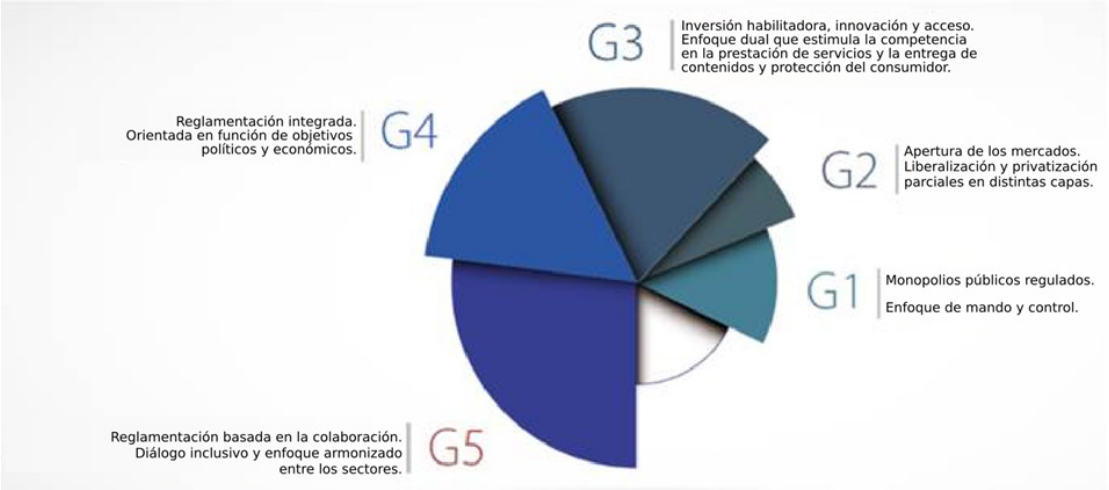
5.3.1 Visión general de la normativa basada en la colaboración

La reglamentación ya ha evolucionado considerablemente entre la primera y la cuarta generación: desde los monopolios regulados hasta las reformas básicas y la liberalización del mercado, pasando por la reglamentación de un entorno que estimule la innovación y, a continuación, el acceso a la cuarta generación de reglamentación integrada centrada en cuestiones relacionadas con Internet (véase la **Figura 15**).[43]

---

39 ISO. ISO/CEI 30141:2018, Internet of Things (IoT) – Reference Architecture. Agosto de 2018.
40 ISO. ISO/CEI 21823-1:2019, Internet of things (IoT) – Interoperability for IoT systems – Part 1: Framework. Febrero de 2019.
41 IEEE. IEEE 2413-2019, IEEE Standard for an Architectural Framework for the Internet of Things (IoT). Mayo de 2019.
42 IEEE. IEEE P2413-1, Standard for a Reference Architecture for Smart City (RASC). Agosto de 2018.
43 UIT-D. Global ICT Regulatory Outlook 2017.

Figura 15: Generaciones de reglamentación de las TIC – un marco conceptual



La reglamentación de quinta generación, o colaborativa, es flexible y está impulsada por el consenso. La reglamentación colaborativa promueve la innovación, la eficiencia, la calidad del servicio, el intercambio de datos y la seguridad, y supera obstáculos como los problemas de interoperabilidad. Además, se basa en la puesta en común de conocimientos, principios rectores y prácticas óptimas y en la identificación de mecanismos de cooperación intersectorial para resolver con mayor eficacia los retos comunes (véase la **Figura 16**).[44]

Figura 16: Reglamentación colaborativa

Las Directrices de prácticas óptimas del GSR-19 se centraron en la reglamentación colaborativa como mecanismo para garantizar el éxito de la transformación digital.[45]

---

44 *Ibid*.

45 UIT. Simposio Mundial para Organismos Reguladores (GSR). Directrices de prácticas óptimas 2019. Port Vila, 2019.

5.3.2 Reglamentación de la IoT

Muchos gobiernos están fomentando la innovación en la IoT y desean reformar su marco reglamentario para no obstaculizar su crecimiento. Sin embargo, como todavía existe un grado de incertidumbre reglamentaria en relación con el mercado de la IoT, las innovaciones y ajustes reglamentarios se harán por fases.

La IoT es diferente de la conectividad que los reguladores de las TIC están tratando de implantar. La conectividad es el servicio principal, mientras que la IoT abarca también las aplicaciones, los dispositivos y los sensores asociados.

En general, aunque todos los reglamentos se aplican a la IoT, esta tecnología puede dar lugar a requisitos adicionales. Las políticas y reglamentaciones deben abordar cuestiones específicas de la IoT, como:

- Confidencialidad, protección de datos y seguridad.
- Normas e interoperabilidad de sistemas, plataformas y objetos conectados.
- Gestión del espectro y concesión de licencias (en muchos casos, los dispositivos de IoT utilizan tecnologías inalámbricas).
- Numeración y portabilidad de los números.
- La necesidad de migrar de IPv4 a IPv6.
- Costes, fiabilidad, QoS y calidad de la experiencia (QoE).
- Medidas para gestionar la competencia.

La reglamentación de las TIC se ha vuelto cada vez más compleja, debido a cuestiones relacionadas con la seguridad, la confidencialidad y la protección de datos. Es posible que muchos países tengan que actualizar normativas obsoletas o excesivamente restrictivas, y que la intensificación de los esfuerzos se vea afectada por la interoperabilidad.

Para mejorar la interoperabilidad y reducir los costes, los profesionales reclaman un ecosistema de IoT abierto construido sobre plataformas, aplicaciones y normas de código abierto y no propietario, promoviendo así el crecimiento económico y la innovación.

5.4 Conclusión

La normalización es fundamental para establecer un mercado único de IoT en el que cualquier dispositivo pueda conectarse y comunicarse desde cualquier lugar. La normalización facilita la interoperabilidad, la compatibilidad, la fiabilidad y la seguridad; estimula la aparición de nuevos ecosistemas y la innovación; e impulsa la competitividad.

Los organismos reguladores deben reconocer los efectos de las nuevas tecnologías de la IoT, y el importante papel que desempeñan en el desarrollo de estas tecnologías, creando más oportunidades al dar paso a una nueva era de reglamentación colaborativa en la que los organismos reguladores de las TIC actúen más como facilitadores, trabajando para mejorar la conectividad y colaborando con otras partes interesadas para promover el uso de las TIC en todos los ámbitos.

En conclusión, una estrategia basada en un marco normativo progresivo puede proteger e impulsar a todas las partes interesadas mediante el despliegue de conocimientos técnicos especializados y recursos financieros y de otro tipo. Además, dicha estrategia puede promover esta nueva tecnología, un mercado competitivo y una rápida innovación.

Capítulo 6 – Transferencia de información, competencias y conocimientos

6.1 Necesidades de aprendizaje y oportunidades educativas en materia de C+I

La C+I requiere un conjunto de calificaciones, y se necesitan profesionales formados para dirigir los programas de C+I. Además, ciertos retos son inherentes a este campo, como:

- Falta de programas formales de formación integral en C+I. Las grandes instituciones forman al personal en C+I emparejándolo con trabajadores experimentados. Aunque puede ser útil, este enfoque tiende a proporcionar una experiencia limitada sin controles de calidad formales. Además, no puede aplicarse en instituciones más pequeñas.
- Los diversos profesionales de la C+I, incluidos los organismos reguladores, los titulares de licencias, los solicitantes de certificaciones (importadores y fabricantes) y los gestores de la conformidad, también deben tener un claro conocimiento de las cuestiones jurídicas, técnicas, de comercio internacional y económicas.
- La rápida evolución de los productos tecnológicos representa un desafío constante para los marcos de C+I (por ejemplo, con respecto a la IoT y a la configuración del software).

En la Resolución 177 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios de la UIT se destacó la necesidad de seguir ofreciendo actividades de capacitación en materia de C+I en el puesto de trabajo, en colaboración con instituciones reconocidas y aprovechando el ecosistema de la Academia de la UIT, incluidas las actividades de prevención de las interferencias de radiocomunicaciones causadas o recibidas por los equipos de TIC.[46]

Las experiencias de 2020 han demostrado la urgente necesidad mundial de aprendizaje digital a través de redes de TIC fiables. Tras la pandemia de la COVID-19, el uso de las TIC con fines educativos se considera más que nunca un bien público. Como se propone en la Resolución 177 (Rev. Dubái, 2018), la Academia de la UIT ofrece soluciones de formación en línea para formadores que deberían ser exploradas por la comunidad mundial de C+I.

6.2 Responder a las necesidades relacionadas con la adquisición/retención de conocimientos

Debería considerarse la posibilidad de crear una plataforma de colaboración basada en mecanismos de garantía de calidad para fomentar el desarrollo de un conjunto más amplio de competencias, siguiendo el ejemplo de la propuesta de la UIT de un programa de formación en materia de conformidad e interoperabilidad (CITP).[47]

---

[46] UIT. Resolución 177 (Rev. Dubái, 2018) de la Conferencia de Plenipotenciarios sobre Conformidad e interoperabilidad.

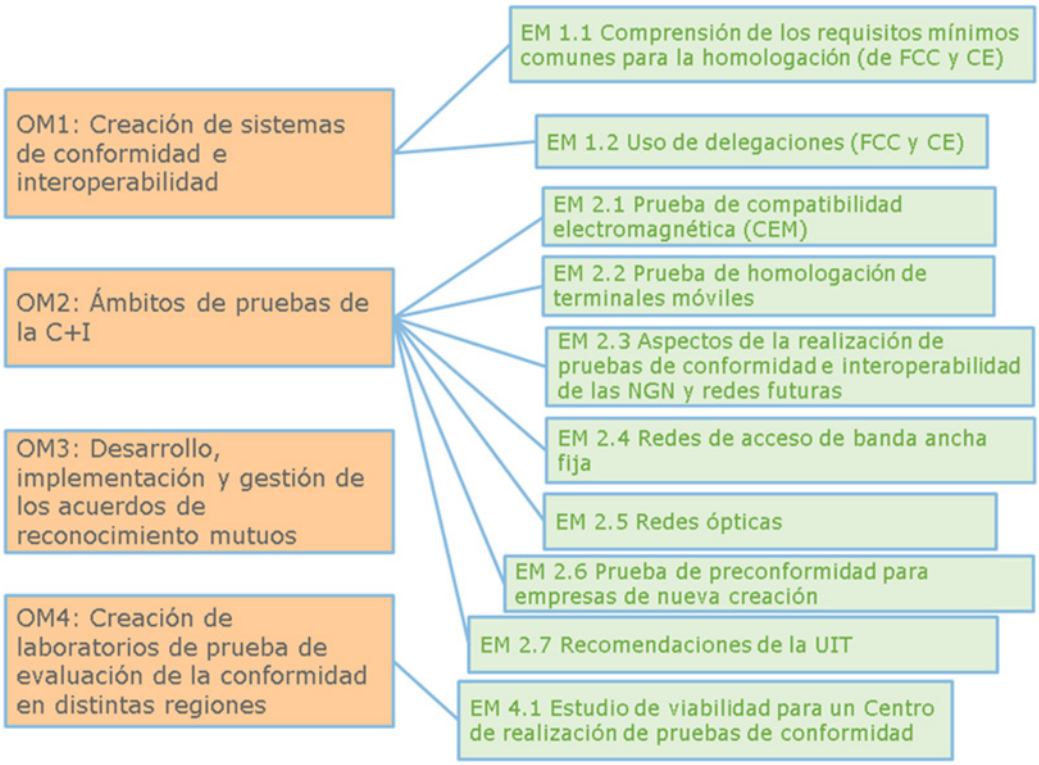
[47] Estos conceptos se presentaron en octubre de 2019 a la Cuestión 4/2 en el Documento de la CE 2 del UIT-D SG2RGQ/194+Annex del Coordinador de la BDT para la Cuestión 4/2.

El CITP se basa en anteriores eventos de formación sobre C+I que han tenido éxito, como las actividades regionales de formación en el puesto de trabajo en los ámbitos de la C+I y de las pruebas, desarrollados conjuntamente con los laboratorios asociados.[48] El programa también tiene en cuenta las enseñanzas extraídas de las publicaciones de la UIT, incluido el informe final sobre la Cuestión 4/2 para el anterior periodo de estudios,[49] y las directrices publicadas.[50]

El trabajo para desarrollar el CITP está siguiendo el modelo establecido por el mecanismo de garantía de calidad de la Academia de la UIT, que incluye un paquete de materiales de alto nivel preparados por expertos en la materia, un proceso de revisión por pares y plantillas preparadas por formadores profesionales para redactar tarjetas de planes de estudio y esquemas de formación.

A continuación se expone una propuesta de estructura de formación que ofrece itinerarios de aprendizaje adaptados:

Figura 17: Módulos de formación del CITP (OM son módulos obligatorios, EM son módulos optativos)



La estructura de la formación se organiza en torno a cuatro temas principales y se divide en subtemas para apoyar el itinerario de aprendizaje seleccionado y garantizar la transferencia modular de conocimientos que necesitan los estudiantes.

48 UIT-D. Eventos de conformidad e interoperabilidad.
49 UIT-D. Informe Final sobre la Cuestión 4/2 de la Comisión de Estudio 2 del UIT-D para el periodo de estudios 2014-2017. Op. cit.
50 UIT-D. Publications and deliverables – C&I.

1) **Diseño y creación de regímenes/marcos de conformidad e interoperabilidad**

   Este módulo se centra en la comprensión de los requisitos técnicos mínimos y en el uso de las estructuras de C+I existentes y de las delegaciones (*proxies*) para encontrar el equilibrio adecuado entre la confianza y el control de los dispositivos de TIC.

2) **Ámbitos de realización de pruebas que abarcan una amplia gama de servicios de laboratorio**

   El ámbito de las pruebas es potencialmente inacabable, y puede abarcar temas como la aprobación de nuevas tecnologías y el apoyo a los jóvenes inventores para ayudarles a conseguir el reconocimiento internacional de sus productos.

   Se entiende claramente que los módulos de formación deben desarrollarse como respuesta a las necesidades y prioridades existentes.

3) **Colaboración regional y armonización de normas y procesos de homologación, incluidos los acuerdos de reconocimiento mutuo**

   Como se ha indicado en el capítulo anterior, la colaboración es clave, y este módulo promueve la puesta en común de los recursos y mecanismos que ya existen para certificar la conformidad de los productos de TIC respecto de los requisitos técnicos internacionales y nacionales.

4) **Creación y mantenimiento de laboratorios de pruebas**

   Este módulo se centra en los procedimientos de calidad y las evaluaciones estratégicas, tales como la optimización de la planificación empresarial.

6.3 Conclusiones

En resumen, un análisis exhaustivo de la manera de elaborar un programa de formación en materia de transferencia de información, aptitudes y conocimientos debe tener en cuenta:

- la colaboración con expertos en la materia: entre los que se incluirán las Comisiones de Estudio de la UIT (la C4/2 de la CE 2 del UIT-D, la CE 11 del UIT-T y los colaboradores de la Oficina de Radiocomunicaciones), los profesionales de la realización de pruebas, los gestores de homologación, y los expertos comerciales;
- material de formación basado en las publicaciones de la UIT sobre el programa de C+I, incluidas las directrices y las Recomendaciones de la UIT elaboradas por el UIT-R y el UIT-T;
- trabajo sobre la transferencia de conocimientos por parte de organizaciones internacionales, regionales y nacionales;
- acceso fácil a la formación en C+I y garantía de un enfoque profesional y orientado al futuro;
- un diseño de curso universalmente accesible, tanto para principiantes como para especialistas;
- un enfoque modular y flexible, que proporcione el nivel de conocimientos adecuado a la tarea en cuestión y garantice que el contenido responda a las necesidades de C+I actuales.

Anexos

Annex 1: Conformance and interoperability frameworks: Country data

Understanding how countries organize themselves for guaranteeing proper levels of conformance and interoperability for the deployment of ICT networks and devices can help C&I operators to establish efficient mechanisms for collaboration. This can be verified in effective technical collaboration agreements in some regions (e.g. Europe, APEC-MRA).

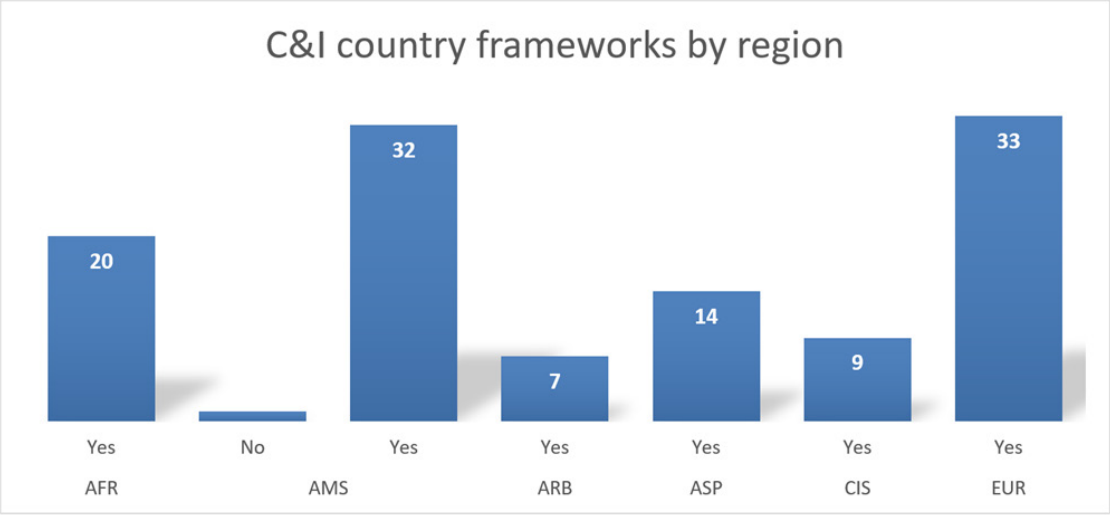
Data show that most of the countries have in place a C&I arrangement aiming to ascertain trust on safe and interoperable use of ICT devices by networks and citizens. Note that procedures and strictness levels of requirements (e.g. recognition of certification and use of proxies, self-declaration, local testing, etc.) can differ significantly.

Various events undertaken under Pillars 3 (capacity building) and 4 (assistance to developing countries)[51] of the ITU C&I Programme made it possible to gather relevant information from 116 countries.[52]

Data research and organization of essential information considered different C&I infrastructure variables, such as:

1) Conformance and interoperability frameworks.
2) ICT standards and technical requirements.
3) Conformance assessment and bodies.
4) Testing laboratories.
5) Quality and metrology.

Figure 1A: C&I legal frameworks from 114 countries that provided information



[51] The source material used for the data research is currently available on the ITU website, from: C&I events; Assessment studies; ITU-D Study Group Question 4/2 inputs as national and regional case studies.
[52] ITU-D SG2 Document SG2RGQ/274+Annex from the BDT Focal Point for Question 4/2.

The figure above displays the number of C&I country frameworks per region from 116 countries: 115 countries indicated the existence of a legal document and a level of procedure for accepting ICT products in their markets (importation fees and taxes not included); only one country, in the Americas region, indicated the absence of any legal procedures for ICT products.

The complete dataset display is a work-in-progress, and complete analysis will be provided through the ITU-C&I development portal (https://itu.int/go/ci_development).

Annex 2: Counterfeiting – a survey of national frameworks and practices

The annual ITU World Telecommunication/ICT Regulatory Survey (edition 2019) included data on regulatory practices related to the distribution and use of counterfeit ICTs.

The data series featured are as follows:

1) Responsibilities of telecom/ICT regulators related to ICT counterfeiting.
2) Types of counterfeit ICTs overseen by the telecom/ICT regulator.
3) Policy/legislation/regulation related to ICT counterfeiting adopted.
4) Areas covered in ICT counterfeiting regulations.
5) Plans to adopt a regulatory framework for ICT counterfeiting.[53]

Table 1A: Summary of ITU World Telecommunication/ICT Regulatory Survey (edition 2019): Survey on regulatory practices related to the distribution and use of counterfeit ICTs

Summary								
Question	Answer	Africa	Arab States	Asia & Pacific	CIS	Europe	The Americas	Total
Does the Telecom/ICT regulator (or the entity in charge of regulation in the sector) have responsibilities related to ICT counterfeiting (e.g., fake mobile phones, smartphones, computers, any network or other computing equipment components)?	Yes	23	12	10	0	9	11	**65**
	No	10	3	10	2	28	14	**67**
Has your country adopted any policy/legislation/regulation related to ICT counterfeiting?	Yes	23	11	7	2	14	14	**71**
	No	10	5	15	3	20	12	**65**
If no, are there plans to adopt a regulatory framework for ICT counterfeiting?	Yes	3	3	4	0	3	3	**16**
	No	4	0	8	4	11	5	**32**
Region size		**44**	**22**	**40**	**9**	**46**	**35**	**196**
* This question allows multiple answers per country/economy								
Year: 2019 or latest available data.								
Source: ITU World Telecommunication/ICT Regulatory Database								
ITU ICT-Eye: http://www.itu.int/icteye								

[53] ITU-D SG2 Document SG2RGQ/38+Annex from the BDT Focal Point for Question 3/1.

Figure 2A: Regional distribution of responses from survey – Question 1

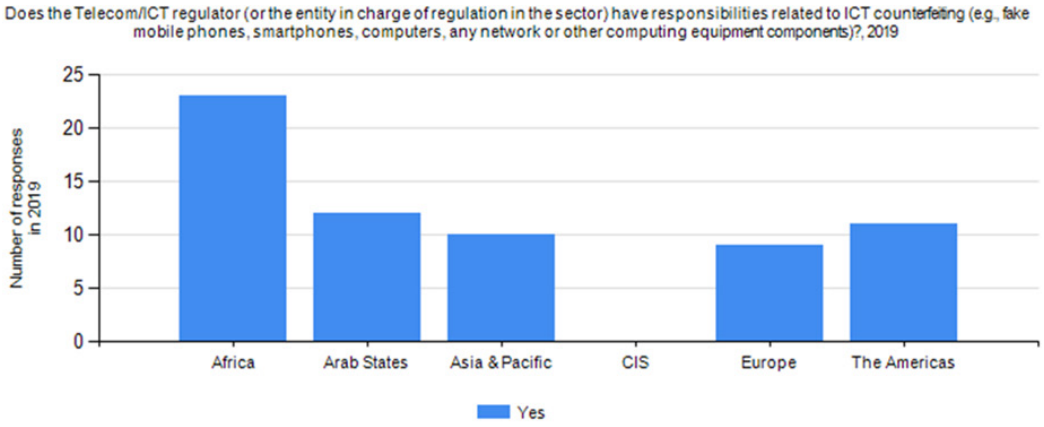


Figure 3A: Regional distribution of responses from survey – Question 2

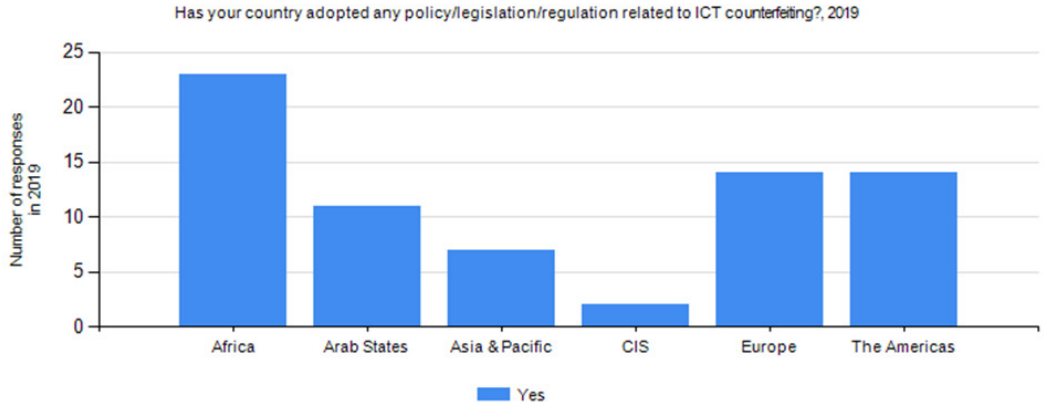
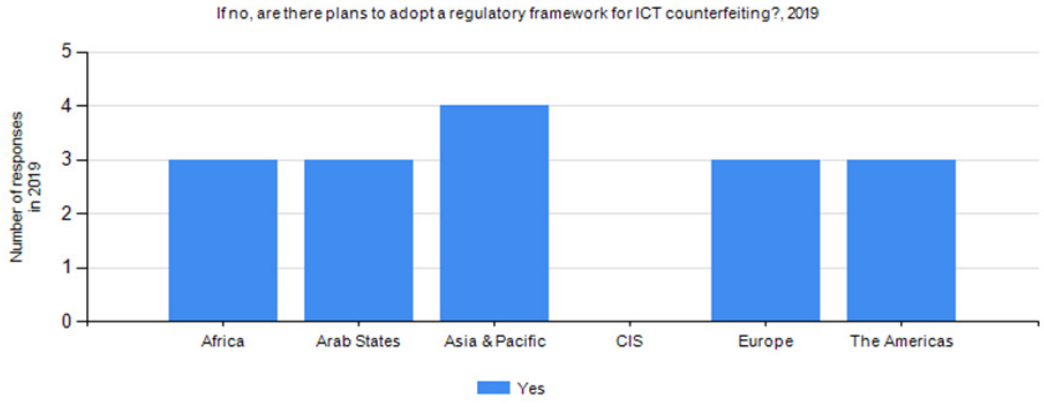


Figure 4A: Regional distribution of responses from survey – Question 3



Annex 3: Initiatives in the fight against equipment counterfeiting and mobile terminal theft in Burundi[54]

A3.1 Introduction

Counterfeiting of mobile phones has numerous negative effects on industry, society, governments and in particular consumers of ICT services. Primarily, it leads to a lower quality of service of mobile telecommunications and safety hazards associated with the use of defective second-hand terminals due to inferior quality or unsuitable technical characteristics.

A3.2 Impact of the proliferation and use of counterfeit mobile terminals

The use of counterfeit mobile terminals by consumers and rising dissatisfaction among mobile subscribers faced with the growing phenomenon of mobile terminal theft has undesirable consequences in the short and long term, including:

- Lowering the QoS of mobile telecommunication services, which in turn has an impact on the experience of consumers and businesses.
- Compromising the security of digital transactions and that of mobile terminal users.
- Increasing evasion from applicable taxes and duties, which has a negative effect on tax revenues.
- Creating risks to the environment and consumer health due to the use of hazardous substances recovered from waste electrical and electronic equipment (WEEE).
- Facilitating the drugs trade, terrorism and other local, regional and international criminal activity.
- Infringing on manufacturers' trademarks.
- Significantly affecting the ICT market by proposing poor-quality, low-cost products that tend to have a greatly reduced lifetime, whence the accumulation of WEEE.

A3.3 National initiatives in the fight against mobile terminal theft and equipment counterfeiting

To combat the use of counterfeit terminals more effectively, the *Agence de régulation et de contrôle des télécommunications* (ARCT) (Telecommunication Regulatory and Control Agency of Burundi) has instituted the following measures:

1) Creation of certification procedures for telecommunication equipment.
2) Registration of the characteristics of telecommunication equipment.
3) Issuance of import certificates for vendors of telecommunication equipment.
4) Enforcement of the requirement that telecommunication equipment vendors be licensed and display their vendor's licence on the establishment's walls, that terminals be certified by ARCT, and that equipment be guaranteed for at least six months.
5) Regular inspections to verify compliance and respect of technical standards and regulations.
6) Creation of a toll-free number (151) for members of the public to report telephone sales where there is a problem with the IMEI number of the phone and that on the package.
7) Organization of public awareness campaigns on the dangers of using counterfeit mobile terminals.

[54] ITU-D SG2 Document 2/390 from Burundi [in French].

8) Inspection of electronic communication terminal equipment in use by public and private organizations.
9) Inspection of providers of value-added services who use numbering resources.

To combat the use of stolen mobile terminals more effectively, ARCT has initiated the following activities:

1) Registration of all mobile telecommunication service subscribers: ARCT regularly assesses compliance with the circular on the registration of subscribers by the telecommunication operators, in order to combat fraud.
2) Automation of the service for requisitioning expert testimony: A management application for processing and managing requisitions for expert testimony in cases of mobile communication terminal theft has been designed and implemented.
3) Combating theft and crimes committed using mobile telephones: ARCT invites members of the public to report the numbers used to send suspicious messages and to forward them to ARCT for systematic verification and deactivation if necessary.

A3.4 Conclusion

It is crucial to put into action all effective means for combating counterfeit terminals being sold or connected to the telecommunication network, so as to protect the consumers of ICT services. This will also enhance security for users, improve the quality of service of networks and stimulate digital economy and financial growth of the country.

Annex 4: Illustrations for chapters of the Output Report on Question 4/2

The following illustrations summarize concepts for Chapters 2, 3 and 5 of the Output Report.

Definitive, high-level resolution images of the illustrations are available at https://itu.int/go/CI_development.

Figure 5A: Illustration for Chapter 2 – What is conformance and interoperability (C&I)

Figure 6A: Illustration for Chapter 2 – C&I frameworks

Figure 7A: Illustration for Chapter 3 – Combating the proliferation of counterfeit, substandard and tampered devices

Figure 8A: Illustration for Chapter 5 – The Internet of Things and C&I

Annex 5: Ideas for the future of the Question

Having regard to the role of C&I in a hyperconnected world where billions of people and objects connect with each other, the study group's work on C&I could focus on:

- **Efforts to manage the increasing number of devices sharing the same limited resources**
- **Measures to cover costs related to conformity procedures and controls of ICT products to allow only approved products to access markets**
- **Harmonization of procedures and collaboration**
  - Robust C&I frameworks: Making sure every country has or is part of a robust C&I framework at minimal cost (e.g. agreements on the shared use of national C&I infrastructure, such as testing facilities and certificates of conformity).
  - Collaboration: Are MRAs effective tools to pursue in the future? What aspects of MRAs need to be adapted to improve existing collaboration agreements or develop new ones? The group could focus on innovative collaboration structures to improve access to high-quality and safe ICT products.
- **Trends**
  - Future challenges for C&I, such as:
    - New technologies outpacing regulation/testing procedures
    - Regulatory aspects for open RAN and interoperability adoption related to 5G
    - Smart objects able to communicate through ICTs
    - Software tampering/hacking vulnerabilities
    - Effective harmonization of procedures and technical collaboration, etc.
  - Means of prioritizing device/type-approval models to achieve a good balance between trust and control.
  - C&I challenges and opportunities during the COVID-19 pandemic.
  - Ways in which new technologies (such as blockchain and artificial intelligence) can help to improve trust in the international C&I framework and trade in and use of ICT devices.

Annex 6: List of contributions and liaison statements received on Question 4/2

Contributions on Question 4/2

Web	Received	Source	Title
2/423	2021-03-18	Rapporteur for Question 4/2	Proposed liaison statement from ITU-D Study Group 2 Question 4/2 to ITU-T Study Group 11, ITU-R WP1A and WP6A, and ISO/CASCO
2/390	2021-02-03	Burundi	Initiatives de lutte contre les équipements de contrefaçon et le vol des terminaux mobiles au Burundi
RGQ2/277	2020-09-22	Algérie Télécom SPA (Algeria)	Revisions to Draft Chapter 3 for the Final Report of Question 4/2
RGQ2/274 +Ann.1	2020-09-22	BDT Focal Point for Question 4/2	C&I Database – updated summary
RGQ2/269	2020-09-22	Rapporteur for Question 4/2	Draft text for new chapter (Ideas for the Future of the Question) of the Output Report for Question 4/2
RGQ2/265	2020-09-22	Rapporteur for Question 4/2	Draft text for Chapter 1 Section 1.4 on COVID-19 impact to type approval procedures
RGQ2/264	2020-09-22	Kenya	Proposed draft text for Chapter 4 of the Output Report for Question 4/2
RGQ2/233	2020-08-20	Algérie Télécom SPA (Algeria)	Proposed text for Chapter 5: Internet of Things and C&I
2/345	2020-02-11	BDT Focal Point for Question 4/2	ITU Conformance and Interoperability Training Programme
2/337	2020-02-11	Algérie Télécom SPA (Algeria)	Revisions to draft Chapter 3 for the Final Report of Q4/2
2/332 +Ann.1	2020-02-11	Kenya	Device Management System – Kenyan Case
2/326	2020-02-10	Oman	Problem of increasing use of fake IMEI
2/323 (Rev.1)	2020-02-07	Ghana	Achieving quality C&I regimes – Challenges from basic Infrastructure to legislative and regulatory frameworks. The experience of Ghana
2/311	2020-01-28	International Telecommunication Academy (Russian Federation)	Regulation on the system to confirm the compliance of communication facilities and services with the ITU standard
2/290	2020-01-08	Mauritania	Mauritania (Islamic Republic of)
2/261	2019-12-24	Guinea	Conformance and interoperability (C&I)

(continuación)

Web	Received	Source	Title
2/257	2019-12-20	Mauritania	Proposed draft text for Chapter 2 of the Final Report for Question 4/2
2/250	2019-12-08	Comoros	Progress of activities for implementing conformance and interoperability programmes in the Union of the Comoros
RGQ2/194 +Ann.1	2019-09-24	BDT Focal Point for Question 4/2	ITU Conformity and Interoperability Training Programme (CITP)
RGQ2/171	2019-09-18	Algérie Télécom SPA (Algeria)	Implementation of Plenipotentiary Conference (PP-18) Resolution 177 (Rev. Dubai, 2018)
RGQ2/170	2019-09-15	Mauritania	Conformité et interopérabilité des équipements TIC dans les pays en développement: normes et procédures – cas de la Mauritanie
RGQ2/144	2019-08-20	Central African Republic	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment and theft of mobile devices
RGQ2/139	2019-08-06	Guinea	Assistance to developing countries for implementing conformance and interoperability (C&I) programmes and combating counterfeit ICT equipment
2/TD/24	2019-03-29	Rapporteur for Question 4/2	Proposed outgoing liaison statements from Q4/2
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/210	2019-03-12	BDT Focal Point for Question 4/2	C&I Programme – Pillars 3 & 4 implementation report
2/202 +Ann.1	2019-03-08	BDT Focal Point for Question 4/2	Summary on national C&I topics
2/177	2019-02-07	Rapporteur for Question 4/2	Draft Chapter 3 for Final Report on Question 4/2
2/166	2019-02-06	Mexico	Regulatory obligations to help combat the theft of mobile devices

(continuación)

Web	Received	Source	Title
2/149	2019-01-24	Guinea	Assistance to developing countries for implementing conformance and interoperability programmes, portability and combating counterfeit ICT equipment and theft of mobile devices
2/142	2019-01-16	Madagascar	Implementing conformance and interoperability programmes
2/133	2019-01-10	Comoros	Realization of a programme for assistance to developing countries for implementing conformance and interoperability programmes: case of Union of the Comoros
RGQ2/TD/8	2018-09-25	South Sudan	Challenges and proposals to deal with counterfeit ICT equipment and mobile device theft in South Sudan and region
RGQ2/TD/7	2018-10-01	Russian Federation	ITU-D SG1 and SG2 coordination: Mapping of ITU-D Study Group 1 and 2 Questions
RGQ2/86 +Ann.1	2018-09-18	BDT Focal Point for Question 4/2	ITU C&I programme: implementation update
RGQ2/85	2018-09-18	Zimbabwe	Actions to combat counterfeit and theft of mobile devices in Zimbabwe
RGQ2/82	2018-09-18	Ghana	Ghana's Type Approval Regime – a sustainable approach to connecting and protecting users of telecommunications/ICTs and networks through conformance assessment
RGQ2/80	2018-09-18	GSM Association	GSMA's IMEI database and services
RGQ2/69	2018-09-17	Rwanda	Regional effort to fight illegal devices, improve the quality of services and minimize health hazard to consumers
RGQ2/66 (Rev.1)	2018-09-16	Senegal	Lutte contre la contrefaçon et le vol de téléphone
RGQ2/38 +Ann.1	2018-08-18	BDT Focal Point for Question 3/1	ITU data on regulatory practices related to counterfeit ICTs
RGQ2/9 (Rev.1)	2018-07-05	Guinea	Implementing conformance and interoperability programmes and combating counterfeit ICT equipment and theft of mobile devices
2/TD/10	2018-05-10	Rapporteur for Question 4/2	Draft reply liaison statements from ITU-D Study Group 2 Question 4/2

(continuación)

Web	Received	Source	Title
2/TD/8	2018-05-09	Rapporteur for Question 4/2	Draft work plan, Table of Contents (ToC) and responsibilities for ITU-D Question 4/2
2/97 (Rev.1)	2018-05-06	Chairman, ITU-D Study Group 2	List of proposed Rapporteurs and Vice-Rapporteurs of ITU-D Study Group 2 study Questions for the 2018-2021 period
2/92 +Ann.1	2018-04-24	BDT Focal Point for Question 4/2	ITU C&I Programme status – Pillars 3 and 4
2/90	2018-04-24	Mauritania	Draft work plan for ITU-D Study Group 2 Question 4/2
2/88 +Ann.1	2018-04-23	BDT	Implementation of ITU C&I Programme and ITU-T activities on combatting counterfeiting and stolen ICT devices
2/83	2018-04-23	Iran University of Science and Technology (Islamic Republic of Iran)	HAMTA: A system for combating counterfeit ICT equipment and theft of mobile devices
2/58	2018-03-22	Algérie Télécom SPA (Algeria)	Conformance and interoperability
2/45	2018-03-12	Madagascar	Monitoring counterfeit terminal devices, building a healthy network that brings in revenues for the Stat

Incoming liaison statements for Question 4/2

Web	Received	Source	Title
RGQ2/219	2020-08-06	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/205 +Ann.1-2	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates on the current work at ITU-T Q15/11 "Combating counterfeit and stolen ICT equipment"
RGQ2/204 +Ann.1	2020-03-25	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on contribution on conformance and interoperability
RGQ2/115 +Ann.1	2019-06-14	ITU-T Study Group 5	Liaison statement from ITU-T SG5 to ITU-D SG2 Q4/2 and Q7/2 on work being carried out under study in ITU-T Study Group 5 Question 3/5

(continuación)

Web	Received	Source	Title
RGQ2/113	2019-05-29	ITU-T Study Group 20	Liaison statement from ITU-T SG20 to ITU-D SG2 Q4/2 on SG20 activities on IoT and Smart Cities & Communities
RGQ2/111 +Ann.1-3	2019-04-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/22 +Ann.1-3	2019-03-27	Rapporteur for Question 4/2	Proposed updates to work plan, table of contents and areas of responsibilities, matrix of contributions received and proposal for second focus session
2/TD/19 +Ann.1-3	2019-03-21	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on collaboration
2/TD/17 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on updates to the Technical Report on the Combat of Counterfeit Devices
2/TD/16 +Ann.1	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on creation of new work item on "Reliability of IMEI identifier"
2/TD/15	2019-03-20	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on impact of counterfeit mobile devices on Quality of Service
2/139	2019-01-16	ITU-T Study Group 20	Liaison statement from ITU-T SG20 on SG20 activities on IoT and Smart City & Community
RGQ2/16 +Ann.1-3	2018-08-02	ITU-T Study Group 11	Liaison statement from ITU-T SG11 to ITU-D SG2 Q4/2 on progress and collaboration on the combat of counterfeit and mobile device theft
2/35	2017-12-01	ITU-T Study Group 11	Liaison Statement from ITU-T SG11 to ITU-D SG2 Question 4/2 on ongoing collaboration

Unión Internacional de las Telecomunicaciones (UIT)
Oficina de Desarrollo de las Telecomunicaciones (BDT)
Oficina del Director
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo-e: bdtdirector@itu.int
Tel.: +41 22 730 5035/5435
Fax: +41 22 730 5484

Director Adjunto y Jefe del Departamento de Administración y Coordinación de las Operaciones (DDR)
Place des Nations
CH-1211 Ginebra 20
Suiza

Correo-e: bdtdeputydir@itu.int
Tel.: +41 22 730 5131
Fax: +41 22 730 5484

Departamento de Redes y Sociedad Digitales (DNS)
Correo-e: bdt-dns@itu.int
Tel.: +41 22 730 5421
Fax: +41 22 730 5484

Departamento del Centro de Conocimientos Digitales (DKH)
Correo-e: bdt-dkh@itu.int
Tel.: +41 22 730 5900
Fax: +41 22 730 5484

Departamento de Asociaciones para el Desarrollo Digital (PDD)
Correo-e: bdt-pdd@itu.int
Tel.: +41 22 730 5447
Fax: +41 22 730 5484

África

Etiopía
International Telecommunication Union (ITU)
Oficina Regional
Gambia Road
Leghar Ethio Telecom Bldg. 3rd floor
P.O. Box 60 005
Adis Abeba
Ethiopía

Correo-e: itu-ro-africa@itu.int
Tel.: +251 11 551 4977
Tel.: +251 11 551 4855
Tel.: +251 11 551 8328
Fax: +251 11 551 7299

Camerún
Union internationale des télécommunications (UIT)
Oficina de Zona
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé
Camerún

Correo-e: itu-yaounde@itu.int
Tel.: + 237 22 22 9292
Tel.: + 237 22 22 9291
Fax: + 237 22 22 9297

Senegal
Union internationale des télécommunications (UIT)
Oficina de Zona
8, Route des Almadies
Immeuble Rokhaya, 3e étage
Boîte postale 29471
Dakar – Yoff
Senegal

Correo-e: itu-dakar@itu.int
Tel.: +221 33 859 7010
Tel.: +221 33 859 7021
Fax: +221 33 868 6386

Zimbabwe
International Telecommunication Union (ITU)
Oficina de Zona
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792
Belvedere Harare
Zimbabwe
Correo-e: itu-harare@itu.int
Tel.: +263 4 77 5939
Tel.: +263 4 77 5941
Fax: +263 4 77 1257

Américas

Brasil
União Internacional de Telecomunicações (UIT)
Oficina Regional
SAUS Quadra 6
Ed. Luis Eduardo Magalhães,
Bloco "E", 10º andar, Ala Sul
(Anatel)
CEP 70070-940 Brasilia – DF
Brasil
Correo-e: itubrasilia@itu.int
Tel.: +55 61 2312 2730-1
Tel.: +55 61 2312 2733-5
Fax: +55 61 2312 2738

Barbados
International Telecommunication Union (ITU)
Oficina de Zona
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown
Barbados
Correo-e: itubridgetown@itu.int
Tel.: +1 246 431 0343
Fax: +1 246 437 7403

Chile
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Merced 753, Piso 4
Santiago de Chile
Chile

Correo-e: itusantiago@itu.int
Tel.: +56 2 632 6134/6147
Fax: +56 2 632 6154

Honduras
Unión Internacional de Telecomunicaciones (UIT)
Oficina de Representación de Área
Colonia Altos de Miramontes
Calle principal, Edificio No. 1583
Frente a Santos y Cía
Apartado Postal 976
Tegucigalpa
Honduras
Correo-e: itutegucigalpa@itu.int
Tel.: +504 2235 5470
Fax: +504 2235 5471

Estados Árabes

Egipto
International Telecommunication Union (ITU)
Oficina Regional
Smart Village,
Building B 147, 3rd floor
Km 28 Cairo
Alexandria Desert Road
Giza Governorate
El Cairo
Egipto

Correo-e: itu-ro-arabstates@itu.int
Tel.: +202 3537 1777
Fax: +202 3537 1888

Asia-Pacífico

Tailandia
International Telecommunication Union (ITU)
Oficina Regional
Thailand Post Training Center, 5th floor
111 Chaengwattana Road
Laksi
Bangkok 10210
Tailandia

Dirección postal:
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210, Tailandia
Correo-e: ituasiapacificregion@itu.int
Tel.: +66 2 575 0055
Fax: +66 2 575 3507

Indonesia
International Telecommunication Union (ITU)
Oficina de Zona
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10110
Indonesia

Dirección postal:
c/o UNDP – P.O. Box 2338
Jakarta 10110, Indonesia
Correo-e: ituasiapacificregion@itu.int
Tel.: +62 21 381 3572
Tel.: +62 21 380 2322/2324
Fax: +62 21 389 55521

Países de la CEI

Federación de Rusia
International Telecommunication Union (ITU)
Oficina Regional
4, Building 1
Sergiy Radonezhsky Str.
Moscú 105120
Federación de Rusia

Correo-e: itumoscow@itu.int
Tel.: +7 495 926 6070

Europa

Suiza
Unión Internacional de las Telecomunicaciones (UIT)
Oficina Regional
Place des Nations
CH-1211 Ginebra 20
Suiza
Correo-e: eurregion@itu.int
Tel.: +41 22 730 5467
Fax: +41 22 730 5484

Unión Internacional de Telecomunicaciones
Oficina de Desarrollo de las Telecomunicaciones
Place des Nations
CH-1211 Ginebra 20
Suiza

ISBN: 978-92-61-34133-6

9 789261 341336

Publicado en Suiza
Ginebra, 2021