Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Q.5050

(03/2019)

SERIE Q: CONMUTACIÓN Y SEÑALIZACIÓN, Y MEDICIONES Y PRUEBAS ASOCIADAS

Lucha contra la falsificación y el robo de dispositivos TIC

Solución marco para contrarrestar la falsificación de dispositivos TIC

Recomendación UIT-T Q.5050

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN, Y MEDICIONES Y PRUEBAS ASOCIADAS

SEÑALIZACIÓN EN EL SERVICIO MANUAL INTERNACIONAL	Q.1–Q.3
EXPLOTACIÓN INTERNACIONAL SEMIAUTOMÁTICA Y AUTOMÁTICA	Q.4–Q.59
FUNCIONES Y FLUJOS DE INFORMACIÓN PARA SERVICIOS DE LA RDSI	Q.60–Q.99
CLÁUSULAS APLICABLES A TODOS LOS SISTEMAS NORMALIZADOS DEL UIT-T	Q.100–Q.119
ESPECIFICACIONES DE LOS SISTEMAS DE SEÑALIZACIÓN N.° 4, 5, 6, R1 Y R2	Q.120–Q.499
CENTRALES DIGITALES	Q.500–Q.599
INTERFUNCIONAMIENTO DE LOS SISTEMAS DE SEÑALIZACIÓN	Q.600–Q.699
ESPECIFICACIONES DEL SISTEMA DE SEÑALIZACIÓN N.° 7	Q.700–Q.799
INTERFAZ Q3	Q.800–Q.849
SISTEMA DE SEÑALIZACIÓN DIGITAL DE ABONADO N.° 1	Q.850–Q.999
RED MÓVIL TERRESTRE PÚBLICA	Q.1000–Q.1099
INTERFUNCIONAMIENTO CON SISTEMAS MÓVILES POR SATÉLITE	Q.1100–Q.1199
RED INTELIGENTE	Q.1200–Q.1699
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA IMT-2000	Q.1700–Q.1799
ESPECIFICACIONES DE LA SEÑALIZACIÓN RELACIONADA CON EL CONTROL DE LLAMADA INDEPENDIENTE DEL PORTADOR	Q.1900–Q.1999
RED DIGITAL DE SERVICIOS INTEGRADOS DE BANDA ANCHA (RDSI-BA)	Q.2000–Q.2999
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA LAS REDES DE PRÓXIMA GENERACIÓN (NGN)	Q.3000–Q.3709
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA LAS REDES DEFINIDAS POR SOFTWARE (SDN)	Q.3710–Q.3899
ESPECIFICACIONES DE PRUEBAS	Q.3900–Q.4099
REQUISITOS Y PROTOCOLOS DE SEÑALIZACIÓN PARA LAS REDES IMT-2020	Q.5000–Q.5049
LUCHA CONTRA LA FALSIFICACIÓN Y EL ROBO DE DISPOSITIVOS TIC	**Q.5050–Q.5069**

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Q.5050

Solución marco para contrarrestar la falsificación de dispositivos TIC

Resumen

En los últimos años se ha producido un incremento en la utilización de equipos de tecnología de la información y la comunicación (TIC) en la vida cotidiana, pero también ha habido efectos secundarios indeseados relacionados con el aumento de la venta, circulación y utilización de dispositivos TIC falsificados en el mercado.

Un dispositivo TIC falsificado es un producto que explícitamente infringe marcas registradas, copia diseños de *hardware* o *software*, o infringe los derechos de marca o embalaje de un producto original o auténtico y que, por lo general, infringe normas técnicas nacionales y/o internacionales aplicables, requisitos reglamentarios o procesos de conformidad, acuerdos de licencia de fabricación u otros requisitos jurídicos aplicables.

Entre los diversos tipos de dispositivos TIC utilizados hoy en día, los teléfonos inteligentes y otros dispositivos móviles se han convertido en omnipresentes y atractivos para la población mundial, entrando así en el punto de mira del mercado negro/gris mundial.

Las consecuencias negativas para los diversos interesados, como los usuarios, los operadores de redes, los fabricantes de dispositivos originales, los comerciantes y los gobiernos, son, entre otras, la disminución de la protección de la seguridad y de la calidad del servicio para los usuarios y, para ciertos interesados, la pérdida de ingresos.

Dado que la economía de la oferta y la demanda de dispositivos TIC falsificados dificulta los intentos de acabar con el mercado mundial de la falsificación, no existe una solución única que pueda resolver el problema por sí sola, por lo que es preciso adoptar un planteamiento global que integre un amplio abanico de medidas.

Por consiguiente, la Recomendación UIT-T Q.5050 tiene por objeto describir un marco de referencia en el que se expongan las dificultades y requisitos generales que se han de tomar en consideración a la hora de desplegar soluciones para contrarrestar la circulación y utilización de dispositivos TIC falsificados.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T Q.5050	15-03-2019	11	11.1002/1000/13702

Palabras clave

Contrarrestar la falsificación de dispositivos TIC, cumplimiento de la normativa, conformidad, evaluación de la conformidad, marco, requisitos, seguridad, normas, identificadores únicos.

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T Q.5050

Solución marco para contrarrestar la falsificación de dispositivos TIC

1 Alcance

En la presente Recomendación se describen el marco de referencia y los requisitos que deben tomarse en consideración a la hora de desplegar soluciones para contrarrestar la circulación y utilización de dispositivos de tecnología de la información y la comunicación (TIC) falsificados.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones, y demás referencias, son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación a que utilicen la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en el marco de esta Recomendación no le confiere carácter de Recomendación.

Ninguna.

3 Definiciones

3.1 Términos definidos en otros documentos

En la presente Recomendación se utilizan los siguientes términos definidos en otros documentos:

3.1.1 evaluación de la conformidad [b-ISO/CEI 17000]: demostración de que se cumplen los requisitos especificados para un producto, proceso, sistema, persona u organismo.

3.1.2 plan (o programa) de evaluación de la conformidad [b-ISO/CEI 17000]: sistema de evaluación de la conformidad para determinados objetos de evaluación de la conformidad a los que se aplican los mismos requisitos, reglas y procedimientos específicos.

3.1.3 vigilancia del mercado [b-CE-Reglamento]: actividades realizadas y medidas adoptadas por los poderes públicos para garantizar que los productos cumplen las prescripciones establecidas en la legislación pertinente y no son perjudiciales para la salud, la seguridad o cualquier otro aspecto de la protección del interés público.

3.1.4 norma [b-OMC-OTC]: documento aprobado por un organismo reconocido que establece, para una utilización común y reiterada, normas, directrices o características para productos o sus procesos y métodos de producción conexos, cuyo cumplimiento no es obligatorio. También puede incluir o tratar exclusivamente de los requisitos de terminología, símbolos, embalaje, marcado o etiquetado aplicables a un producto, proceso o método de producción.

3.1.5 vigilancia [b-ISO/CEI 17000]: iteración sistemática de las actividades de evaluación de la conformidad con el fin de mantener la validez de la declaración de conformidad.

3.1.6 obstáculos técnicos al comercio (OTC) [b-OMC-OTC]: el Acuerdo sobre Obstáculos Técnicos al Comercio de la Organización Mundial del Comercio (OMC) tiene por objeto garantizar que los reglamentos técnicos, las normas y los procedimientos de evaluación de la conformidad no sean discriminatorios ni creen obstáculos innecesarios al comercio.

3.1.7 reglamentación técnica [b-OMC-OTC]: documento que establece las características del producto o sus procesos y métodos de producción conexos, incluidas las disposiciones administrativas aplicables, cuyo cumplimiento es obligatorio. También puede incluir o tratar exclusivamente de los requisitos de terminología, símbolos, embalaje, marcado o etiquetado aplicables a un producto, proceso o método de producción.

3.1.8 mercado gris [b-Gartner]: importación y venta de dispositivos fuera de los canales comerciales ordinarios definidos por el fabricante original o el gobierno pertinente, creando así un mercado paralelo a los canales de distribución autorizados.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 dispositivo TIC falsificado: dispositivo de tecnología de la información y la comunicación (TIC) que explícitamente infringe marcas registradas, copia diseños de *hardware* o *software*, o infringe los derechos de marca o embalaje de un producto original o auténtico y que, por lo general, infringe normas técnicas nacionales y/o internacionales aplicables, requisitos reglamentarios o procesos de conformidad, acuerdos de licencia de fabricación u otros requisitos jurídicos aplicables.

3.2.2 dispositivo TIC alterados: dispositivo de tecnología de la información y la comunicación (TIC) en el que se han alterado o tratado de alterar, sin el consentimiento explícito del fabricante o su representante legal, sus componentes, *software*, identificador único, elementos protegidos por derechos de propiedad intelectual o marcas registradas.

3.2.3 identificador único: identificador asociado a un único dispositivo cuyo objetivo es identificarlo de forma exclusiva.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos:

ADPIC Aspectos de los derechos de propiedad intelectual relacionados con el comercio

DevID Identificador de dispositivo (*device identifier*)

DIRBS Sistema de identificación, registro y bloqueo de dispositivos (*device identification, registration, and blocking system*)

DPI Derechos de propiedad intelectual

EAP Protocolo de autenticación extensible (*extensible authentication protocol*)

IMEI Identidad internacional de equipos móviles (*international mobile equipment identity*)

IoT Internet de las cosas (*Internet of things*)

IVR Respuesta vocal interactiva (*interactive voice response*)

OTC Obstáculo técnico al comercio

PCB Placa de circuitos impresos (*printed circuit board*)

PEC Plan de evaluación de la conformidad

RIE Registro de identidades de equipos

SIM Módulo de identificación de abonado (*subscriber identification module*)

TAC Código de asignación de tipo (*type allocation code*)

TEE Entorno de ejecución de confianza (*trusted execution environment*)

TIC Tecnología de la información y la comunicación

TPM Módulo de plataforma de confianza (*trusted platform module*)

5 Convenios

La presente Recomendación aplica las siguientes formas verbales de expresión del grado de obligatoriedad de las disposiciones:

a) La expresión "se requiere" indica que el requisito es absolutamente obligatorio y debe aplicarse sin excepción si se pretende declarar la conformidad con esta Recomendación.

b) La expresión "se recomienda" indica que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

c) La expresión "se tiene la opción de" u "opcionalmente" indica que el requisito se permite, sin que ello signifique que se recomiende. Esta expresión no implica que el fabricante deba ofrecer la opción correspondiente, que puede ser habilitada de manera opcional por el operador de red/proveedor de servicios. Significa, más bien, que el fabricante tiene la opción de proporcionar esta función sin que ello afecte a la conformidad con la presente Recomendación.

6 Consideraciones generales

En los últimos años se ha producido un incremento en la utilización de dispositivos TIC en la vida cotidiana, pero también ha habido efectos secundarios indeseados relacionados con el aumento de la venta, circulación y utilización de dispositivos TIC falsificados en el mercado. Las consecuencias negativas para los diversos interesados, como los usuarios, los operadores de redes, los fabricantes de dispositivos originales, los comerciantes y los gobiernos, son, entre otras, la disminución de la protección de la seguridad y de la calidad del servicio para los usuarios y, para ciertos interesados, la pérdida de ingresos.

Se reconoce que la economía de la oferta y la demanda de dispositivos TIC falsificados dificulta los intentos de acabar con el mercado negro/gris mundial y que ninguna solución única contra la falsificación puede ser una panacea. En la presente Recomendación se propone un marco integrado por un amplio abanico de medidas que pueden adoptarse y aplicarse con el contexto de un planteamiento general para resolver este problema. También se debe abordar este problema en el origen de los productos falsificados, es decir en los mercados donde se fabrican y exportan, con la ayuda de los países en los que se venden.

Diferenciar los dispositivos TIC auténticos de los falsificados puede resultar particularmente difícil para cualquiera que inspeccione o pruebe un producto, ya que los falsificadores procuran crear productos muy similares a los dispositivos auténticos y aportan documentación falsa u original robada, incluyen a veces *hardware* procedente del producto original o de sus accesorios e incluso copian el *software* legítimo o los identificadores únicos, todo ello con el fin de dificultar la identificación por los interesados. Es fundamental que se tengan en cuenta éstos y otros factores a la hora de desplegar soluciones, para evitar que éstas causen más problemas a los usuarios y a los fabricantes de los que se pretende resolver.

Entre los diversos tipos de dispositivos TIC utilizados hoy en día, los teléfonos inteligentes y otros dispositivos móviles se han convertido en omnipresentes y atractivos para la población mundial, entrando así en el punto de mira del mercado negro/gris mundial. En respuesta al problema de la falsificación de dispositivos TIC, algunos países han adoptado medidas y aplicado soluciones satisfactorias para disuadir la circulación y utilización de dispositivos TIC falsificados, mientras que otros países no saben cómo actuar y no tienen claro cuáles son las mejores estrategias.

Muchas de las soluciones adoptadas para neutralizar la utilización de dispositivos TIC falsificados tienen ciertas similitudes, como identificadores únicos de dispositivos, la ayuda de un régimen de evaluación de la conformidad y mecanismos para impedir el acceso a la red por estos dispositivos fraudulentos (como se propone para los dispositivos móviles en el Anexo A).

Sin embargo, sigue habiendo gobiernos de todo el mundo con dificultades para contrarrestar la falsificación de dispositivos TIC por diferentes razones, como los aspectos técnicos, los esfuerzos de los falsificadores por evitar y eludir la detección y el gran atractivo que estos productos tienen para los consumidores, que los incita a comprar voluntariamente productos falsificados.

Por consiguiente, los países que opten por contrarrestar la falsificación de dispositivos TIC deben considerar la posibilidad de aplicar planteamientos globales en los que intervengan múltiples partes y organismos, así como soluciones tecnológicas adoptadas en otros países que ya se ocupan de la cuestión, a fin de obtener orientación y ejemplos de prácticas óptimas.

7 Fundamentos de un mercado ordenado de equipos de telecomunicaciones

Son muchos los factores que fomentan la creación de un mercado ordenado de productos y servicios de telecomunicaciones. El más importante es establecer requisitos técnicos sólidos para los productos que entran al mercado. Estos factores se refieren, entre otras cosas, a la seguridad del personal, tanto de la comunidad de usuarios como del proveedor de servicios de red, y a la creación de un entorno sin interferencias para los servicios de telecomunicaciones.

Los servicios sin interferencias (inalámbricos y alámbricos) fomentan el desarrollo económico de una sociedad, ya que la participación en la economía digital mundial exige plataformas de telecomunicaciones sólidas, seguras y fiables en las que tenga lugar la actividad económica. Además, un régimen de acceso al mercado bien definido, bien gestionado, no discriminatorio y transparente inspira confianza en los proveedores de equipos, los proveedores de servicios y las personas en general. Este régimen, respaldado por un marco legislativo y reglamentario adecuado, constituye un componente fundamental para ofrecer conectividad nacional e internacional con la calidad necesaria, aspecto éste fundamental para la participación en la economía digital mundial. De hecho, este régimen se corresponde realmente con las prioridades y los valores de una sociedad.
[b-UIT-D-CI-Directrices].

8 Consideraciones relativas al despliegue de soluciones para contrarrestar la falsificación de dispositivos TIC

Las partes interesadas deben afrontar varios retos a la hora de desplegar soluciones para contrarrestar la falsificación de dispositivos TIC:

8.1 Detección e identificación de dispositivos TIC falsificados

Uno de los objetivos del falsificador es lograr que su producto se venda en mercados de todo el mundo. Los falsificadores harán todo lo posible para que su producto se parezca lo más posible al auténtico original, desde el aspecto visual, la copia de identificadores únicos, el *software* hasta incluso los componentes internos de los dispositivos TIC.

Esto presenta algunas dificultades. Por ejemplo, todos los identificadores creados por fabricantes auténticos de bienes pueden y son utilizados de forma abusiva por los falsificadores para lograr su objetivo de hacer creer al consumidor y a las autoridades que su producto es auténtico. Cualquier mecanismo de identificación, y su seguridad inherente, puede convertirse en un objetivo para los falsificadores y delincuentes. Los logotipos e iconos de las homologaciones, así como los identificadores electrónicos, a menudo se subvierten deliberadamente o incluso se dejan en blanco para que se programen luego en los mercados locales, a fin de eludir los controles aduaneros y policiales en las fronteras. [b-UIT-T TR-Falsificación]

Por ejemplo, todos los identificadores creados por fabricantes auténticos de bienes pueden ser alterados por los falsificadores para lograr su objetivo de hacer creer al consumidor y a las autoridades que su producto es auténtico. Este es un problema en muchas industrias, no sólo en las TIC. El lector debe tener en cuenta que cualquier mecanismo de identificación y su seguridad inherente se convertirán en un objetivo para los falsificadores y delincuentes. [b-UIT-T TR-Falsificación]

Por ejemplo, una práctica común de los falsificadores es manipular los identificadores únicos que algunos dispositivos utilizan para autentificarse en la red de manera que ésta reconozca los dispositivos TIC falsificados como si fueran auténticos. Otra práctica consiste en interceptar dispositivos auténticos y manipular su *software* para que parezca una versión mejorada (y más cara) o incluso cambiar las piezas auténticas internas, como las baterías, por versiones falsificadas para vender las piezas auténticas en el mercado.

Los logotipos e iconos de las homologaciones, así como los identificadores electrónicos, a menudo se subvierten deliberadamente para eludir los controles aduaneros y policiales en las fronteras. Esto crea problemas prácticos para los fabricantes, los consumidores, los funcionarios de aduanas y las fuerzas del orden, a quienes resulta difícil distinguir entre marcas de identificación falsas de los equipos falsificados y las de los auténticos, incluso antes de examinar el producto en sí.

8.2 Seguimiento de productores y traficantes de dispositivos TIC falsificados

Cuando se identifica un dispositivo irregular, los agentes involucrados deben rastrear el país de origen, los productores y traficantes de los dispositivos ilícitos y eliminar a los productores y traficantes del mercado [b-OCDE].

Sin medidas eficaces de identificación y observancia de la ley contra los productores y traficantes en los países de procedencia, las medidas que se adopten en las economías de destino podrían ser ineficaces.

8.3 Eliminación de los dispositivos TIC falsificados utilizados en el mercado

El control postventa de los dispositivos TIC falsificados depende de las oportunidades que surjan de actuar en consecuencia. Entre las posibles medidas potenciales cabe citar: i) la detección y verificación, física o remota, de las características del producto original; ii) el cese de su utilización; y/o iii) la incautación del artículo.

Estas oportunidades y acciones presentan varios retos:

– Son pocas las oportunidades de verificar físicamente un artículo: durante un servicio de reparación, un evento de vigilancia del mercado o en situaciones donde una autoridad jurídica tenga derecho a verificar el dispositivo. La dificultad radica en despertar el interés y crear los conocimientos necesarios en los organismos para llevar a cabo esas tareas.

– La verificación podría realizarse de forma lógica o remota, por ejemplo, cotejando los identificadores únicos y huellas de productos durante algún tipo de registro en línea del sistema; sin embargo, para ello se requiere generalmente una conexión a Internet, lo que puede resultar difícil en entornos remotos o rurales, en particular en los países en desarrollo. Aunque deben intervenir procesos electrónicos, es necesario poder contrastar las características físicas con la información contenida en las bases de datos del producto.

– Si el dispositivo utiliza un identificador único para registrarse en la red, se podría impedir el registro de dispositivos TIC falsificados utilizando una base de datos que contenga los dispositivos autorizados para funcionar en un determinado mercado. La dificultad estriba en construir y mantener el sistema de registro y la base de datos, especialmente si ya se ha desplegado un número considerable de dispositivos sin este tipo de control.

– Debe procurarse evitar el abuso de los sistemas de identificación y registro, respetar los derechos del consumidor y no afectar negativamente al usuario de los dispositivos TIC. También debe protegerse al consumidor contra la desconexión arbitraria de la red.

– La incautación de dispositivos TIC falsificados está supeditada a la verificación física y, en la mayoría de los casos, implicará o requerirá la intervención de las fuerzas del orden, con arreglo al marco jurídico que prevé las actuaciones judiciales aplicables. Lo difícil en este caso es lograr la cooperación entre los diferentes organismos, definir un marco jurídico y determinar la responsabilidad por los dispositivos TIC falsificados.

– No hay que subestimar las repercusiones para el usuario. Debe tenerse en cuenta que desconectar dispositivos no está permitido en algunos países y puede poner en peligro la vida del usuario.

8.4 Restricciones a la importación, circulación y venta de nuevos dispositivos TIC falsificados en el mercado

Deben aplicarse medidas que limiten la importación, el contrabando, la circulación y la venta de nuevos dispositivos TIC falsificados en el mercado, además de las medidas destinadas a eliminar los que están inventariados o ya se utilizan.

Esta solución puede contribuir a reducir la presencia general de dispositivos TIC falsificados en el mercado, con sujeción a las limitaciones financieras y de tiempo de la administración que decida adoptar estas medidas y, además, las repercusiones para el usuario final son menores, en comparación con la desconexión de los dispositivos TIC falsificados.

Como se indica en la cláusula 8.2, estas medidas también deberían centrarse en los orígenes del dispositivo TIC falsificado.

8.5 Diferenciación entre dispositivos TIC auténticos y falsificados

Para garantizar la eficacia de las medidas destinadas a eliminar los dispositivos TIC falsificados desplegados en el mercado y disuadir la entrada de nuevos dispositivos, es necesario aplicar soluciones y criterios que permitan diferenciar los dispositivos auténticos de los falsificados. Es indispensable actuar con gran precisión, incluso al examinar identificadores únicos clonados, de modo que las acciones perturbadoras se adopten preferiblemente mediante sistemas automatizados o, para un número reducido de dispositivos TIC, manualmente.

A la hora de diferenciar entre dispositivos TIC auténticos y falsificados, deben tenerse en cuenta los siguientes aspectos:

– El objetivo del falsificador es crear un producto que se parezca mucho al producto auténtico original.

– El falsificador puede tratar activamente de despistar la inspección proporcionando documentación, *hardware* y *software* falsos o robados para disimular que se trata de un producto falsificado.

– Algunos aspectos del producto falsificado pueden provenir de un producto genuino y sus accesorios, por ejemplo: *software*, identificadores únicos, *hardware* exterior, diseño de la placa de circuitos impresos (PCB) y microcircuitos.

– Los productos originales son objeto de actualizaciones periódicas del *software* del fabricante (*firmware*), principalmente por razones de seguridad. También se actualizan las aplicaciones y algunos accesorios. La "huella" del dispositivo correspondiente a un producto genuino puede resultar difícil de verificar.

– Muchas veces, no basta la inspección visual para determinar si el dispositivo es genuino y podrían ser necesario recurrir a expertos, asistencia técnica o pruebas de laboratorio.

8.6 Reducción de las repercusiones para los fabricantes de dispositivos TIC auténticos

Las soluciones utilizadas para contrarrestar la falsificación de dispositivos TIC deben reducir en la medida de lo posible las repercusiones para los fabricantes de dispositivos TIC auténticos y concentrarse en los dispositivos falsificados de TIC, los productores y los traficantes de esos productos.

Por consiguiente, deben evitarse los sistemas que supongan para el fabricante legítimo un coste adicional en la fabricación y eliminación de dispositivos auténticos, por cuanto con ello beneficia involuntariamente al falsificador, que por lo general cuenta con precios más económicos para lograr que el consumidor se decida voluntariamente por el dispositivo TIC falsificado.

8.7 Reducción de la incidencia en el usuario final al considerar la posibilidad de eliminar dispositivos TIC falsificados

Toda solución que se adopte para eliminar o desconectar los dispositivos TIC falsificados debe examinarse meticulosamente a fin de determinar las repercusiones para el usuario final y, cuando se disponga de múltiples opciones para lograr el mismo resultado, adoptar la que afecte menos al consumidor.

Por lo tanto, se deben considerar las siguientes dificultades:

– En algunos países no está permitido desconectar dispositivos TIC.

– No siempre es posible contactar al usuario a través del dispositivo antes de desconectarlo (por ejemplo, dispositivos de sólo datos o SMS, desvío de llamadas, sistemas de respuesta vocal interactiva (IVR), que no tengan contacto con el usuario).

– Bloquear dispositivos TIC falsificados utilizados en actividades importantes puede tener consecuencias graves (por ejemplo, aplicaciones médicas o servicios financieros, entre otros).

– Se ha de velar por que no se vulneren los derechos de los usuarios y por que toda actuación se lleve a cabo de conformidad con la legislación nacional.

8.8 Información al consumidor

Debe informarse al consumidor sobre las cuestiones relacionadas con la compra y utilización prolongada de dispositivos TIC falsificados, en particular de los riesgos potenciales para la salud y/o la pésima calidad del servicio.

Debe tenerse en cuenta que, a pesar de las posibles consecuencias, los consumidores suelen tomar voluntariamente la decisión de comprar productos falsificados por su precio, por lo que resulta fundamental sensibilizar al consumidor sobre las repercusiones negativas de utilizar TIC falsificadas y las ventajas de los dispositivos auténticos.

8.9 Eliminación de obstáculos técnicos al comercio (OTC)

Hay que extremar las precauciones para no impedir la importación y utilización de dispositivos TIC genuinos, lo que constituiría un obstáculo técnico al comercio (OTC), conforme a lo estipulado en el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio (ADPIC) de la Organización Mundial del Comercio (OMC) [b-Acuerdo sobre los ADPIC].

Por ejemplo, la utilización de "listas blancas" podría impedir, por error o por una mala decisión de diseño, la utilización de un dispositivo TIC por los usuarios legítimos, incluidos los viajeros y turistas. La obligación de registrar dispositivos podría crear inadvertidamente un OTC.

9 Requisitos marco

Al desplegar una solución para contrarrestar los dispositivos TIC falsificados, los países deben tener en cuenta los siguientes requisitos:

9.1 Identificación y medidas represivas contra productores y traficantes de dispositivos falsificados

A la vez que se lucha contra la utilización de dispositivos TIC falsificados que se despliegan en el mercado o que entran en el país, es necesario instaurar un proceso para rastrear el origen y eliminar del mercado a los productores y traficantes que importaron esos productos.

A tal efecto, y dado que los dispositivos TIC falsificados suelen pasar a través de diferentes países antes de ser vendidos, es indispensable una estrecha colaboración entre las partes que intervienen en este proceso y entre las partes homólogas de los demás países implicados.

Es preciso identificar y emprender acciones judiciales contra los productores y traficantes en los países de origen, como se señala en la cláusula 8.2.

9.2 Consulta a las asociaciones industriales y de consumidores

Antes de adoptar cualquier medida correctora es necesario establecer una comunicación con todas las partes implicadas, como los operadores de red y las asociaciones industriales y de consumidores, de modo que las iniciativas de la industria puedan ser objeto de consulta y se celebren acuerdos sobre formas de proceder adecuadas y razonables, cuyas repercusiones para los usuarios finales sean mínimas.

Además, el consumidor puede ser consciente de sus derechos y obligaciones en relación con la adquisición y utilización de dispositivos TIC y las repercusiones negativas de contrarrestar la falsificación de dispositivos TIC pueden ser menores para todas las partes interesadas. Se debe hacer todo lo posible para minimizar y evitar cualquier interrupción o malentendido. Toda la información suministrada debe ser clara y fácil de entender para el usuario final.

También es necesario tomar medidas destinadas fomentar la disponibilidad y accesibilidad de los dispositivos y a la educación del consumidor que muestren las ventajas de utilizar dispositivos genuinos y las repercusiones negativas de emplear productos falsificados.

9.3 Identificadores únicos fiables

Los dispositivos TIC genuinos deben tener identificadores únicos y persistentes que sean seguros, en el sentido de que no puedan ser modificados por entidades no autorizadas, sean diferentes para cada equipo y hayan sido asignados por el asignatario autorizado.

Se recomienda a los fabricantes que integran este identificador único en un componente del equipo y que apliquen medidas de seguridad, en la medida en que sea tecnológicamente viable, para detectar toda alteración del identificador único y, en su caso, inutilizar el dispositivo hasta que se restablezca el identificador original.

Se recomienda que la entidad emisora del identificador aplique un proceso que garantice la utilización correcta y segura de estos identificadores únicos.

9.4 Base de datos de referencia centralizada

Se recomienda desplegar una base de datos de referencia centralizada de equipos autorizados en un determinado mercado, basada en identificadores únicos, para diferenciar eficazmente los dispositivos TIC auténticos de los falsificados.

Se deben considerar los siguientes aspectos al construir esta base de datos:

– Esta base de datos centralizada debe compartirse con las partes pertinentes del país, como las autoridades aduaneras, la policía y los organismos reguladores, a fin de que las instituciones puedan conocer el tránsito de mercancías y, en su caso, impedir la importación, la circulación y la venta en el mercado de dispositivos TIC falsificados y ayudar a rastrear a los productores y traficantes de dichos productos falsificados.
– Esta base de datos centralizada debe ser la piedra angular de la solución para eliminar los dispositivos TIC falsificados que ya se emplean en el mercado.
– Hay bases de datos de mercados específicos que pueden proporcionar información sobre productos dentro de ese país, algunos de los cuales son subconjuntos naturales o incluso están vinculados de alguna manera a una base de datos mundial.

9.5 Implantación de un régimen de evaluación de la conformidad

La utilización (o creación) de un plan de evaluación de la conformidad (PEC) robusto es indispensable para crear eficazmente una base de datos nacional centralizada de referencia sobre equipos autorizados, basada en logotipos de homologación, iconos u otros identificadores únicos creados por fabricantes genuinos de dispositivos, de modo que todas las partes (por ejemplo, las autoridades aduaneras, los clientes y la industria) puedan diferenciar los dispositivos TIC auténticos de los falsificados.

– Varias administraciones nacionales, organizaciones regionales e internacionales, empresas privadas y muchos agentes del sector de las TIC han instaurado un PEC eficaz. En general, cuando se trata de la utilización de las TIC a escala mundial, los dispositivos necesarios se ajustan a un conjunto de normas aceptadas internacionalmente y pasan por procedimientos de evaluación de la conformidad (por ejemplo, reconocimiento de laboratorios de la UIT: CASC, ISO/CASCO, IECEE CB, GSMA, FCC, Innovation, Science and Economic Development Canada, ANATEL, GCF, PTCRB, ARIB, etc.).
– Estas organizaciones poseen grandes volúmenes de datos relacionados con el control de productos, por ejemplo: entidades responsables de la fabricación y venta de dichos productos; conjuntos de normas y reglamentos nacionales (como los relativos a asignación de espectro) y el origen de los productos.
– Hay varias maneras de progresar en el establecimiento de un mercado ordenado de las TIC. Un ejemplo es: En el Pilar 4 del Programa de C+I de la UIT se han elaborado diferentes directrices. El portal de programas de C+I puede consultarse en: http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

9.6 Estrecha colaboración con las autoridades aduaneras y los organismos nacionales competentes

Para limitar de manera efectiva la circulación, importación y venta de nuevos dispositivos TIC falsificados en el mercado, es necesario establecer una estrecha colaboración entre las autoridades responsables de la base de datos nacional de referencia centralizada, las autoridades aduaneras y las aduanas de los distintos países.

– Dado que las autoridades aduaneras y otras autoridades nacionales competentes y autorizadas en materia de consumo desempeñan un papel fundamental en la interceptación de productos falsificados, es importante proporcionarles los instrumentos necesarios para identificar dispositivos TIC falsificados, como la base de datos nacional de referencia centralizada.
– El comercio ilícito de dispositivos TIC, incluidos los dispositivos falsificados, de contrabando y robados, puede contrarrestarse mediante mecanismos que permitan autentificar la identidad de un determinado dispositivo a fin de comprobar si auténtico, en virtud de la legislación y reglamentación de ese país.

– Los procedimientos de observancia de la ley y la comunicación entre las diferentes organizaciones deben estar establecidos y ser plenamente operativos. Queda comprendido el intercambio de información pertinente, como la base de datos nacional de dispositivos TIC de conformidad con las normas nacionales, regionales o internacionales.
– Se recomienda que las aduanas adopten una plataforma intergubernamental en línea para compartir información sobre productos y alertas que ayuden a identificar equipos falsificados, como la Organización Mundial de Aduanas IPM [b-OMA-IPM].

9.7 Información para el usuario final antes de cualquier acción correctiva

Es necesario informar a los consumidores de los riesgos que conlleva la compra de dispositivos TIC falsificados y de que éstos quizá no ofrezcan la misma seguridad y funcionamiento que los artículos auténticos.

Además, deben explicarse claramente a los consumidores los motivos por los que no se permiten los dispositivos TIC falsificados, por ejemplo, riesgos de seguridad, menor calidad del servicio y, por consiguiente, aumento de las reclamaciones, riesgos de interferencia, quebrantamiento de los derechos de propiedad intelectual (DPI), etc. Además se les debe aclarar cualquier posible información errónea sobre las razones que subyacen a los procedimientos que pueden afectar al mercado.

En caso de desarrollar soluciones tecnológicas para identificar dispositivos TIC falsificados, se recomienda proporcionar al ciudadano una herramienta que le permita verificar la autenticidad de un producto.

9.8 Apoyo a los marcos jurídicos y reglamentarios nacionales aplicables

Antes de aplicar cualquier medida restrictiva contra los dispositivos TIC falsificados, ésta debe fundamentarse en un marco jurídico y reglamentario nacional aplicable que consista en:

– restringir la activación de dispositivos TIC falsificados en las redes de telecomunicaciones;
– limitar la importación, circulación y venta en el mercado de dispositivos y accesorios TIC falsificados que no sean conformes con el marco legislativo y reglamentario del país;
– establecer las soluciones necesarias para que las autoridades, los consumidores y el canal de venta puedan diferenciar los productos auténticos de los falsificados;
– mejorar las medidas de seguridad que disuaden la fabricación de productos falsificados y otros productos ilegales;
– establecer un marco jurídico contra la alteración de identificadores únicos.

En este contexto, debe hacerse la debida referencia a la legislación y los marcos reglamentarios nacionales existentes que quizá ya contemplen los aspectos considerados.

9.9 Consideración de productos que ya se utilizan en el mercado

Antes de adoptar cualquier medida perturbadora de los dispositivos TIC falsificados en el mercado, se recomienda considerar la necesidad de proteger al usuario de estos productos. Se mitigaría así el impacto negativo para los usuarios de estos dispositivos que desconocen las disposiciones legales o reglamentarias nacionales o los requisitos relacionados con la compra y utilización de estos dispositivos TIC falsificados.

El bloqueo de los dispositivos operativos de TIC puede tener consecuencias graves e inesperadas para diferentes tipos de redes, usuarios finales e infraestructura. En este caso, una opción es adoptar mecanismos transitorios aplicables, como empezar por bloquear solamente los terminales nuevos y permitir que los dispositivos que ya están en la red sigan funcionando, aunque, en última instancia, los usuarios tendrán que adoptar terminales auténticos.

10 Posibles soluciones para contrarrestar las TIC falsificadas

Habida cuenta de los requisitos citados anteriormente y sobre la base de la información proporcionada en los estudios de casos contenidos en [b-UIT-T TR-Falsificación] y extraída de otras fuentes, a continuación se presentan posibles soluciones para contrarrestar la utilización de dispositivos TIC falsificados y algunas consideraciones que deben tomarse en consideración al desplegar algunas de estas soluciones.

10.1 Prohibición de la utilización de identificadores de dispositivos que no son válidos ni originales

Si el dispositivo utiliza un identificador único para registrarse en la red, puede impedirse el registro de dispositivos TIC falsificados utilizando bases de datos que contengan los dispositivos autorizados en un determinado mercado.

En estos casos, si el dispositivo TIC posee de hecho un identificador único fiable, se podrán desplegar soluciones que bloqueen:

– los equipos cuyos identificadores únicos no sean válidos en la red;

– la utilización de equipos no homologados por el regulador;

– la importación y venta ilícitas de estos dispositivos.

Si se opta por esta forma de proceder, se recomienda además sensibilizar a los consumidores sobre estas prescripciones. Por otra parte, puede ser necesario modificar en consecuencia la legislación nacional, como se indica en la cláusula 9.8.

Cuando se adopte una solución para contrarrestar la falsificación de dispositivos TIC mediante la determinación y el bloqueo de dispositivos cuyos códigos de identificación únicos no sean válidos, esta solución también puede ser útil para:

– garantizar que sólo se importen o vendan dispositivos legales, aumentando así la recaudación en concepto de derechos de aduana y de impuesto sobre el valor añadido;

– combatir el robo de dispositivos mediante la inscripción en una "lista negra" de los códigos de identificación únicos de los equipos robados, previa solicitud legal;

– garantizar la protección del consumidor contra la utilización de equipos de baja calidad que no estén autorizados o sean peligrosos para la salud, o que no garanticen una calidad del servicio adecuada (la protección se garantiza mediante una herramienta que permita verificar la autenticidad de los equipos antes de su adquisición).

En el proceso de normalización se debe tener presente la protección de la información personal y no afectar negativamente a los usuarios de dispositivos TIC a través de mecanismos de registro de identificadores. También se debe proteger al consumidor contra la desconexión arbitraria de la red.

Para más información sobre una posible implementación de una solución para dispositivos móviles, véase el Anexo A.

10.2 Certificación de los dispositivos TIC y vigilancia del mercado

Como se ha señalado en la cláusula 9.5, la implantación de un plan de evaluación de la conformidad (PEC) puede ayudar a construir una base de datos nacional de referencia de equipos autorizados que contenga la lista de identificadores únicos e información adicional sobre los dispositivos (como marcas de homologación, especificaciones técnicas y características físicas), de modo que todas las partes interesadas (como las autoridades aduaneras, los clientes y la industria) puedan identificar los dispositivos aprobados.

Además, con esta información, los funcionarios de aduanas podrían identificar los productos falsificados imponiendo así medidas de vigilancia del mercado y otras que pudieran ser necesarias. Además, se podrían identificar a los importadores que tengan un historial de ignorar los controles de importación e inscribirlos en una lista especial. Cuando se reciben cargamentos de dispositivos TIC de contrabando, se podría notificar a las autoridades reguladoras para que decida realizar una inspección, en cuyo caso se debe proceder a hacer cumplir la ley.

La vigilancia del mercado de los equipos de telecomunicación, que forma parte integrante de la política de PEC, tiene por objeto garantizar que los productos comercializados no causen interferencias electromagnéticas, no dañen la red pública de telecomunicaciones ni pongan en peligro la salud, la seguridad ni cualquier otro aspecto de protección ciudadana.

En la práctica, la vigilancia del mercado incluye cualquier medida necesaria (por ejemplo, prohibición, retiro y recuperación) para inmovilizar la circulación de productos que no cumplan todos los requisitos previstos en la legislación y la reglamentación pertinentes, lograr que los productos cumplan las normas 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 para organizar 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 [b-UIT-T-CI-Portal]. Los reglamentos exigen que se establezcan procedimientos para dar seguimiento a las reclamaciones, supervisar los accidentes, verificar las medidas preventivas adoptadas y recopilar conocimientos científicos y técnicos sobre cuestiones de seguridad. Además, los Estados Miembros de la UIT establecen, aplican y actualizan periódicamente los programas nacionales de vigilancia del mercado y examinan y evalúan regularmente el funcionamiento de sus actividades de vigilancia, por ejemplo, cada pocos años. [b-UIT-D-CI-Directrices]

El Reglamento CE Nº 765/2008 define la vigilancia del mercado como: las actividades realizadas y las medidas adoptadas por las autoridades designadas para garantizar que los productos cumplen los requisitos establecidos en la legislación pertinente y no ponen en peligro la salud, la seguridad o cualquier otro aspecto de la protección del interés público. [b-CE-Reglamento]

Por consiguiente, para complementar las acciones adoptadas cuando el producto llega a las fronteras del país, se recomienda contar con una vigilancia adicional, posterior a la comercialización, que ayude a identificar las mercancías falsificadas y, por lo tanto, garantizar que el producto que se pone a la venta se corresponda realmente con el que fue sometido al proceso de certificación.
[b-UIT-D-Informe]

La Comisión Económica para Europa (CEPE) recomienda que se coordinen las actividades nacionales de vigilancia del mercado y las actividades aduaneras y que se brinde a los titulares de los derechos la posibilidad de informar a las autoridades de vigilancia del mercado sobre las falsificaciones. [b-CEPE]

10.3 Gestión del ciclo de vida de los dispositivos

Conviene disponer de la capacidad de discernir entre un dispositivo TIC original y un clon, sin comprometer los derechos de un usuario. Estos clones suelen alterar los identificadores u otros elementos de identificación únicos para hacerse pasar por el dispositivo original.

Una posible solución para ayudar a estas partes interesadas y garantizar la autenticidad de los productos debería consistir en implantar un sistema de gestión del ciclo de vida de los dispositivos, basado en estos identificadores únicos, que permiten realizar un seguimiento de los dispositivos TIC desde el inicio del proceso de fabricación (incluidos el origen de los componentes, el transporte y la tienda minorista en la que se venderán) hasta la venta al usuario final.

Esta información debe estar a disposición de todas las partes interesadas y, aunque se clonen los identificadores únicos, tanto las autoridades como el usuario final podrán verificar la autenticidad de esta información. Por ejemplo, si un usuario se encuentra en una tienda de un país y, al comprobar el identificador único, la herramienta muestra que el producto en cuestión debería estar a la venta en otro minorista o incluso en otro país, esto debería constituir una prueba fehaciente de que, aun cuando el identificador único sea válido, el producto es una falsificación.

Es preciso tomar precauciones a la hora de aplicar este tipo de solución a casos en que un usuario final revende un producto usado, ya que la legislación nacional debe contemplar las posibles repercusiones para la protección de la información personal del vínculo existente entre el usuario y el dispositivo gestionado.

Cabe considerar la posibilidad de que el producto identificado por este tipo de solución no sea una falsificación, sino un producto auténtico vendido en el mercado gris, por lo que será necesario adoptar medidas adicionales para determinar si el producto falsificado.

11 Marco de referencia

Habida cuenta de los aspectos comunes a los diferentes planteamientos posibles descritos en la cláusula 10, la Figura 1 ilustra una propuesta de marco para examinar la producción, circulación y utilización de dispositivos TIC falsificados:

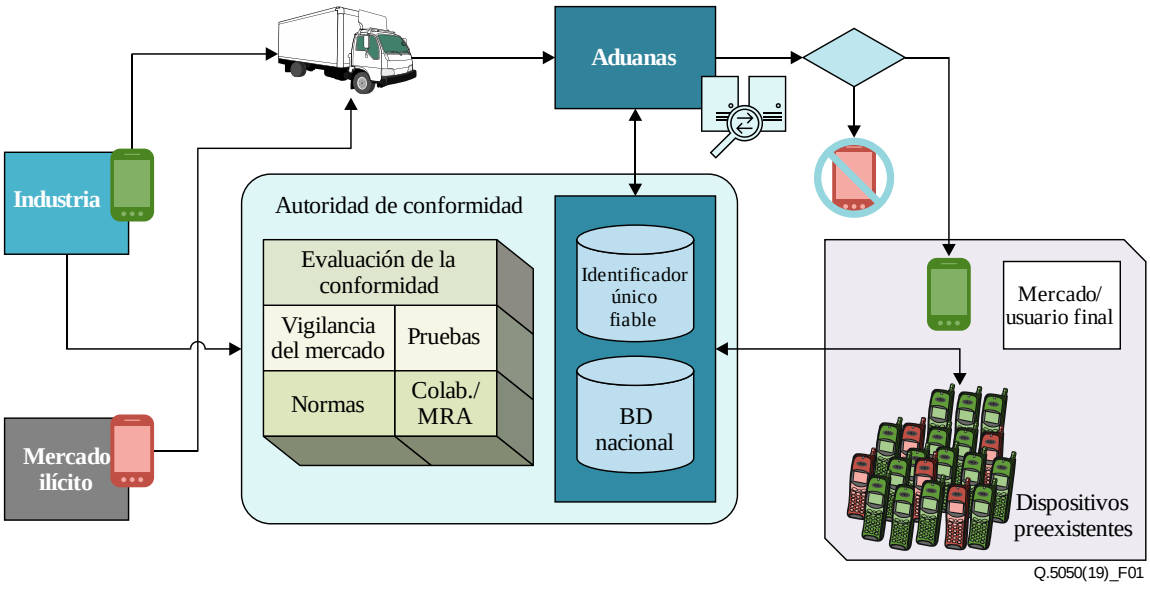

Figura 1 – Marco general propuesto

Deben combinarse actividades y sistemas de información muy diversos, operados por diferentes organizaciones, con el fin de controlar y obtener información esencial para identificar los dispositivos falsificados y alterados e impedir su utilización.

El comercio lícito permite comprobar que los productos importados al país son conforme y tienen un representante/responsable para el equipo.

Cuando los productos llegan a un punto de control, una entidad (por ejemplo, una aduana) verifica todos los aspectos legales de dichos dispositivos, incluyendo el cumplimiento de los requisitos reglamentarios y la certificación aplicables, como la asignación de radiofrecuencias, la seguridad y la interoperabilidad, etc. También puede verificarse si el dispositivo figura en una lista blanca[1] de productos con el fin de comprobar que los identificadores de los productos importados han sido atribuidos de forma legítima y que la marca y el modelo del producto considerado coinciden con los datos registrados en el momento en que se expidieron los identificadores.

Llegado este punto, se impide la entrada en el mercado de los productos no autorizados, por ejemplo, los falsificados. El personal de la entidad del caso puede apelar al eventual régimen de evaluación de la conformidad y a una base de datos con información almacenada sobre lo que debe haber en los contenedores importados.

Estas bases de datos de inventario también pueden ser de utilidad en las actividades de control una vez que el equipo (legal o no) se comercializa.

1 Por ejemplo, puede recurrirse a la base de datos global de códigos TAC de la GSMA a efectso de la elaboración de la lista blanca para dispositivos conformes con 3GPP.

Anexo A

Soluciones para dispositivos móviles

(El presente anexo forma parte integrante de la presente Recomendación.)

Cuando se trata de dispositivos móviles compatibles con 3GPP, algunas soluciones para identificar terminales móviles auténticos y legalmente importados se basan en el sistema de registro de identidades internacionales de equipos móviles (IMEI). Las soluciones que parten del IMEI para impedir la proliferación de dispositivos móviles falsificados se basan en:

– bloquear en sus redes los dispositivos móviles con números IMEI no válidos (por ejemplo, sin IMEI, IMEI totalmente nulo, cadenas con formato no normalizado, IMEI duplicados, IMEI asignados por organizaciones no autorizadas y IMEI válidos no asignados por la organización designada)[2];

– realizar otras actividades de sensibilización del consumidor, medidas de observancia y cambios legislativos adecuados en el plano nacional.

Para bloquear la utilización de dispositivos móviles falsificados, el sistema puede utilizar un registro de todos los códigos IMEI válidos (identificador que se ajustan a las normas, asignados oficialmente por una organización designada, importado legalmente y homologado) de los dispositivos móviles activos en redes nacionales. El registro de IMEI de dispositivos móviles garantiza que los dispositivos móviles cumplen con la normativa nacional y, en algunos países, que han sido importados legalmente.

- **Bases de datos de referencia**

Los códigos IMEI se utilizan para crear una base de datos de dispositivos con "lista blanca", "lista gris" y "lista negra". La "lista blanca" es el registro de los dispositivos cuya utilización en el país está autorizada (por ejemplo, aquellos legalmente importados o fabricados en el país), la "lista gris" es el registro de dispositivos cuyo estado aún no se confirmado (no inscritos en la "lista blanca" ni en la "lista negra") y la "lista negra" es el registro de dispositivos cuyos servicios debe rechazar la red de telecomunicaciones.

Se debe realizar un análisis previo sobre qué repercusiones podrían tener en las redes y en los usuarios la implantación de "listas blancas", "listas grises" y "listas negras", ya que esta medida podría limitar el movimiento de dispositivos entre países y afectar a los visitantes extranjeros y a los operadores de red.

La "lista gris" y la "lista negra" se generan automáticamente procesando los datos de la "lista blanca" y los datos de los operadores, importadores y autoridades aduaneras.

- **Integración con la red del operador**

Para garantizar una interacción activa con el sistema de registro, los operadores de telecomunicaciones deben mantener sus registros de identidades de equipos (RIE) y garantizar la sincronización periódica y el intercambio automático de datos entre los RIE y la base de datos de códigos IMEI (por ejemplo, diariamente).

Cuando se conecta y registra por vez primera un teléfono móvil en la red de uno de los operadores móviles, éste envía el código IMEI del terminal a la base de datos. El sistema comprueba los códigos IMEI que no están disponibles en la "lista blanca", identifica los dispositivos móviles falsificados y registra los códigos IMEI correspondientes en la "lista gris". El propietario del terminal del caso

---

[2] La base de datos global de códigos TAC de la Asociación GSMA puede utilizarse a fin de validar identidades IMEI de dispositivos compatibles con 3GPP que hayan sido objeto de apropiación indebida o clonación.

recibe un aviso por SMS y tiene que confirmar el origen legal del terminal dentro del plazo especificado desde la fecha en que se inscribe en la "lista gris".

Debe garantizarse la fiabilidad y seguridad del sistema de registro y de los procesos conexos. Por lo general, se facilita acceso a la base de datos a las autoridades reguladoras y aduaneras, a los operadores de redes y a la población en general con los adecuados niveles de privilegios de acceso. Los usuarios deben tener acceso a esta base de datos para verificar si un determinado dispositivo móvil puede utilizarse en el país (normalmente, por SMS o a través de una página web).

Es importante tener en cuenta que los SMS deben considerarse un medio de comunicación inseguro con el cliente, que los estafadores podrían explotar, por lo que convendría tomar medidas adicionales.

- **Detección de IMEI clonados**

Dado que es posible alterar los identificadores únicos de algunos dispositivos y es probable que los traficantes comiencen a clonar los IMEI de dispositivos ordinarios para evitar este sistema de control, deben aplicarse medidas adicionales para identificar y actuar contra dispositivos irregulares con IMEI legítimos clonados.

Una posible opción es crear una base de datos que contenga información adicional sobre el producto, que podría utilizarse para verificar si el producto que utiliza los identificadores guarda conformidad con los otros atributos. Estas herramientas podrían contar con la ayuda de un régimen de evaluación de la conformidad auxiliar, que recabaría esta información durante el proceso de certificación del dispositivo y la almacenaría en una base de datos accesible por todas las partes interesadas.

- **Consideraciones adicionales**

Por otra parte, la solución para contrarrestar los dispositivos móviles falsificados mediante la determinación y el bloqueo de los dispositivos móviles con códigos IMEI inválidos o alterados, también puede ayudar a:

– bloquear la importación ilícita de estos dispositivos y, por lo tanto, garantizar que los dispositivos móviles se han importado y vendido legalmente, generando así más ingresos en concepto de derechos de aduana y de impuesto sobre el valor añadido;

– contrarrestar el robo de terminales mediante el registro de los códigos IMEI de los terminales robados en la "lista negra" previa solicitud legal, inutilizando así los terminales robados (el mismo procedimiento puede aplicarse al bloqueo de terminales a petición de los propietarios de los dispositivos móviles perdidos);

– bloquear la utilización de equipos no homologados por el organismo regulador, garantizando así la protección de los consumidores contra la utilización de terminales móviles de baja calidad, que quizá no estén autorizados o sean peligrosos para la salud o que no garanticen una calidad adecuada de los servicios de comunicaciones móviles (la protección se garantiza mediante una herramienta que permita verificar fácilmente la legalidad de un teléfono móvil antes de su adquisición).

La coordinación a escala nacional es importante, ya que los dispositivos TIC falsificados pueden estar presentes en más de una red, y el proceso de detección debe ser eficiente en cuanto a las medidas que deben adoptarse para evitar los efectos múltiples para usuarios, la duplicación de esfuerzos y las controversias entre los distintos operadores móviles.

Las primeras etapas del diagnóstico (dimensionamiento del problema de los identificadores no válidos, clonados, etc.), la planificación del proceso de detección y control, los recursos necesarios (fondos, personal, tiempo) y el análisis de impacto para reducir los efectos que afectan a los usuarios finales deben llevarse a cabo y discutirse con todas las partes interesadas para poner en marcha estas soluciones.

También debe tenerse en cuenta que, en algunos casos, estos mecanismos pueden causar problemas a los usuarios legítimos, como viajeros y turistas, por ejemplo:

– Un visitante extranjero que viaja a un país y luego utiliza una tarjeta de módulo de identificación de abonado (SIM) local en su dispositivo puede quedar atrapado en una trampa de listas blancas que le impida utilizar totalmente su dispositivo.

– Un visitante itinerante que sigue utilizando su dispositivo durante unos meses también puede ser injustamente penalizado por una lista blanca local después de cierto período de utilización.

– El visitante de un país que está utilizando una tarjeta SIM local puede recibir un mensaje de registro, pero quizá no hable el idioma local y por tanto no entienda el mensaje. Por consiguiente, al no responder su dispositivo acaba registrado en la lista negra. Esto puede causar: i) la desconexión del visitante de la red local; o ii) que el dispositivo legítimo del visitante se incluya en una lista negra en otros países debido a acuerdos de colaboración, pese a que el dispositivo es totalmente legítimo.

Estos mecanismos, si se utilizan mal, pueden causar problemas, los cuales deben evitarse en la fase de diseño. Por último, esta funcionalidad no debe utilizarse para desconectar arbitrariamente a los usuarios de las redes por otras razones.

Apéndice I

Otras soluciones de la industria

(Este apéndice no forma parte integrante de la presente Recomendación.)

La industria ha invertido en múltiples iniciativas para resolver el problema de los equipos falsificados y mejorar la fiabilidad de los equipos y las empresas. Se trata de iniciativas de la industria para desarrollar soluciones voluntarias que mejoren la seguridad de la cadena de suministro. La falsificación de equipos es uno de los aspectos de estas iniciativas, pero no el único. La industria también debe colaborar con los gobiernos, concretamente con las autoridades policiales y aduaneras. Lo ideal es concebir los resultados de estas iniciativas como un conjunto de herramientas que las empresas pueden utilizar en función de sus necesidades y circunstancias específicas (por ejemplo, producto, mercado, etc.).

Obsérvese que las actividades de la industria sobre productos falsificados abarcan muy diversos productos con distintas cadenas de suministro, cuyas necesidades son a veces diferentes. Se trata de una interacción compleja y multipartita. Además de estas actividades externas, las empresas llevan a cabo actividades de investigación y desarrollo muy delicadas y confidenciales destinadas a desarrollar métodos para contrarrestar la falsificación.

A continuación figura una descripción general no exhaustiva de algunas de las iniciativas para mejorar la seguridad de los dispositivos que pueden contribuir a dificultar la falsificación.

- **Base de datos IMEI de la Asociación GSMA**

El IMEI es un número de 15 dígitos que se utiliza para identificar los dispositivos en una red móvil. El código de asignación de tipo (TAC) se encuentra en los primeros 8 dígitos del IMEI e identifica un modelo específico.

La Global System for Mobile communications Association (GSMA) mantiene una base de datos global que contiene información sobre los TAC específicos que se asignan a los dispositivos compatibles con 3GPP. Esta base de datos se conoce como base de datos IMEI.

Esta base de datos puede ser utilizada de las siguientes maneras:

– La identificación de dispositivos TIC falsificados puede realizarse en colaboración con el fabricante genuino, que puede consultarse en la lista de la base de datos TAC de la GSMA.

– La base de datos TAC de la GSMA puede ponerse a disposición de entidades gubernamentales, tales como ministerios, reguladores, aduanas y fuerzas del orden, para que sirva de fuente de información sobre la procedencia y especificación de los dispositivos móviles. Esta información se puede utilizar para identificar anomalías y al fabricante del dispositivo que no puede confirmar si el dispositivo es auténtico.

– La autenticidad de los fabricantes de dispositivos móviles y su IMEI puede verificarse utilizando la base de datos TAC de la GSMA. Las agencias de aduanas y las fuerzas de seguridad pueden utilizar el servicio de asistencia técnica de la GSMA para verificar el número de serie del certificado TAC presentado por el fabricante. Se trata de un segundo número de serie vinculado a cada TAC. Si estos identificadores no coinciden, hay indicios de alguna forma de falsificación del identificador.

– Los reguladores pueden utilizar la base de datos TAC de la GSMA para asegurarse de que los dispositivos móviles que están pasando las pruebas de evaluación de conformidad se corresponden con la descripción del modelo que figura en la base de datos.

Base de datos IMEI de la GSMA: https://imeidb.gsma.com/imei/index

Servicios IMEI de la GSMA: https://www.gsma.com/services/tac-allocation/the-imei-database/

- **Sistema de identificación, registro y bloqueo de dispositivos**

El sistema de identificación, registro y bloqueo de dispositivos (DIRBS) es una plataforma de *software* basada en un servidor, cuyo objetivo es detectar los dispositivos móviles falsificados, ilegales y robados en un país. La plataforma de *software* DIRBS está disponible en código abierto para ayudar a los gobiernos, organismos reguladores y otras entidades a contrarrestar la utilización indebida de dispositivos falsificados, ilegales o robados en las redes celulares. La plataforma se ajusta a las recomendaciones de la Unión Internacional de Telecomunicaciones encaminadas a solucionar el problema de los dispositivos ilegales y no homologados a escala nacional.

El DIRBS consiste en una base de datos de dispositivos a nivel de país que interactúa a diferentes niveles de detalle con los operadores, los fabricantes locales, los importadores, los consumidores, las aduanas, las fuerzas del orden y la base de datos mundial IMEI de la GSMA. La plataforma DIRBS se compone de un motor de análisis y los subsistemas conexos que suministran información para poder bloquear dispositivos falsificados y fraudulentos; el bloqueo real está determinado por la normativa específica de cada país y se efectúa a través de los mecanismos del registro de identidades de equipos (RIE) del operador.

Para más información, véase: www.qualcomm.com/dirbs.

- **Grupo Trusted Computing**

El Trusted Computing Group (TCG) es una organización sin ánimo de lucro creada para desarrollar, definir y promover normas mundiales industriales abiertas y neutrales para los proveedores, que permita crear un núcleo de confianza basado en *hardware*, para plataformas informáticas de confianza y compatibles.

Entre otros ámbitos, el TCG ha desarrollado una especificación para un módulo de plataforma de confianza (TPM) que resulta pertinente para este tema:

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

Como se indica en el sitio web antes mencionado, el TPM es un chip (microcontrolador) que puede almacenar de forma segura los objetos utilizados para autenticar la plataforma (su PC o portátil). Estos objetos son, entre otros, contraseñas, certificados o claves de encriptación.

Este mecanismo permite la certificación local y remota que ayuda a confiar en que el equipo es auténtico.

El TCG también ha creado un grupo de trabajo sobre sistemas integrados para abordar la seguridad de los sistemas integrados, incluida la Internet de las cosas (IoT):

http://www.trustedcomputinggroup.org/developers/embedded_systems

- **Plataforma Global**

La Plataforma Global ha elaborado normas para el entorno de ejecución de confianza (TEE) que han sido adoptadas en los dispositivos móviles modernos como método seguro de almacenamiento y ejecución de código de seguridad y activos sensibles.

Para más información, véase: https://www.globalplatform.org/specificationsdevice.asp.

- **JTC1/SC27 de la ISO/CEI**

El alcance de la SC27 es importante para las actividades de la industria relacionadas con la seguridad, la mitigación de la falsificación y la elaboración de normas para proteger la información y las TIC. Esto incluye métodos, técnicas y directrices genéricas tanto para la seguridad como para la protección de la información personal.

Entre otros trabajos, SC27 ha publicado normas relativas a los equipos falsificados, tales como:

– [b-ISO/CEI 15408]: *Information technology – Security techniques – Evaluation criteria for IT security (Common Criteria)*;

– [b-ISO/CEI 27034]: *Information Technology – Security Techniques – Application Security*;

– [b-ISO/CEI 27036-3]: *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*;

– [b-ISO/CEI 20243]: *Information Technology – Open Trusted Technology ProviderTM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

Para más información, véase: http://www.din.de/en/meta/jtc1sc27.

- **Open Group Trusted Technology Forum**

El Foro OTTF (Open Group Trusted Technology Forum) lidera el desarrollo de un programa y marco de integridad de la cadena de suministro global con el fin de proporcionar a los compradores de productos de TI una selección de asociados y proveedores de tecnología acreditados. Obsérvese que la norma [b-ISO/CEI 20243] antes mencionada fue desarrollada por primera vez por el Open Group.

Para más información, véase: http://www.opengroup.org/getinvolved/forums/trusted.

- **Instituto de Ingenieros Eléctricos y Electrónicos**

El Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) ha desarrollado una norma relativa a la identidad segura de dispositivos y un método para vincular criptográficamente la identidad al dispositivo, a saber, la norma IEEE 802.1ar – "Standard for Local and Metropolitan Area Networks: Secure Device Identity".

Como se señala en el sitio web del IEEE: "Esta norma especifica identificadores de dispositivos seguros (DevID) diseñados para ser utilizados como credenciales de autentificación de dispositivos seguras y compatibles con el protocolo de autenticación extensible (EAP) y otros protocolos normalizados de autentificación y configura de la industria. La identidad de dispositivo normalizada facilita la autentificación segura y compatible de dispositivos y simplifica el despliegue y administración seguros de dispositivos."

Para más información, véase: http://www.ieee802.org/1/pages/802.1ar.html.

- **Otras actividades de la industria relacionadas con la falsificación**

ICC – Oficina de inteligencia sobre falsificaciones (*Counterfeiting Intelligence Bureau*)

http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

ICC – Acción empresarial contra la falsificación y el pirateo (*Business Action to Stop Counterfeiting and Piracy*, BASCAP)

http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/

Bibliografía

[b-UIT-T-CI-Portal] Con arreglo al Pilar 4, el portal de C+I de la UIT contiene información actualizada sobre los marcos reglamentarios de C+I de los países.
http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx

[b-UIT-T TR-Falsificación] Informe Técnico sobre Equipos TIC falsificados (2015).

[b-IEEE 802.1] IEEE 802.1 (2009), *Standard for Local and Metropolitan Area Networks: Secure Device Identity*. –
http://www.ieee802.org/1/pages/802.1ar.html

[b-ISO/CEI 15408-1] ISO/CEI 15408-1:2009, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model*.

[b-ISO/CEI 17000] ISO/CEI 17000:2004, *Conformity assessment – Vocabulary and general principles*.

[b-ISO/CEI 20243] ISO/CEI 20243:2015, *Information Technology – Open Trusted Technology Provider TM Standard (O-TTPS) – Mitigating maliciously tainted and counterfeit products*.

[b-ISO/CEI 27034] ISO/CEI 27034:2011, *Information technology – Security techniques – Application security*.

[b-ISO/CEI 27036-3] ISO/CEI 27036-3:2013, *Information technology – Security techniques – Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security*.

[b-CE-Reglamento] Reglamento sobre vigilancia del mercado, CE Nº 765/2008.

[b-Gartner] https://www.gartner.com/it-glossary/gray-market

[b-UIT-D-CI-Directrices] Directrices de la UIT sobre el establecimiento de regímenes de conformidad e interoperabilidad: Directrices completas (2015), UIT.
http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf

[b-UIT-D-Informe] Informe Final para la Cuestión 4/2 – Cuestión 4/2: Asistencia a los países en desarrollo para la ejecución de programas de conformidad e interoperatividad, Comisiones de Estudio del UIT-D, 2017.
https://www.itu.int/pub/D-STG-SG02.04.1-2017

[b-OCDE] Informe de la OCDE de 2017, "Trade in Counterfeit ICT Goods".

[b-Acuerdo sobre los ADPIC] Aspectos de los derechos de propiedad intelectual relacionados con el comercio; Anexo al Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio, firmado en Marrakech (Marruecos), el 15 de abril de 1994.

[b-CEPE] Recomendación M. sobre el: Uso de infraestructuras de vigilancia del mercado como medio complementario para proteger a los consumidores y usuarios contra las mercancías falsificadas.
http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[b-OMA-IPM] Organización Mundial de Aduanas IPM – http://www.wcoipm.org/

[b-OMC-OTC] Organización Mundial del Comercio (OMC) – Acuerdo de la OMC sobre los obstáculos técnicos al comercio (OTC).

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	**Conmutación y señalización, y mediciones y pruebas asociadas**
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	Infraestructura mundial de la información, aspectos del protocolo Internet, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2019