Unión Internacional de Telecomunicaciones

UIT-T Informe Técnico

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

(11 de diciembre de 2015)

Equipos TIC falsificados

ITU-T

International Telecommunication Union

Resumen

La falsificación está ampliamente reconocida como un problema socioeconómico creciente e importante. El presente Informe Técnico proporciona información básica sobre la naturaleza de las cuestiones relativas a la falsificación de equipos de tecnologías de la información y de la comunicación (TIC), considera los convenios internacionales que tratan este tipo de infracción de los derechos de propiedad intelectual y las actividades de las organizaciones para hacer cumplir esos derechos y describe una serie de medios para combatir el comercio de productos falsificados. Además, en el Anexo A se describen algunas iniciativas nacionales e internacionales para combatir la falsificación de dispositivos móviles.

Palabras clave

Falsificación, de baja calidad.

Número de referencia

QSTR-COUNTERFEIT.

Registro de cambios

La presente versión 2 del Informe Técnico del UIT-T sobre "*Equipos TIC falsificados*" se aprobó durante la reunión de la Comisión de Estudio 11 del UIT-T celebrada en Ginebra del 2 al 11 de diciembre de 2015.

Editor: Keith Mainwaring
UNIS
Tel.: +46 76 107 6877
Correo-e: keith.mainwaring@ukrainesystems.com

ÍNDICE

Lista de Figuras

Página

Informe Técnico del UIT-T

Equipos TIC falsificados

Resumen

La falsificación está ampliamente reconocida como un problema socioeconómico creciente e importante. El presente Informe Técnico proporciona información básica sobre la naturaleza de las cuestiones relativas a la falsificación de equipos de tecnologías de la información y de la comunicación (TIC), considera los convenios internacionales que tratan este tipo de infracción de los derechos de propiedad intelectual y las actividades de las organizaciones para hacer cumplir esos derechos y describe una serie de medios para combatir el comercio de productos falsificados. Además, en el Anexo A se describen algunas iniciativas nacionales e internacionales para combatir la falsificación de dispositivos móviles.

1 Introducción: falsificación de productos – un problema creciente

Aunque resulte muy difícil de cuantificar, existen cada vez más evidencias de que la distribución de productos falsificados es un problema en crecimiento, tanto por su extensión como por la gama de productos afectados. En 2008, la OCDE [1] publicó un informe en el que se estimaba, basándose en las decomisos en las aduanas, que el comercio internacional total de mercancías falsificadas y piratas (sin incluir productos digitales y aquellos productos generados y consumidos en el ámbito doméstico) superaba los 200 000 millones USD en 2005. Esta estimación se actualizó a partir del crecimiento y de la composición variable del mercado internacional de 100 000 millones USD en el año 2000 a 250 000 millones USD para el año 2007, lo que supone el 1,95% del mercado internacional [2]. Algunas estimaciones son incluso superiores, la Oficina de Inteligencia contra la Falsificación de la Cámara de Comercio Internacional (CCI) estima que la falsificación supone entre el 5% y el 7% del mercado mundial por un valor de 600 000 millones USD anuales [3].

La Iniciativa de lucha contra la falsificación y la piratería (BASCAP) de la CCI encargó un estudio [4] para completar el enfoque sobre el impacto social y económico de la falsificación y la piratería ofrecido por la OCDE. Este informe presenta una estimación del valor económico mundial total de los productos falsificados y piratas que asciende a 650 000 millones USD al año, de los cuales más de la mitad corresponden al mercado internacional (entre 285 000 y 360 000 millones USD), a la producción y consumo nacionales entre 140 000 y 215 000 millones USD, y al contenido digital (música, películas y programas informáticos) entre 30 000 y 75 000 millones USD. Además, se estima que la falsificación y la piratería cuestan a los gobiernos y a los consumidores del G20 más de 125 000 USD cada año (debido a factores tales como la disminución de los ingresos por impuestos y el aumento de los costes de las contramedidas y de la asistencia sanitaria) y a la pérdida de aproximadamente 2,5 millones de puestos de trabajo.

Las autoridades nacionales de aduanas de la Unión Europea (UE) han constatado que entre 2005 y 2010 se ha triplicado la cantidad de mercancías falsificadas que se han introducido en la UE. Las estadísticas publicadas por la Comisión Europea en julio de 2011 muestran una tendencia ascendente desmedida en la cantidad de envíos sospechosos de violar los derechos de propiedad intelectual (DPI). Las autoridades de aduanas registraron cerca de 80 000 casos en 2010, una cifra que prácticamente se ha duplicado desde 2009. Se incautaron más de 130 millones de productos falsificados en las fronteras exteriores de la UE.
http://trade.ec.europa.eu/doclib/docs/2012/january/tradoc_149003.pdf

Se falsifica una gama de productos extraordinariamente amplia – alimentos y bebidas, productos farmacéuticos, componentes eléctricos y de automoción, todo tipo de productos de consumo e incluso tiendas enteras. Se falsifican componentes de ordenadores (pantallas, estuches, discos duros), equipamiento informático, enrutadores, cámaras web, mandos a distancia, teléfonos

móviles, televisores (TV), discos compactos (CD) y reproductores de discos digitales (DVD), altavoces, cámaras, auriculares, adaptadores bus en serie universal (USB), programas informáticos, certificados, sellos de certificación y datos (como datos biomédicos).

Además, cada vez se utiliza más Internet para la piratería digital y también para comercializar mercancías falsificadas. Todos los factores que hacen de Internet un recurso atractivo para los minoristas, en particular para aquellos destinados a pequeños mercados (acceso al mercado mundial, facilidad de crear, cambiar y cerrar sitos Web que pueden resultar muy convincentes y el reducido coste de enviar correos electrónicos), junto con la posibilidad del anonimato, resultan atrayentes para los vendedores de mercancías falsificadas. Asimismo, la enorme cantidad de sitios en Internet hace muy difícil a los titulares de derechos de propiedad intelectual y a los organismos de aplicación de la ley la identificación de las operaciones ilegales. Para intentar vender mercancías falsificadas se utilizan la publicidad por Internet, el comercio electrónico y los sitios de subastas.

En lo que respecta al sector de las TIC, un informe del KPMG y de AGMA estimó que en 2007 entre el 8% y el 10% de todas las mercancías del sector de las tecnologías de la información vendidas en el mundo estaban falsificadas, lo que supone unas pérdidas de ingresos de 100 000 millones USD para el sector. Hewlett-Packard realizó más de 4 620 averiguaciones en 55 países entre 2005 y 2009 que consiguieron decomisar suministros de impresión falsificados por valor de más de 795 millones USD [6]. La electrónica de consumo supone el 22% de las incautaciones en aduanas de los Estados Unidos en 2011, aumentando el valor de las mercancías más de 16% en 2010. Cerca de un tercio de las mercancías en esta categoría eran teléfonos móviles [5].

En 2011 existía un mercado mundial estimado en 250,4 millones de teléfonos móviles falsificados. http://press.ihs.com/press-release/design-supply-chain/cellphone-gray-market-goes-legit-sales-continue-decline. Esto corresponde a cerca del 16% de los 1 546 millones de móviles vendidos en 2011 [8]. Se trata de una estimación de la amplitud de la penetración de las falsificaciones en el mercado de la telefonía móvil similar a la del estudio sobre la internacionalización y fragmentación de las cadenas de valor y de la seguridad elaborado en 2011 para la Comisión Europea, según el cual, los teléfonos móviles falsificados constituyen entre el 15% y el 20% del mercado mundial en términos de unidades vendidas por un valor de cerca de 9 000 millones USD.

Además de la fabricación de dispositivos falsificados, se están introduciendo componentes electrónicos falsificados en las cadenas legales de suministro de productos. En otoño de 2011 se publicó en los titulares de la prensa el uso de componentes falsificados en equipamiento militar de los Estados Unidos de América durante un proceso en el Comité de las fuerzas armadas del senado sobre componentes electrónicos falsificados en las cadenas de producción del Ministerio de Defensa [9]. En un estudio del Departamento de Industria y Seguridad del Ministerio de Comercio [10] se estimó que se habían introducido en las cadenas de contratación de defensa cerca de 1 800 casos de componentes electrónicos falsificados, implicando a más de un millón de componentes. También se demostró que el número de incidentes había aumentado de 3 868 en 2005 a 9 356 en 2008. Como consecuencia de este proceso, la Ley nacional de autorización de la defensa (National Defence Authorisation Act (NDAA)) incluye directrices sobre cómo tratar el asunto de los componentes falsificados, incluida la realización de inspecciones adicionales a los componentes electrónicos importados, y atribuye toda la responsabilidad a los contratistas para que detecten los componentes falsos y para que corrijan cualquier caso en el que se hayan introducido componentes falsificados en productos [11].

El estudio de la OCDE de 2008 concluye que la mayoría de los productos falsificados proviene de un país asiático (correspondiendo al 69,7% de las aprehensiones de productos falsificados).

El presente Informe Técnico proporciona información básica sobre el problema de la falsificación y sobre cómo se puede solucionar, centrándose en la falsificación de equipos TIC y en las herramientas TIC que podrían utilizarse para paliar el problema.

Además de los dispositivos falsificados proliferan los equipos y accesorios TIC a los que normalmente se denomina "de baja calidad" o "no autorizados". Aunque no existe ninguna definición normalizada universal de estos términos, estos dispositivos utilizan a menudo componentes de menor calidad y, en la mayoría de los casos, no cumplen los requisitos legales nacionales en lo que respecta a la certificación, aprobación, distribución y venta de dispositivos móviles. No todos estos dispositivos infringen los derechos de propiedad intelectual de los fabricantes y, por tanto, no se ciñen a la definición aceptada de "falsificación". Por consiguiente, están fuera del ámbito del presente Informe Técnico que se centra en los dispositivos falsificados. Los dispositivos "de baja calidad" constituyen y presentan un conjunto propio de problemas y soluciones que precisan especial consideración.

2 ¿Qué se entiende por falsificación?

El Acuerdo de la OMC sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio (el Acuerdo ADPIC) define las mercancías de marca fábrica o de comercio falsificadas como "cualesquiera mercancías, incluido su embalaje, que lleven puesta sin autorización una marca de fábrica o de comercio idéntica a la marca válidamente registrada para tales mercancías, o que no pueda distinguirse en sus aspectos esenciales de esa marca, y que de ese modo lesione los derechos que al titular de la marca de que se trate otorga la legislación del país de importación" (nota 14 al Artículo 51). El término "falsificado" se utiliza por lo tanto en el Acuerdo ADPIC únicamente en el ámbito de las marcas de comercio. Se refiere a las mercancías infractoras que están definidas con mayor precisión que las infracciones ordinarias de la marca de comercio debido a que la marca de comercio es idéntica o indistinguible del original. El presente texto no menciona las intenciones ocultas del uso de la marca de comercio falsificada. Define un producto falsificado en términos de parecido con la marca utilizada por un producto registrado y aplica a casos en los que las mercancías son las mismas que las que se han registrado como marca. En la práctica, este tipo de mercancía infractora incluirá normalmente casos en los que se ha copiado exactamente una marca de forma deliberada para dar la impresión de que se trata de un producto genuino. Normalmente esto implica un intento de fraude puesto que es deliberada la confusión entre un producto auténtico y una copia.

La misma nota del Acuerdo ADPIC define las mercancías pirata que lesionan el derecho de autor como "cualesquiera copias hechas sin el consentimiento del titular del derecho o de una persona debidamente autorizada por él en el país de producción y que se realicen directa o indirectamente a partir de un artículo cuando la realización de esa copia habría constituido infracción del derecho de autor o de un derecho conexo en virtud de la legislación del país de importación". El término "pirata", por tanto, se refiere a la infracción del derecho de autor o de un derecho conexo del Acuerdo ADPIC.

3 Repercusiones de la falsificación de equipos y componentes TIC

Los equipos TIC falsificados tienen repercusiones particulares en la sociedad que no producen otros tipos de violaciones de los derechos de propiedad intelectual. Los productos falsificados, por ejemplo, normalmente no han sido comprobados ni se han aceptado formalmente de conformidad con los requisitos legales que sean de aplicación. El uso de productos falsificados puede resultar extremadamente peligroso. Por ejemplo, existen casos de muertes debidas a la explosión de baterías falsificadas, casos de electrocución y de incendios producidos por cargadores y ejemplos documentados de que estos dispositivos tienen cantidades elevadas de sustancias peligrosas como el plomo y el cadmio.

El informe de 2008 de la OCDE incluye evaluaciones de los efectos socioeconómicos y de las consecuencias para los titulares de derechos de autor, los consumidores y los gobiernos:

- Habida cuenta de los efectos socioeconómicos, la falsificación puede tener efectos negativos sobre la innovación, las inversiones directas del exterior, el crecimiento de la economía y la tasa de empleo y también puede derivar recursos hacia las redes de delincuencia organizada.
- Es probable que la falsificación tenga un impacto económico en los titulares de los derechos puesto que se pueden ver afectados las ventas y los derechos de autor, los precios, el valor y la reputación de la marca, los costes y los objetivos de las operaciones.
- Los consumidores pueden constatar que la calidad de las mercancías falsificadas es menor y también se pueden enfrentar a graves riesgos para su salud y seguridad.
- Los gobiernos recaudarán menos en impuestos y probablemente se enfrentarán a problemas de corrupción, por lo que tendrán que dedicar más recursos para combatir las actividades de falsificación.

3.1 Ejemplos de equipos TIC falsificados

A continuación se presentan ejemplos clave de las repercusiones de la falsificación de equipos TIC.

3.1.1 Teléfonos móviles

La falsificación de teléfonos móviles y de sus accesorios afecta a la sociedad, entre otras cosas[1]:

- reduciendo la calidad del servicio de telecomunicaciones móviles, afectando por lo tanto a la percepción de los consumidores y de las empresas;
- generando un riesgo de seguridad para los consumidores debido al uso de componentes o materiales deficientes o inadecuados;
- aumentando las amenazas relacionadas con la ciberseguridad;
- comprometiendo la privacidad del consumidor;
- menoscabando la seguridad de las transacciones digitales;
- evadiendo impuestos y aranceles aplicables, afectando por lo tanto negativamente a la recaudación gubernamental de impuestos;
- perjudicando a los consumidores más vulnerables desde el punto de vista financiero al no proporcionarles garantías y violando a su vez los derechos legales de los consumidores;
- creando riesgos para el medio ambiente y la salud de los consumidores debido al uso de sustancias peligrosas en la fabricación de esos dispositivos;
- facilitando el narcotráfico, el terrorismo y otras actividades delictivas nacionales e internacionales;
- causando un perjuicio económico dada la distorsión del mercado generada por la competencia desleal y las prácticas fraudulentas; y
- dañando las marcas registradas de las empresas fabricantes de productos originales.

Un estudio realizado por el Instituto Nokia de Tecnología (INdT), entidad independiente de investigación y desarrollo con sede en Brasil, confirmó la mala calidad de los teléfonos falsificados y el potencial impacto negativo que pudiera producir en los consumidores, los operadores de telefonía y las economías locales. El estudio analiza 44 teléfonos celulares falsificados y de baja calidad, comparándolos con equipos genuinos y homologados. El estudio muestra que los teléfonos falsificados fallaron en un 26% de los intentos de llamada y que un 24% de las llamadas se

[1] Lo siguiente se basa en Teléfonos móviles falsificados/de baja calidad – Guía de recursos para los gobiernos, del Foro de Fabricantes de Sistemas Móviles (MMF). http://spotafakephone.com//docs/eng/MMF%5FCounterfeitPhones%5FEN%2Epdf

cortaron. Además, en lugares en los que un teléfono auténtico funcionaba perfectamente, los teléfonos falsificados no se pudieron utilizar debido a su inferior calidad de transmisión frente a los teléfonos originales. También hubo problemas con la transmisión entre celdas (la capacidad de mantener la llamada mientras se mueve entre celdas) con una duración de la transferencia de un 41% mayor que la de los teléfonos originales y el 34% de las llamadas se cortaron durante la transferencia. Véanse las figuras del Anexo 1 del Foro de Fabricantes de Sistemas Móviles (MMF) sobre Teléfonos móviles falsificados/de baja calidad – Guía de recursos para los gobiernos. http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf.

La falsificación de teléfonos móviles también plantea riesgos significativos para la salud y la seguridad. Estos dispositivos pueden contener cantidades de productos químicos que superan las normas de seguridad establecidas y que son más difíciles de recuperar mediante programas de gestión de residuos electrónicos. Esto repercute en particular en los países en desarrollo, que prácticamente no disponen de instalaciones de reciclaje adecuadas desde el punto de vista medioambiental y que tienen grandes cantidades de dispositivos móviles falsificados. Abordar el asunto de los dispositivos falsificados inhabilitando estos dispositivos complica aún más el problema para los países en desarrollo.

Los productos falsificados, debido a su mal ensamblado y la utilización de componentes de baja calidad, contienen sustancias peligrosas que están prohibidas en muchos países en cumplimiento de la normativa sobre restricciones a la utilización de sustancias peligrosas (RUSP) o de la legislación nacional equivalente.

Otro estudio reciente llevado a cabo por el Instituto Nokia de Tecnología en Brasil (INdT) sobre sustancias peligrosas ilustra los peligros potenciales de los teléfonos falsificados. En particular, el objetivo consistía en evaluar si los teléfonos falsificados cumplían la normativa RUSP y la Directiva de la UE sobre las restricciones a la utilización de algunas sustancias peligrosas en equipos eléctricos y electrónicos. Esta directiva limita el uso de seis materiales peligrosos en diversos tipos de equipos eléctricos y electrónicos.

Durante el estudio, que utilizó el método de pruebas de la norma CEI 62321 [75], se realizaron pruebas a cinco teléfonos falsificados y a 158 partes como tapas, pantallas, circuitos integrados, teclados y otros componentes montados sobre su superficie. El estudio del INdT reveló la presencia de dos substancias peligrosas (plomo y cadmio) tanto en componentes internos como externos y concentraciones muy superiores a los valores máximos permitidos por la normativa RUSP. La Figura A: Análisis químico de sustancias peligrosas en teléfonos móviles falsificados o de baja calidad del MMF – Guía de recursos para los gobiernos http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf ilustra la cantidad excesiva de plomo y cadmio encontrada en componentes internos y externos de los teléfonos móviles probados.

Otros estudios llevados a cabo en otros países han confirmado la existencia de sustancias peligrosas en teléfonos móviles falsificados. El Centro de Materiales para Tecnologías Electrónicas (Centre for Materials for Electronics Technology (C-MET)), de Hyderabad, India, emprendió un estudio para comprobar el cumplimiento de la normativa RUSP de los dispositivos móviles introducidos en el mercado indio. Para este estudio, el C-MET seleccionó para las pruebas 15 modelos de teléfono móvil ampliamente disponibles. Los teléfonos se eligieron en función de su popularidad y disponibilidad en el mercado indio y las pruebas se realizaron siguiendo los procedimientos de la norma CEI 62321 (2008).

El resultado fue que todos los teléfonos móviles falsificados contenían tasas alarmantemente altas de sustancias peligrosas, en particular plomo (Pb). En algunos casos, las cantidades eran 35 y hasta 40 veces superiores a los límites aceptables para el plomo en todo el mundo. Muchos de los componentes críticos, como la ranura de la tarjeta de memoria, la ranura del módulo de identificación de usuario (SIM), la cámara, etc., que se encuentran en contacto directo con el

usuario, demostraron ser los peores en cuanto a contenido de materiales peligrosos, lo que obviamente supone un mayor riesgo para los consumidores que si estos componentes estuvieran en el interior del dispositivo. Por el contrario, los teléfonos móviles comprobados provenientes de marcas mundiales y reconocidas demostraron cumplir los límites RUSP y ser, por tanto, seguros para el consumidor. La Figura B de la Guía de recursos para los gobiernos del MMF http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf presenta un resumen de los resultados del estudio, mientras la Figura C http://spotafakephone.com//docs/eng/MMF_CounterfeitPhones_EN.pdf muestra gráficamente las zonas en las que se pueden encontrar altas concentraciones de plomo.

Además, el uso de teléfonos con números de identidad internacional de equipos móviles (IMEI) duplicados/falsos/perdidos puede presentar amenazas para la seguridad nacional y personal que son difíciles de rastrear en la red.

Finalmente, como ejemplo de los ingresos que se pueden perder en el comercio de dispositivos móviles falsificados, la autoridad de Kenia contra la falsificación indica que el país perdió en torno a 38,5 millones USD debido a la comercialización de teléfonos falsificados [39]. La instalación de un sistema automatizado de información para el registro de terminales móviles en Ucrania (AISMTRU) en 2009 dio como resultado unos ingresos adicionales de 500 millones USD entre 2010 y 2012, obtenidos del pago de aranceles a la importación de terminales móviles. Antes de la implantación de este sistema en 2009, solo entre el 5% y el 7% de los dispositivos móviles utilizados en Ucrania se importaban legalmente, mientras que hoy en día del 92% al 95% se importan legalmente [40].

3.1.2 Accesorios y componentes para productos TIC

A menudo son los accesorios de los productos TIC que se venden los que están falsificados. En el caso de los teléfonos móviles, así como de otros productos TIC, se trata de las baterías, los cargadores y los auriculares. En el caso de las impresoras, a menudo se falsifican los cartuchos de tinta. En lo que respecta a las cámaras digitales, destacan lentes falsas que se adaptan correctamente al cuerpo de la cámara entre otros accesorios falsos como los cables y las tarjetas de memoria. Estos componentes falsificados pueden incluso llegar a ser los propios circuitos electrónicos. La sustitución accidental o intencionada con componentes electrónicos falsificados podría causar problemas graves a los usuarios cuando se utilizan en equipos médicos u otros productos TIC críticos desde el punto de vista de la seguridad. En 2013, se incautaron clones no autorizados MIFARE sin contrato durante la conferencia CarteS en París. http://www.mifare.net/files/6114/2295/3702/NXP_Whitepaper_Protect_your_reputation_with_genuine_MIFARE_products_2015.pdf.

La falsificación de baterías está muy extendida en todo el mundo y es causa de gran preocupación. Las baterías falsificadas son responsables de algunos incendios. Los tipos de baterías falsificadas van desde las alcalinas AA a las baterías recargables de litio-ión que utilizan muchos tipos diferentes de productos, en particular los teléfonos móviles.

Se ha informado de que las baterías falsificadas han causado muertes. http://www.bloomberg.com/apps/news?pid=newsarchive&sid=aLWvmmrHx9F0. En relación con ese informe, se destacó que las baterías falsificadas están muy extendidas en las zonas más pobres, dado que se usan más los teléfonos y, por tanto, se precisa cambiar de batería más a menudo.

Se han producido incidentes similares en países en todo el mundo. Resulta cada vez más preocupante que estas baterías causen problemas a bordo de aviones después de que se haya informado de algunos incidentes. En febrero de 2014, la filtración Geoff Leach de la Autoridad de aviación civil del Reino Unido dijo que estaban preocupados porque "las baterías baratas y falsificadas de origen dudoso adquiridas por Internet podrían fallar con consecuencias dramáticas". http://www.bbc.co.uk/news/business-25733346.

En 2004, un representante de Gillette, que declaraba como testigo ante el Comité Judicial del Senado de los Estados Unidos, explicó que en una operación de una semana habían incautado un millón de baterías Duracell entre muchos otros artículos falsificados. http://www.judiciary.senate.gov/meetings/counterfeiting-and-theft-of-tangible-intellectual-property-challenges-and-solutions & http://www.judiciary.senate.gov/imo/media/doc/Willard%20Testimony%20032304.pdf.

Los auriculares plantean un problema debido a que la mala calidad de los auriculares falsificados no solo puede afectar al oído sino también puede suponer un riesgo de incendio. En 2013, se informó que la policía había incautado teléfonos móviles falsificados por valor de 15 millones de libras esterlinas. http://www.express.co.uk/news/uk/387869/Designer-headphones-top-16m-deluge-of-fake-goods.

3.1.3 Radioteléfonos

Motorola Solutions Inc. ha advertido a sus clientes que no compren los radioteléfonos falsificados que se encontraron en Viet Nam en 2013. Estos radioteléfonos falsificados pueden resultar peligrosos para los usuarios; no solo se trata de copias de diseños de Motorola, sino que también muestran el logo y los números de serie de Motorola sin autorización, lo que hace que resulte difícil distinguirlos. http://uk.reuters.com/article/2013/07/09/motorola-solutions-idUSnBw085384a+100+BSW20130709.

3.1.4 Cámaras digitales

Las cámaras digitales forman parte de la larga lista de productos TIC que se están falsificando. Como ocurre con otros productos son muy difíciles de identificar y los vendedores, comerciantes y clientes voluntariosos ayudan a los consumidores para que sepan identificar las falsificaciones. http://www.ebay.co.uk/gds/How-to-Identify-a-Fake-Nikon-Camera-/10000000177984982/g.html. Los riesgos para la seguridad y la privacidad de dispositivos falsificados tales como las cámaras web pueden ser elevados para los usuarios. El software en estos productos no solo es de mala calidad e imperfecto inicialmente sino que el usuario tampoco tendrá actualizaciones de seguridad ni servicio técnico posteriormente, exponiéndose a riesgos en el ciberespacio.

3.1.5 Ordenadores personales y tabletas

La popularidad de ciertos tipos de ordenador y de tableta ha dado lugar a una falsificación muy extendida. En algunos casos estos productos son realmente "señuelos" que ni siquiera tienen una tarjeta electrónica. http://www.cnn.com/2013/03/22/tech/mobile/fake-ipads-walmart/. Para los que sí tienen electrónica, algunos tienen preinstalado software malicioso en las versiones falsificadas de los sistemas operativos. http://www.computerworld.com/s/article/9231277/Microsoft_finds_new_computers_in_China_preinstalled_with_malware.

3.1.6 Juegos electrónicos para niños

En 2014, la mayoría de los juegos para niños contienen elementos electrónicos de algún tipo. Desde las consolas de juego a los dispositivos de juego portátiles falsos, todos son potencialmente peligrosos para los niños. Como ejemplo de riesgo de seguridad se pueden citar las fuentes de alimentación sin toma de tierra que plantean riesgo de electrocución. http://www.theguardian.com/money/2011/dec/07/christmas-shopping-counterfeit-toys.

4 Convenios sobre Derechos de propiedad intelectual

Algunos acuerdos y convenios internacionales han promovido normas adecuadas para la protección de los derechos de propiedad intelectual, así como las excepciones y limitaciones permisibles, en leyes nacionales y definen los procedimientos necesarios que llevan a cabo los gobiernos para facilitar a la judicatura que tome medidas efectivas contra los actos delictivos.

4.1 Convenio de París para la Protección de la propiedad industrial y Convenio de Berna para la Protección de las obras literarias y artísticas

La Organización Mundial de la Propiedad Intelectual (OMPI) administra tratados multilaterales relativos a la propiedad intelectual. Los tratados fundamentales son el Convenio de París para la Protección de la propiedad industrial y el Convenio de Berna para la Protección de las obras literarias y artísticas.

El Convenio de París se ultimó en 1883 y ha sido revisado posteriormente en varias ocasiones. Su objeto es la protección de "las patentes de invención, los modelos de utilidad, los dibujos o modelos industriales, las marcas de fábrica o de comercio, las marcas de servicio, el nombre comercial, las indicaciones de procedencia o denominaciones de origen, así como la represión de la competencia desleal" [18]. En lo que se refiere a la falsificación, este convenio requiere a los estados contratantes que tomen medidas contra "la utilización directa o indirecta de una indicación falsa concerniente a la procedencia del producto o a la identidad del productor, fabricante o comerciante".

4.2 Aspectos de los Derechos de propiedad intelectual relacionados con el comercio (ADPIC) de la Organización Mundial del Comercio (OMC)

La Organización Mundial del Comercio (OMC) administra el Acuerdo sobre los ADPIC que establece las normas mínimas que deben aplicar todos los Miembros de la OMC tanto para proteger como para hacer valer los Derechos de propiedad intelectual en permanencia. El Acuerdo sobre los ADPIC introduce por lo tanto un conjunto completo de disposiciones sobre observancia por primera vez en un acuerdo multilateral. Cualquier diferencia entre los Miembros de la OMC en este ámbito se resolverá según lo dispuesto en el Entendimiento sobre solución de diferencias de la OMC.

Las disposiciones de los ADPIC sobre observancia tienen dos objetivos básicos, a saber, poner a disposición de los beneficiarios medios efectivos para la observancia y garantizar que los procedimientos de observancia son equilibrados y proporcionados y no impiden el comercio legítimo. Se dividen en cinco secciones. La primera sección establece las obligaciones generales que deben cumplir todos los procedimientos de observancia. Estos, sobretodo, se destinan a garantizar su eficacia y a que se cumplan ciertos principios básicos del proceso correspondiente. Las secciones siguientes tratan de los procedimientos y recursos administrativos y civiles, las medidas provisionales, las prescripciones especiales relacionadas con las medidas en frontera y los procedimientos penales.

El Acuerdo establece una distinción entre actividades de infracción en general, para las que deben estar disponibles los procedimientos y recursos administrativos, la falsificación y la piratería – las formas más evidentes e importantes de actividad delictiva – para los que son obligatorios ciertos procedimientos y recursos adicionales como las medidas en frontera y los procedimientos penales. Con este fin, se definen las mercancías falsificadas fundamentalmente como mercancías que implican la copia literal de la marca de fábrica y las mercancías piratas como aquellas mercancías que constituyan infracción del derecho de autor o de un derecho conexo.

Concretamente, las obligaciones de los Miembros de la OMC son las siguientes:

a) Procedimientos civiles y administrativos: Los titulares de derechos deben poder iniciar procedimientos judiciales civiles u, opcionalmente, administrativos contra los infractores de los derechos de propiedad intelectual. Estos procedimientos serán justos y equitativos. Se establecen ciertas normas para sustanciar pruebas. Además, se insta a los Miembros a que faculten a las autoridades judiciales para decretar tres tipos de recursos: amonestaciones, perjuicios y otros recursos. Para disuadir de los abusos, las obligaciones también contemplan la indemnización del demandado cuando el titular de los derechos haya abusado de los procedimientos de observancia.

b) Medidas provisionales: Los requerimientos judiciales provisionales constituyen un instrumento importante para la solución de una disputa en un juicio. Por tanto, las autoridades judiciales deben estar facultadas para ordenar medidas provisionales rápidas y eficaces a la hora de

actuar contra las infracciones alegadas. Como en otras secciones sobre observancia, se proporcionan ciertos requisitos de procedimiento y salvaguardias contra los abusos.

c) Medidas en frontera: Permiten al titular de los derechos obtener la cooperación de las administraciones de aduanas para interceptar mercancías infractoras en la frontera y evitar que esas mercancías sigan en circulación. Son obligatorias para mercancías infractoras, falsificadas y piratas, y los Miembros pueden también disponer de estas medidas ante la infracción de otros derechos de propiedad intelectual, mercancías infractoras destinadas a la exportación, mercancías en tránsito, importaciones insignificantes e importaciones paralelas. Las medidas en frontera están sujetas a ciertos requisitos de procedimiento y garantías contra los abusos similares a los de las medidas provisionales. En lo que respecta a los recursos, las autoridades competentes estarán facultadas para ordenar la destrucción o eliminación de las mercancías infractoras de los canales comerciales.

d) Procedimientos penales: Estos procedimientos deben establecerse para solucionar los casos de falsificación de marcas de fábrica o de piratería lesiva del derecho de autor a escala comercial. Su aplicación a otros derechos de propiedad intelectual es optativa. En términos de recursos, el acuerdo estipula que las sanciones deben incluir la prisión y/o sanciones pecuniarias y, cuando proceda, la confiscación, el decomiso y la destrucción de las mercancías infractoras y de todos los materiales y accesorios utilizados para producirlas.

Los países menos desarrollados Miembros de la OMC se benefician actualmente de disposiciones transitorias que les eximen de la obligación de aplicar las normas de protección y observancia establecidas en el Acuerdo sobre los ADPIC en general hasta el mes de julio de 2021, así como de cumplir las disposiciones relativas a la protección y observancia de las patentes y de los datos no publicados del sector farmacéutico hasta enero de 2016. El objetivo es, entre otros, permitir que estos países puedan dotarse de una tecnología viable.

5 Observancia de los Derechos de propiedad intelectual

Aunque están vigentes tratados internacionales relativos a la protección de los Derechos de propiedad intelectual desde hace más de un siglo, la observancia solo se ha tratado recientemente en los foros internacionales. Esto se debe a los fundamentos que figuran en el Acuerdo sobre los ADPIC y también a las repercusiones socioeconómicas crecientes de las infracciones de los derechos de propiedad intelectual. La observancia de estos derechos se encuentra ahora en los órdenes del día de muchas organizaciones internacionales, tales como la OMPI, la Organización Mundial de Aduanas (OMA) y la Interpol, de la Unión Europea y de muchas naciones.

5.1 Organización Mundial de la Propiedad Intelectual (OMPI)

La Organización Mundial de la Propiedad Intelectual (OMPI) creó su Comité asesor sobre observancia (ACE) en 2012 con fines de coordinación con otras organizaciones internacionales y el sector privado, para combatir la falsificación y la piratería. El Comité facilita programas de formación y realiza actividades de asistencia técnica.

La OMPI también está colaborando con el Programa de las Naciones Unidas para el Medio Ambiente (PNUMA) y con otras organizaciones como la Comisión Económica y Social para Asia y el Pacífico (CESPAP) de las Naciones Unidas para sensibilizar sobre los retos del reciclaje y la eliminación de cantidades crecientes de productos falsificados.
http://www.wipo.int/wipo_magazine/en/2012/06/article_0007.html
http://www.unep.org/ozonaction/News/Features/2012/SoutheastAsiaexploressynergies/tabid/104354/Default.aspx http://www.unescap.org/events/wipoescapunep-workshop-environmentally-safe-disposal-ip-infringing-goods

5.2 Organización Mundial del Comercio – Consejo sobre los ADPIC

El Consejo sobre los ADPIC es uno de los Consejos sectoriales de la OMC dependiente del Consejo General de la OMC. Está encargado de administrar el Acuerdo sobre los ADPIC y, en particular, de hacer un seguimiento de la ejecución del Acuerdo y del cumplimiento de las obligaciones de los Miembros relativas a este Acuerdo. El Consejo celebra reuniones formales en Ginebra tres veces al año y también mantiene reuniones informales cuando procede. Las reuniones constituyen un foro para el debate y la consulta de cualquier asunto relacionado con el Acuerdo sobre los ADPIC y, asimismo, para aclarar o interpretar las disposiciones del Acuerdo. La observancia de los Derechos de propiedad intelectual se ha debatido según las necesidades en el Consejo de los ADPIC en diversas ocasiones, siendo la última en 2012.

5.3 La Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD)

La ONUDD es quien custodia la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, que es la plataforma mundial para la cooperación en la lucha contra todas las formas de delincuencia organizada. Actualmente forman parte de la Convención 167 países que se han comprometido a luchar contra la delincuencia organizada mediante la colaboración y a garantizar que se estructuran adecuadamente sus legislaciones nacionales.

La ONUDD celebra reuniones semestrales de las Partes de la Convención de las Naciones Unidas contra la delincuencia organizada transnacional. Estas reuniones reúnen a los gobiernos de todo el mundo para promover y analizar la ejecución de la Convención con el fin de garantizar mejores planteamientos en la lucha contra la delincuencia organizada. La última reunión tuvo lugar en octubre de 2012.

La Oficina de las Naciones Unidas contra la Droga y el Delito se ha centrado en el vínculo entre el comercio de mercancías falsificadas y la delincuencia organizada transnacional http://www.unodc.org/counterfeit/. La ONUDD lanzó en enero de 2014 la campaña "Productos falsificados: no apoyes el crimen organizado" para sensibilizar al consumidor sobre el tráfico ilícito de mercancías falsificadas por valor de 250 000 millones USD al año. La campaña "Productos falsificados: no apoyes el crimen organizado" informa a los consumidores de que la compra de mercancías falsificada puede estar financiando a grupos de delincuentes organizados, amenaza la salud y la seguridad del consumidor, y contribuye a otros problemas éticos y medioambientales.

La ONUDD también trabaja para detener el flujo de mercancías ilícitas tales como productos falsificados y drogas mediante programas de asistencia técnica. La ONUDD y la Organización Mundial de Aduanas iniciaron en 2006 el Programa de fiscalización de contenedores (Container Control Programme (CCP)). Este programa ha logrado la incautación de 487 contenedores con mercancías fraudulentas y de contrabando, junto con 195 contenedores de droga.

https://www.unodc.org/unodc/en/frontpage/2014/January/counterfeit-dont-buy-into-organized-crime---unodc-launches-new-outreach-campaign-on-250-billion-a-year-counterfeit-business.html

https://www.unodc.org/unodc/en/frontpage/2012/July/criminals-rake-in-250-billion-per-year-in-counterfeit-goods-that-pose-health-security-risks-to-unsuspecting-public.html

5.4 Organización Mundial de Aduanas (OMA)

La OMA es una organización intergubernamental que comprende 179 administraciones de aduanas y proporciona liderazgo, asesoría y apoyo a sus Miembros para asegurar y facilitar el comercio legal, obtener beneficios, proteger a la sociedad y crear capacidad. Puesto que las administraciones de aduanas están encargadas de proteger las fronteras nacionales contra el flujo ilegal de mercancías falsificadas y piratas, la OMA lidera los debates sobre los esfuerzos mundiales para combatir dichos delitos. Esto implica potenciar los esfuerzos para combatir la falsificación y la piratería mejorando

los métodos de observancia y promoviendo el intercambio de información entre aduanas, así como entre aduanas y el sector privado.

El fin último del Programa sobre derechos de propiedad intelectual y salud y seguridad de la OMA es captar la atención de los agentes de aduana y de la industria en todo el mundo y garantizar su vigilancia respecto de los productos falsificados. Siendo la protección de la salud y de la seguridad de los consumidores la prioridad principal, la OMA es extraordinariamente activa en la organización de actividades intensivas de creación de capacidad y en el desarrollo de diversas herramientas de observancia.

Consciente de la importancia de la colaboración con el sector privado, la OMA trabaja muy estrechamente con los miembros del sector y con asociaciones con el fin de evaluar sus necesidades y dificultades cuando se enfrentan a este fenómeno. La OMA invita periódicamente a los titulares de derechos para que participen en sus diversas actividades contra la falsificación, tales como operaciones sobre el terreno y seminarios nacionales o regionales, y ha elaborado una herramienta en Internet, interfaz entre el público y los miembros (IPM), para dotar a los agentes de aduana con medios para detectar productos falsificados y piratas y para comunicar con los agentes económicos en tiempo real.

Las operaciones a gran escala son una parte vital de las iniciativas contra la falsificación de la OMA, en las que un gran número de administraciones de aduanas aumentan simultáneamente su nivel de persecución de los elementos falsificados para cuantificar y calificar el impacto de las actividades mundiales de falsificación. Solo durante el año 2013, las autoridades de aduanas interceptaron más de 1 100 millones de elementos falsificados en una operación en la región de África y en una operación en la región de América Latina.

La OMA también ha elaborado una herramienta de detección mundial por Internet, IPM, destinada a los agentes de aduana en activo para facilitar la distinción entre productos genuinos y sus reproducciones falsificadas. Desde su lanzamiento en 2010, IPM se ha convertido en un centro real de comunicaciones entre agentes de aduana sobre el terreno y el sector privado permitiendo el intercambio de información crucial en tiempo real con el fin de interceptar mercancías falsificadas.

Con el lanzamiento reciente de IPM, los agentes de aduana pueden ahora acceder a IPM mediante sus dispositivos móviles y recopilar toda la información pertinente incluida en la base de datos. Esta nueva versión ofrece la posibilidad de utilizar dispositivos móviles para escanear los códigos de barras normalizados GS1 del sector que figuran en millones de productos, permitiendo la búsqueda en la base de datos de productos de una forma más rápida y eficiente. Es más, el examen de los códigos de barras permitirá la conexión automática a cualquier servicio de autenticación vinculado al producto controlado. Esta nueva característica se conoce como Conectado a IPM – una red mundial de proveedores de características de seguridad (SFP) que hace de interfaz con el IPM. Con esta red de SFP en crecimiento, también se está incrementando el número de titulares de derechos que se unen al IPM, superando actualmente las 700 marcas, que cubren una amplia gama de sectores industriales desde el farmacéutico, la alimentación o los pesticidas hasta mercancías de rápido consumo y artículos de lujo [16].

5.5 Unión Europea

En la Unión Europea se lleva a cabo, desde 2011, una serie de consultas públicas sobre la Directiva 2004/48/EC relativa al respeto de los derechos de propiedad intelectual. La anterior consulta pública sobre la eficacia de los sistemas de observancia civil en materia de propiedad intelectual en los Estados Miembros de la UE finalizó en marzo de 2013. La Comisión Europea publicó un resumen de las respuestas en julio de 2013.

La Comisión adoptó, el 1 de julio, la Comunicación "Hacia un consenso renovado sobre el respeto de los derechos de propiedad intelectual: Un plan de acción de la UE" – COM (2014)932.

Las diez acciones enumeradas en el Plan de Acción se centran en las infracciones a nivel comercial (el denominado método de "seguir el dinero") y están destinadas a mejorar la prevención, aumentar la cooperación transfronteriza entre Estados Miembros y dar prioridad a la política de observancia en materia de propiedad intelectual a partir de datos objetivos.

El Observatorio Europeo de la Falsificación y la Piratería fue creado en 2009 como parte de la Comisión Europea. Mediante el Reglamento Nº 386/2012 del Parlamento Europeo y el Consejo pasó a llamarse Observatorio Europeo de las Vulneraciones de los Derechos de Propiedad Intelectual, plenamente dependiente de la Oficina de Armonización del Mercado Interior desde el 5 de junio de 2012. El Observatorio sirve de plataforma donde los actores públicos y privados pueden compartir prácticas idóneas y experiencias en materia de aplicación de los DPI, pueden sensibilizar al público y colaborar en la recopilación de datos y su examen.

La Comisión Europea elevó al nivel de la UE un Memorándum de Acuerdo sobre la venta de mercancías falsificadas a través de Internet. Este Memorándum fue concluido en mayo de 2011 entre plataformas Internet, titulares de derechos de propiedad intelectual y asociaciones profesionales. En el Memorándum de Acuerdo se establece un código de práctica para luchar contra la venta de mercancías falsificadas en Internet y para aumentar la colaboración entre los signatarios.

Aduanas

El Reglamento Nº 1383/2003 del Consejo, de 22 de julio de 2003, relativo a la intervención de las autoridades aduaneras en los casos de mercancías sospechosas de vulnerar determinados derechos de propiedad intelectual, fue sustituido por el Reglamento 608/2013.

5.6 Interpol

Interpol, la organización internacional de la policía con 190 países miembros, creó en 2002 un Grupo de acción dedicado a combatir los delitos que atentan contra la propiedad intelectual. Este grupo apoya las operaciones regionales y mundiales para decomisar mercancías falsificadas, organiza cursos de formación con el International IP Crime Investigators College (IIPCIC) y ha creado una base de datos relativa a los delitos internacionales contra la propiedad intelectual.

5.7 Comisión Económica de las Naciones Unidas para Europa (CEPE)

El Grupo de Trabajo de la CEPE sobre cooperación en materia de reglamentación y políticas de normalización (GT.6) ha creado un grupo asesor sobre vigilancia del mercado (grupo MARS) que pretende alentar a los estados miembros a que coordinen sus esfuerzos para reducir el problema de las mercancías falsificadas. Han elaborado la 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" [18].

5.8 Iniciativas nacionales (algunos ejemplos)

5.8.1 Francia

El CNAC (*Comité National Anti Contrefaçon*) es el comité nacional francés contra la falsificación http://www.industrie.gouv.fr/enjeux/pi/cnac.php

y el INPI (*Institut National pour la Propriété Industrielle*) es el instituto nacional para la propiedad industrial http://www.inpi.fr/fr/accueil.html. El Ministerio de Finanzas (*Ministère de l'économie et des finances*) también está implicado en las actividades contra la falsificación. http://www.economie.gouv.fr/signature-deux-nouvelles-chartes-lutte-contre-contrefacon-sur-internet

5.8.2 Oficina de la propiedad intelectual del Reino Unido

La oficina de la propiedad intelectual del Gobierno del Reino Unido creó el Grupo de delitos contra la propiedad intelectual en 2004. Elabora un informe anual sobre los delitos contra la propiedad intelectual y también ha proporcionado una herramienta para la cadena de suministro [19]. El Reino Unido dispone también de un Ministerio para la propiedad intelectual.

5.8.3 Agencia contra la falsificación de Kenya

El Parlamento de Kenya aprobó la ley contra la falsificación (Nº 13) en 2008. Esta ley prohíbe el comercio de mercancías falsificadas y también crea la Agencia contra la falsificación [20].

5.8.4 US – Comisión conjunta sobre comercio y transacciones comerciales de China

Los Estados Unidos y China han establecido una Comisión conjunta sobre comercio. En su vigesimocuarta reunión en diciembre de 2013, el grupo nacional rector de China en materia de lucha contra la infracción de los derechos de propiedad intelectual y el grupo sobre fabricación y venta de mercancías falsificadas y de baja calidad se comprometieron a adoptar un plan de acción en 2014 que incluyera la sensibilización de la población, los requisitos para el cumplimiento de todas las leyes y reglamentos relativos a la protección de la propiedad intelectual y las políticas de observancia de la ley. www.commerce.gov/news/fact-sheets/2013/12/20/fact-sheet-24th-us-china-joint-commission-commerce-and-trade-fact-sheet

6 Foros de la industria contra la falsificación

Las empresas han reaccionado ante el problema de la falsificación mediante la creación de foros para defender sus intereses. Estos foros facilitan información sobre la amplitud del problema, sugieren formas de reducir los efectos de la falsificación y colaboran con los gobiernos y con organizaciones internacionales para tomar medidas contra la falsificación.

6.1 Cámara de Comercio Internacional (CCI)

La CCI representa a las empresas de todo el mundo. Son miembros miles de empresas y asociaciones de cerca de 120 países. Actúa en nombre de las empresas creando representaciones ante los gobiernos y organizaciones intergubernamentales. La CCI se fundó en 1919 y creó el Tribunal Internacional de Arbitraje de la CCI en 1923.

La CCI estableció la Oficina de información sobre falsificación en 1985 y, recientemente, la iniciativa de lucha contra la falsificación y la piratería (BASCAP).

La Oficina de información sobre falsificación de la CCI mantiene una base de datos de estudios de caso y también presta servicios de investigación.

La BASCAP prosiguió el estudio de las repercusiones económicas y sociales de la falsificación y la piratería que inició la OCDE [4] y ha creado un centro de intercambio de información que facilita información por países [21] y sectores [22] así como la protección de marcas [23] y directorios de contactos de todo el mundo [24].

La CCI publica también un programa de trabajo sobre la propiedad intelectual [25].

6.2 Coalición internacional contra la falsificación (IACC)

La IACC [26] se fundó en 1979 y tiene miembros de todos los sectores industriales. Su objeto es la lucha contra la falsificación y la piratería promoviendo leyes contra la falsificación.

6.3 Foro de fabricantes de sistemas móviles (MMF)

El Foro de Fabricantes de Sistemas Móviles mantiene una página en Internet (spotafakephone.com) que facilita información sobre teléfonos y baterías falsificados.

6.4 Association of Service and Computer Dealers International and North American Association of Telecommunications Dealers (AscdiNatd)

La AscdiNatd ha elaborado un programa contra la falsificación que incluye una política contra la falsificación que adoptan las empresas miembro y recursos de información sobre productos falsificados, incluida información proveniente de HP y Cisco [27].

6.5 Alliance for Gray Market and Counterfeit Abatement (AGMA)

3Com, Cisco Systems, Hewlett-Packard, Nortel y Xerox formaron la AGMA en 2001 con el objetivo de combatir el comercio de productos de alta tecnología falsificados.

6.6 Grupo de Trabajo contra la falsificación de la British Electrotechnical and Allied Manufacturers Association (BEAMA)

La BEAMA es una base de conocimientos y un foro de expertos independientes para la industria electrotécnica para el Reino Unido y toda Europa. Representa a más de 300 fabricantes del sector electrotécnico y tiene una influencia notable a escala internacional así como en las políticas comerciales y de normalización del Reino Unido.

El Grupo de Trabajo de la BEAMA contra la falsificación (ACWG) se constituyó en 2000. Su objetivo es actuar contra los fabricantes de productos de instalaciones eléctricas falsificados y contra los comerciantes que los distribuyen en muchos mercados internacionales, incluidos los de Europa, Oriente Medio y África. Al igual que los miembros de la BEAMA, el GT incluye muchas de las asociaciones líderes del sector dedicadas a la instalación, distribución, pruebas y certificación y los sectores responsables del cumplimiento de las leyes. Ha conseguido el reconocimiento mundial por su trabajo proactivo y colabora con asociaciones comerciales y organismos dedicados a la aplicación de las leyes de todo el mundo.

Se ha creado una base de datos de falsificadores para que la utilice el sector de instalaciones eléctricas, que se ha trasferido a las autoridades en todo el mundo para que realicen el seguimiento en los mercados locales.

Las actividades de los grupos de trabajo se divulgan mediante artículos en revistas, presentaciones, participaciones en conferencias y mediante la elaboración de guías y carteles para sensibilizar sobre esta amenaza para la seguridad del consumidor y la integridad de las empresas que crece con rapidez y puede ser perniciosa.

Este Grupo de Trabajo es responsable de gestionar proyectos de acción contra la falsificación, recopilando y difundiendo información sobre asuntos relacionados con la protección de los derechos de propiedad intelectual y de responder ante el gobierno y otros organismos en nombre de la asociación. Ofrece también asesoramiento e información a cualquier empresa o asociación que tenga algún problema con asuntos relacionados con los derechos de propiedad intelectual.

Entre las actividades actuales figuran proyectos en China, los Emiratos Árabes Unidos, el Reino Unido, Nigeria e Iraq, además de programas completos de vigilancia de puertos y en la web.

En el Reino Unido, la BEAMA está trabajando con muchos de los organismos industriales punteros para sensibilizar y luchar contra los productos falsificados o de baja calidad – se ha creado el portal www.counterfeit-kills.co.uk para este fin concreto.

6.7 UKEA (United Kingdom Electronics Alliance)

La UKEA es un consorcio de asociaciones comerciales del Reino Unido que representan al sector de la electrónica. Su objetivo es coordinar los debates sobre asuntos relativos al sector e informar al gobierno. La UKEA ha creado un Foro contra la falsificación [28] que publica información sobre el problema de los componentes electrónicos falsificados, las posibles soluciones y las mejores prácticas.

6.8 Anti-Counterfeiting Group (ACG)

El ACG es una asociación de comercio del Reino Unido creada en 1980 con miembros provenientes fundamentalmente del sector de la automoción, aunque actualmente representa a la mayoría de los sectores industriales.

6.9 UNIFAB – *Union des Fabricants*

La *Union des Fabricants* es una organización francesa dedicada a la lucha contra la falsificación mediante la sensibilización de la población (gracias a la apertura de un museo de la falsificación entre otras actividades), que facilita información a las empresas y medios de presión.
http://www.unifab.com/en/

6.10 International Electronics Manufacturing Initiative (iNEMI)

La iNEMI ha definido un proyecto sobre "Componentes falsificados – Metodología de evaluación y desarrollo de medidas".
http://thor.inemi.org/webdownload/projects/Miniaturization/Counterfeit_WhitePaper_110513.pdf.

7 Medidas para luchar contra los equipos falsificados

7.1 Introducción

Se puede luchar contra la falsificación fabricando productos de forma que se puedan autentificar mediante un control estricto de sus ciclos de vida. Se pueden adosar a los productos etiquetas difíciles de fabricar y asignar números de serie que se puedan utilizar para demostrar que el elemento es auténtico (accediendo a una base de datos, por ejemplo).

Se pueden asignar identificadores únicos a cada elemento. mPedigree es un ejemplo de sistema utilizado para combatir la falsificación de productos farmacéuticos en África. Este sistema permite que los consumidores comprueben si los medicamentos son genuinos o falsificados y potencialmente peligrosos enviando sin coste un mensaje corto (SMS) a un registro de productos farmacéuticos.

Para garantizar la seguridad del producto y que se mantiene la adecuada calidad, es necesario un control estricto de las cadenas de suministro, y probablemente de todos ciclos de vida de los productos, mediante pruebas, evaluaciones y certificación. Además, es preciso dotar a los funcionarios de aduanas con herramientas para identificar productos falsificados y se pueden emplear mecanismos de vigilancia del mercado.

Los identificadores se pueden adosar a un objeto en texto sin cifrar o se puede codificar en una "etiqueta de identificación (ID)" como un código de barras, una etiqueta de identificación por radiofrecuencia (RFID), una tarjeta inteligente o un marcador por infrarrojos de forma que se pueda leer automáticamente. En la identificación de un objeto se pueden distinguir tres niveles. En primer lugar, se encuentra el nivel del propio identificador en el que los objetos se identifican de manera exclusiva, por ejemplo, mediante un código de producto electrónico (EPC). El segundo nivel es un nivel de codificación puesto que los propios identificadores se pueden codificar en diferentes formatos, y finalmente está la ejecución física, en la que se escribe la identidad codificada, por ejemplo, en una etiqueta RFID.

Para garantizar que los identificadores son únicos en todo el mundo para aplicaciones concretas, deben gestionarse de forma organizada, con algún tipo de procedimiento de atribución. Por ejemplo, la Asociación GSM (GSMA) gestiona las identidades internacionales de los equipos móviles (IMEI) para el sistema mundial de comunicaciones móviles (GSM), para el sistema de telecomunicaciones móviles universales (UMTS) y para dispositivos de evolución a largo plazo (LTE); la Asociación del sector de las telecomunicaciones atribuye los identificadores de los equipos móviles (MEID) para dispositivos con acceso múltiple por división de código (AMDC) y

GS1 gestiona los identificadores de código de barras. La ISO gestiona algunos dominios de identificadores y también actúa como la autoridad superior, incorporando los esquemas de identificador de otras organizaciones como la GS1.

Otro ejemplo es la marcación de los equipos para indicar que han sido aprobados para su comercialización en un determinado país. Por ejemplo, Anatel obliga a que los cargadores y baterías de sus teléfonos móviles lleven una etiqueta segura definida en su Resolución 481/2007[2]. Véase la Figura 1.

Figura 1 – Ejemplo de etiqueta segura exigida por Anatel definida en su Resolución 481/2007

Este planteamiento se ha utilizado en el sector de los equipos de telecomunicaciones durante muchos años y se llevó a cabo con éxito en algunos países y algunas regiones[3] (por ejemplo, FCC[4], Anatel[5], UE[6]).

Los funcionarios de aduanas deben ser capaces de identificar productos falsificados y de vigilar el mercado y de aplicar otras medidas necesarias para la observancia de la ley. Además, se puede identificar a los importadores con antecedentes de ignorar los controles de importación e incluirlos en una lista especial. Cuando importadores clandestinos importan envíos de equipos TIC se puede alertar al organismo regulador para que pueda tomar medidas y llevar a cabo inspecciones con el fin de garantizar el cumplimiento de las leyes. Véase la Figura 2.

---

2 https://translate.google.com/translate?sl=pt&tl=en&js=y&prev=_t&hl=fr&ie=UTF-8&u=legislacao.anatel.gov.br%2Fresolu%C3%A7%C3%B5es%2F2007%2F192-resolu%C3%A7%C3%A3o-481&edit-text=

3 Mediante algún sistema de evaluación de conformidad, que puede necesitar certificación, declaración de conformidad y/o aplicando Acuerdos de Reconocimiento Mutuo (MRA).

4 https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=30744&switch=P

5 http://www.anatel.gov.br/grandeseventos/en/frequently-asked-questions-faqs

6 http://exporthelp.europa.eu/thdapp/display.htm?page=rt%2frt_TechnicalRequirements.html&docType=main&languageId=en

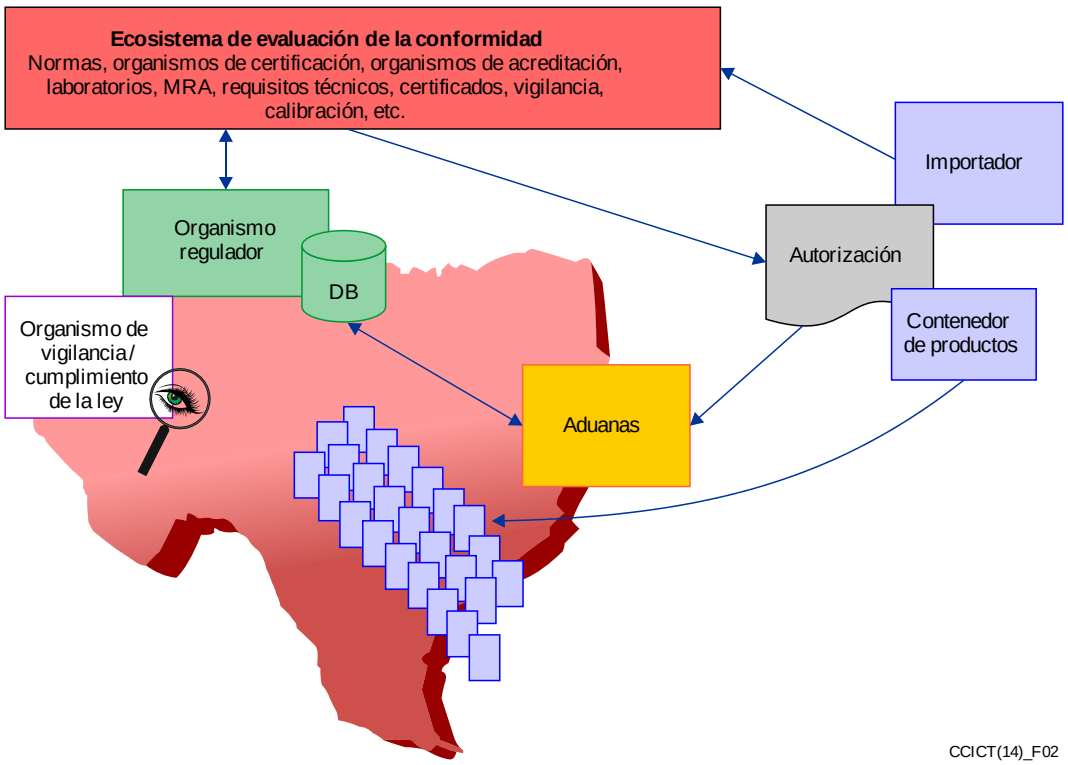

Figura 2 – Ecosistema de evaluación de la conformidad

Cabe destacar que los productos falsificados podrían de hecho cumplir determinados requisitos, interactuar con productos auténticos y, por tanto, superar las pruebas de conformidad y de interfuncionamiento. En este caso, puede ser necesaria la evaluación por el propietario de la marca registrada para identificar con precisión los productos falsificados y distinguirlos de los productos auténticos.

El sector de las TIC se distingue por la amplia presencia de competidores internacionales que promueven una innovación constante. Aunque sea una condición deseable, el mercado, al mismo tiempo, está expuesto a fabricantes y vendedores nada comprometidos con el cumplimiento de las normas vigentes internacionales, regionales o nacionales.

El problema de la información asimétrica resulta más evidente en los países en desarrollo, en los que poco o nada se han desarrollado tecnologías y procedimientos de evaluación de la conformidad. Los problemas típicos a los que habitualmente se enfrentan al gestionar sistemas de evaluación de la conformidad son la falta de información contrastada y comprobable como en los casos siguientes: i) identificación del origen o del responsable jurídico de los productos; ii) emplazamientos de los fabricantes; iii) organismos de certificación; y iv) laboratorios cualificados con certificados de acreditación legitimados. En algunos casos, importadores sin conocimientos técnicos ni capacidad para proporcionar asistencia pueden representar a empresas extranjeras que han subcontratado sus unidades de ingeniería y de fabricación en otros países (por ejemplo, esquemas de subcontratación). Aunque estos procesos supongan un ahorro en los procesos de producción, la calidad y la responsabilidad en la fabricación de equipos de telecomunicaciones y de las TIC se ven disminuidas.

Uno puede suponer que los intereses, la codicia, la falta de normas y/o su escasa aplicación redundan en equipos de baja calidad. En algunos casos, equipos de la misma marca o modelo, certificados, están hechos y vendidos con componentes electrónicos diferentes, algunos buenos, otros malos, y enviados a un destino u otro, en función de su laxitud con la calidad. El procedimiento conocido como tropicalização (tropicalización en portugués) viene a la mente como

un ejemplo de este comportamiento con los equipos destinados a la venta al Sur del Ecuador. Véase la Figura 3.

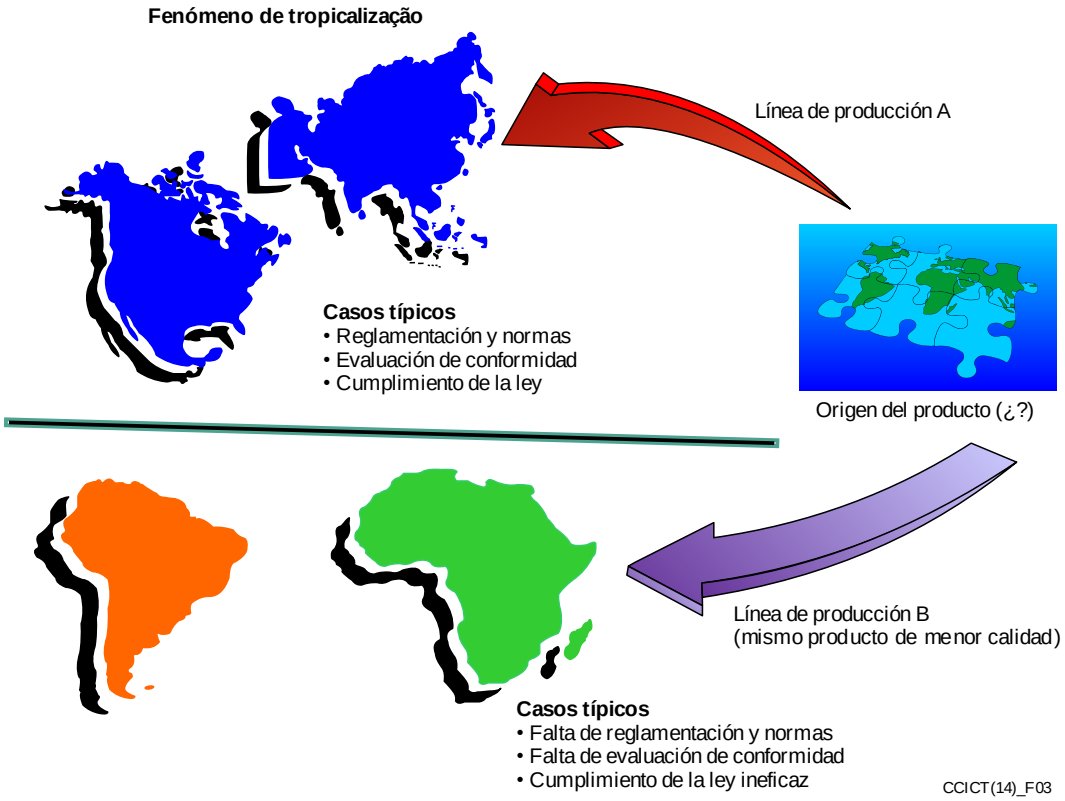

Figura 3 – Procedimiento conocido como tropicalização (tropicalización en portugués)

7.2 Falsificación de identificadores y de logotipos de homologación

Todos los identificadores generados por fabricantes de mercancías auténticas pueden y son falsificados por falsificadores con el fin de lograr sus objetivos de engañar al consumidor y a las autoridades para hacerles creer que el producto es genuino. Es un problema para muchos sectores, no sólo para el de las TIC. El lector debe tener en cuenta que cualquier mecanismo de identificación y su seguridad pueden ser el objetivo de los falsificadores y de los delincuentes. Los logotipos e iconos de homologación así como los identificadores electrónicos a menudo se subvierten deliberadamente con el fin de evadir el control de las aduanas y el cumplimiento de la ley en las fronteras. Esto genera problemas prácticos para los fabricantes, los consumidores y los funcionarios encargados de las aduanas y de observancia de la ley que tienen dificultades a la hora de identificar las marcas de identificación fraudulentas de las auténticas, incluso antes de tomar en consideración el propio producto.

7.3 Identidad internacional de equipo móvil (IMEI)

Como se ha indicado anteriormente, los teléfonos móviles han sido un objetivo particularmente atractivo para los falsificadores y, a su vez, el Foro de fabricantes de dispositivos móviles (MMF) ha creado una página web que ofrece información a los consumidores sobre cómo detectar teléfonos y baterías falsificados. http://spotafakephone.com. Advierten de que se debe conocer la apariencia, capacidades, disponibilidad y precio de los artículos auténticos y también se debe comprobar el número de identidad internacional del equipo móvil (IMEI). La IMEI es un identificador exclusivo para cada teléfono móvil y las falsificaciones a menudo no tienen una IMEI o tienen un número falso. Un problema para los fabricantes, operadores de red y autoridades es que los falsificadores han mejorado su fabricación de forma que a veces el robo de números legítimos de los fabricantes

forma parte de su estrategia de falsificación y se puede utilizar este método para que sus sistemas superen las comprobaciones de los números IMEI.

La atribución de las IMEI corresponde a la GSMA para garantizar que sean únicos. El esquema de atribución es jerárquico, asignando la GSMA identificadores de dos dígitos a órganos notificantes que atribuyen posteriormente la IMEI y el número de serie a cada equipo. Los órganos notificantes autorizados actualmente para asignar IMEI son la CTIA – Asociación Inalámbrica, la BABT (British Approvals Board for Telecommunications), el TAF (Telecommunications Terminal Testing and Approval Forum) (China) y la MSAI (Mobile Standards Alliance of India).

El formato de IMEI válido desde el 1 de enero de 2013 se muestra en la Figura 4 [37]:

Código de homologación (TAC)	Número de serie	Dígito de comprobación
NNXXXX YY	ZZZZZZ	A

TAC	Código de homologación
NN	Identificador del órgano notificador
XXXXYY	Identificador del tipo de equipo móvil definido por el órgano notificador
ZZZZZZ	Atribuido por el órgano notificador pero asignado a cada equipo móvil por el fabricante
A	Dígito de comprobación, definido como una función del resto de dígitos de la IMEI

Figura 4 – Formato de IMEI

La GSMA registra información adicional, como el nombre del fabricante y el número de modelo y características técnicas como las bandas de frecuencias y el consumo de potencia, para cada dispositivo identificado por su IMEI.

La GSMA mantiene la base de datos de IMEI (IMEI DB) [38], denominada anteriormente como el Registro Central de Identidad de Equipos (CEIR). La IMEI DB incluye una "lista blanca" con los equipos que se consideran adecuados para su uso en todo el mundo y una "lista negra" de IMEI relativa a dispositivos que no se consideran adecuados para su uso por haber sido perdidos, robados o ser defectuosos planteando una amenaza para la integridad de la red. Conviene destacar que la lista blanca de la IMEI DB es una lista de TAC en lugar de IMEI completos y los datos están disponibles gratuitamente a determinadas entidades, incluidos los reguladores nacionales, agencias responsables del cumplimiento de la ley y agentes de aduanas. Además de la IMEI DB, los propios operadores de redes pueden implementar sus propios registros de identidad de equipos (EIR), en los que pueden descargar la "lista blanca", lo que les permite controlar qué dispositivos pueden acceder a sus redes. http://www.gsma.com/managedservices/mobile-equipment-identity/the-imei-database/accessing-the-imei-database/

El fin fundamental de la IMEI DB consiste en ayudar a los operadores a identificar los dispositivos, y sus características, que se utilizan en sus redes y en bloquear los teléfonos perdidos. La IMEI DB también se puede usar para detectar dispositivos falsificados, lo que contribuye a impedir el blanqueo de dispositivos y la delincuencia y contribuye a su persecución.

No obstante, surgieron problemas a la hora de implementar la IMEI. Se ha informado de casos de equipos sin IMEI, con una IMEI con solo ceros, IMEI duplicadas e IMEI asignadas por organizaciones no autorizadas. Algunos de estos dispositivos con IMEI no válidos o no únicos son falsificaciones pero otros son auténticos aunque no cumplan el procedimiento de atribución de IMEI de la GSMA debido a malentendidos de los fabricantes. Por ejemplo, se estima que existen 30 millones de teléfonos GSM en India sin IMEI y la GSMA autorizó a la MSAI para que

propusiera un programa temporal de amnistía para implantar IMEI genuinos (programa de implantación de IMEI genuinos (GII)) con el fin de poder identificar cada dispositivo de forma unívoca.

Como ejemplo de IMEI duplicado, en Australia se han detectado 6 500 teléfonos con la IMEI 135790246811220. En lo que respecta a las IMEI no registradas, un operador de red en Uganda ha informado que la cantidad de TAC que no están registrados en la IMEI DB es mayor que el número atribuido por la GSMA y que están registrados en la IMEI DB.

Existe, por lo tanto, una buena razón para garantizar que el uso de la IMEI esté controlado y que se asignen las IMEI de conformidad con el proceso de la GSMA. La IMEI DB es una herramienta para detectar móviles falsificados y, por dar un ejemplo, Kenya negó el acceso a móviles con IMEI no válidos a partir de finales de septiembre de 2012 puesto que se estimaba que existían 2,3 millones de abonados con teléfonos falsificados. El Anexo A facilita más información sobre estos ejemplos y otros casos en los que se han utilizado las IMEI para identificar los teléfonos móviles falsificados. Puesto que varias iniciativas nacionales destinadas a afrontar el problema de los dispositivos móviles falsificados se basan en el uso de IMEI, es fundamental que el procedimiento de asignación de IMEI y la base de datos sean seguros y fiables y que la IMEI esté codificada con seguridad dentro de los dispositivos.

Una posibilidad es exigir a los operadores que bloqueen los dispositivos con una IMEI duplicada o no válida ya que estos dispositivos deben ser autenticados en la red para poder funcionar. Bloquear estos dispositivos cuando se conectan por primera vez es probablemente la forma más efectiva de resolver el problema actualmente.

No obstante, se plantean varias limitaciones para bloquear los dispositivos. La primera es que la GSMA no mantiene una lista blanca completa sino más bien una lista blanca de códigos TAC. En segundo lugar, las IMEI de dispositivos legítimos se han clonado en dispositivos falsificados y de baja calidad lo que complica el proceso de bloqueo y, finalmente, cualquier solución de bloqueo debe evitar o prohibir que se copien otros IMEI clonados en los dispositivos en cuestión.

Aunque el bloqueo plantea retos, existen soluciones disponibles en el mercado. Al mismo tiempo, resulta importante evitar la aplicación parcial de soluciones nacionales propias que sencillamente trasladarán el problema a través de las fronteras nacionales. Puesto que las IMEI son atribuidas por la GSMA y que es la GSMA quien mantiene la IMEI DB, parecería lógico que se implicara de alguna manera en las iniciativas nacionales con el fin de utilizar la serie completa de listas disponibles y otras medidas técnicas.

Sin embargo, teniendo en cuenta que la cantidad de dispositivos falsificados es sencillamente enorme, no se puede pasar por alto que bloquear sólo los terminales operativos causaría serios e inesperados problemas a las redes y a los usuarios finales.

A este respecto, es importante tener en cuenta el hecho de que en los países en desarrollo, con condiciones sociales y económicas limitadas, los teléfonos móviles son el principal medio de comunicación y de participación en la sociedad de la información[7]. Desgraciadamente, esto se consigue utilizando una cantidad considerable de dispositivos baratos y falsificados.

Por esta razón, toda la sociedad debe estar preparada para este cambio. Hay que estudiar, considerar y planificar los mejores planteamientos. Por ejemplo, se deben explicar con claridad a los consumidores los motivos (riesgos de seguridad, baja calidad del servicio y aumento consiguiente de las reclamaciones, riesgos de interferencias e incumplimiento de los derechos de propiedad intelectual, etc.) para no permitir el uso de dispositivos falsificados.

---

[7] Iniciativa de la UIT M-Poderar el desarrollo: http://www.itu.int/en/ITU-D/Initiatives/m-Powering/Pages/default.aspx.

En este sentido, si los reguladores y los gobiernos eligen poner en práctica el bloqueo de terminales, resulta importante adoptar políticas de transición, tales como empezar bloqueando únicamente los terminales nuevos y permitir que sigan funcionando dispositivos que están de alta en la red, aunque finalmente, los usuarios tendrán que cambiar sus dispositivos por dispositivos auténticos puesto que el ciclo de vida estimado de un terminal móvil es de 18 meses[8].

7.4 Identificadores únicos

Los códigos de producto electrónico (EPC) se desarrollaron en primer lugar en el Centro Auto-ID del Instituto Tecnológico de Massachusetts que se creó en 1999 y, actualmente, están gestionados por EPCglobal, una filial de GS1 que ha definido la especificación más ampliamente utilizada por los sistemas mundiales de cadenas de suministro. La Organización Internacional de Normalización (ISO) y el Ubiquitous ID Centre (Japón) también han definido identificadores para algunas aplicaciones.

GS1 define nueve "claves de identificación" para la identificación de elementos, emplazamientos, contenedores de transporte, bienes, servicios, documentos, envíos y transporte, de la forma siguiente:

- GTIN – número mundial de artículo comercial
- GLN – número mundial de localización
- SSCC – código seriado de contenedor de embarque
- GRAI – identificador mundial de bienes retornables
- GIAI – identificador mundial de bienes individuales
- GSRN – número mundial de relación de servicio
- GDTI – identificador mundial de tipo de documento
- GSIN – número mundial de identificación de embarque
- GINC – número mundial de identificación para el envío

El GTIN se utiliza para identificar categorías de objetos mientras GLN, SSCC, GIAI y GSRN identifican objetos individuales; GRAI y GDTI se pueden utilizar para identificar categorías de objetos o artículos individuales dependiendo de si disponen o no de un número de serie. El GINC y el GSIN identifican agrupaciones lógicas en lugar de objetos físicos. Estas claves de identificación pretenden racionalizar del uso de los códigos de barras. Existe una correspondencia entre estos códigos y los EPC definidos por EPCglobal para su uso con etiquetas RFID. El GTIN se complementa en el esquema EPC añadiendo un número de serie de forma a identificar un objeto unívocamente. Las restantes claves que se usan para identificar objetos individuales tienen un equivalente directo en EPC. Se han definido los siguientes EPC [41]:

- Identificador general (GID)
  - urn:epc:id:gid:*Númerodegestor.Clasedeobjeto.Númerodeserie*
- Número mundial seriado artículo comercial (SGTIN)
  - urn:epc:id:sgtin:*Prefijodelacompañia.Referenciadelartículo.Númerodeserie*
- Código seriado de contenedor de embarque (SSCC)
  - urn:epc:id:sscc:*Prefijodelacompañía.Referenciadelaserie*
- Número mundial de localización con o sin ampliación (SGLN)

[8] http://www3.epa.gov/epawaste/education/quest/pdfs/unit1/chap2/u1-2_product-life.pdf: "Los teléfonos móviles sólo se usan durante un promedio de 18 meses antes de ser sustituidos, aunque puedan funcionar durante mucho más tiempo".

  - urn:epc:id:sgln:*Prefijodelacompañía.Referenciadelocalización.Ampliación*
- Identificador mundial de bienes retornables (GRAI)
  - urn:epc:id:grai:*Prefijodelacompañía.Tipodebien.Númerodeserie*
- Identificador mundial de bienes individuales (GIAI)
  - urn:epc:id:giai:*Prefijodelacompañía.Referenciadelbienindividual*
- Identificador mundial de tipo de documento (GDTI)
  - urn:epc:id:gdti:*Prefijodelacompañía.Tipodedocumento.Númerodeserie*
- Número mundial de relación de servicio (GSRN)
  - urn:epc:id:gsrn:*Prefijodelacompañía.Referenciadelservicio*
- Ministerio de Defensa de EE.UU. (DoD)
  - urn:epc:id:usdod:*CAGEOrDODAAC.Númerodeserie*
- Identificador aeroespacial y de defensa (ADI)
  - urn:epc:id:adi:*CAGEOrDODAAC.Númerooriginaldeparte.Serie*

La norma ISO/CEI 15459 [42] define identificadores únicos para el seguimiento de la cadena de producto que se pueden representar en medios automáticos de identificación y captura de datos (AIDC) tales como los códigos de barras y los RFID.

Las partes 1, 4, 5, 6 y 8 de ISO/CEI 15459 especifican la cadena de caracteres única para identificar las unidades de transporte, los artículos individuales, las unidades de transporte restituibles, agrupaciones de productos y unidades de transporte, respectivamente. En cada caso, el identificador único se estructura en diferentes clases para facilitar la gestión eficiente de los identificadores para esa clase de objeto.

La parte 2 especifica los requisitos de procedimiento para atribuir identificadores únicos para aplicaciones de gestión de artículos y describe las obligaciones de la autoridad de registro y de las agencias editoras. Estos procedimientos no aplican a aquellos artículos para los que la ISO ya haya designado autoridades de registro o agencias de mantenimiento para proporcionar esquemas de identificación. Por tanto, no aplica a:

- contenedores de carga, puesto que su única codificación se especifica en la norma ISO 6346 [43];
- vehículos, puesto que su única codificación se especifica en la norma ISO 3779 [44];
- radios de automóvil, puesto que su única codificación se especifica en la norma ISO 10486 [45]; y
- los esquemas ISBN [46] y ISSN [47].

La parte 3 especifica las reglas comunes que aplican a identificadores únicos para la gestión de artículos necesarios para garantizar una compatibilidad completa entre clases de identificadores únicos.

El Comité Técnico 246 de la ISO tiene como cometido elaborar herramientas normalizadas contra la falsificación. Este Comité está desarrollando una norma sobre los criterios de calidad de funcionamiento para soluciones de autenticación con el fin de luchar contra la producción de mercancías falsificadas [48].

Además de la ISO y de EPCglobal, el Ubiquitous ID Centre de Japón ha definido identificadores genéricos denominados "ucódigos" [49], que no sólo pretenden identificar objetos físicos sino que también se pueden utilizar para identificar lugares e información digital, véase la Figura 5. Los ucódigos básicos tiene una longitud de 128 bits (pero se pueden ampliar en múltiplos de 128 bits) y pueden incluir otros identificadores como los ISBN, direcciones de protocolo de Internet (IP) o números de teléfono UIT-T E.164 [76]. El ucódigo es fundamentalmente un número que necesita

que se le asigne un significado en una base de datos racional. Cualquier individuo u organización puede obtener ucódigos del Ubiquitous ID Centre, que ejerce de autoridad de registro para estos números.

Versión (4 bits)	TLDc (16 bits)	cc (4 bits)	SLDc (variable)	ic (variable)
TLDc:	código de dominio de nivel superior (asignado por el Ubiquitous ID Centre)			
cc:	código de clase (indica la frontera entre SLDc e ic)			
SLDc:	código de dominio de segundo nivel			
ic:	código de identificación para objetos individuales			

Figura 5 – Formato de ucódigo

El UIT-T está trabajando en sistemas para acceder a información multimedios en respuesta a la identificación de las cosas basada en etiquetas. Como parte de estos trabajos se está elaborando una descripción de los diversos esquemas ID que se podrían utilizar para esta identificación. El Ubiquitous ID Centre ha presentado su esquema de ucódigos de forma que a cada ucódigo se le asigne un identificador de objeto (OID) registrado según la rama {joint-iso-itu-t(2) tag-based(27)} cumpliendo así la Recomendación UIT-T X.668 [50]. Al esquema de ID único de ISO/CEI descrito anteriormente se le asigna un identificador de objetos según la rama {iso(1)} del árbol de identificadores de objeto. El resultado es que los esquemas de identificación del ISO/CEI (incluido EPCglobal) y del Ubiquitous ID Centre asignan identificadores de objetos ya sea según la rama **{iso}** (ISO y EPCglobal) o según la rama **{joint-iso-itu-t}** (Ubiquitous ID Centre) y permite la coexistencia de los diversos esquemas de identificación que tienen diferentes autoridades de registro. Para la etiquetas RFID, el identificador de objetos (OID) y el ID se codificarían según la norma ISO/CEI 15962 [77].

NOTA – El término "objeto" de "identificador de objetos" no se utiliza aquí para referirse a una "cosa" en general sino que se usa más bien de conformidad con la definición que figura en la norma ISO/CEI 15961 [78] como: "información, definición o especificación bien definidas que requiere un nombre para poder identificar su uso en una instancia de comunicación". Un identificador de objetos identifica sin ambigüedades tales objetos. Los identificadores de objetos están organizados jerárquicamente, indicando las raíces del árbol o "arcos" superiores la organización responsable de la definición de la información. Los arcos superiores representan al UIT-T, la ISO y conjuntamente a ISO-UIT-T. Se les asigna los valores numéricos 0, 1 y 2, respectivamente. Al arco "basado en etiquetas" en el árbol conjunto ISO-UIT-T se le asigna el valor numérico 27.

Los datos asociados con un objeto se pueden almacenar en una etiqueta junto con el identificador si la etiqueta tiene suficiente memoria. No obstante, otro medio posible para encontrar información asociada con un identificador consiste en utilizar un mecanismo de resolución de identificadores.

Cabe prever una amplia gama de servicios y aplicaciones, ya que la información inherente al identificador de la etiqueta se puede proporcionar de diversas formas (texto, audio o imagen). Por ejemplo en un museo, se puede utilizar un identificador en una etiqueta pegada a una pintura para recibir información adicional sobre la obra y el artista. En un almacén de comestibles se puede usar un identificador en un paquete de productos alimentarios para verificar que su ingestión es segura y no pertenece a una clase de alimento que podría estar contaminada. Otras esferas en las que puede resultar útil el acceso a información a través de un identificador son la medicina/los productos farmacéuticos, la agricultura, las bibliotecas, el comercio minorista, la industria turística, la logística y la gestión de la cadena de suministro. Estos mecanismos podrían utilizarse para luchar contra la falsificación. En la Recomendación UIT-T F.771 [55] se describen algunos servicios que podrían basarse en el empleo de la información inherente a los objetos etiquetados, así como los requisitos de esos servicios.

En la Recomendación UIT-T H.621 [52] se especifica un modelo para acceder a la información sobre un objeto etiquetado (véase la Figura 6). Conforme a ese modelo, una función de descubrimiento de información multimedios puede enviar el identificador obtenido de un lector de etiqueta ID a una función de resolución ID, obteniendo de ese modo un puntero (tal como un URL) para el correspondiente gestor de información multimedios. Como resultado de ello se puede acceder a la información asociada al ID de la etiqueta. Como se prevé que el número de identificadores será muy elevado, es probable que la función de resolución ID esté distribuida en una estructura arborescente.

La función de resolución ID puede estar basada en el sistema de nombres de dominio de Internet (DNS) que se utiliza para proporcionar la dirección IP correspondiente a un localizador de recursos uniforme (URL). El servicio de denominación de objetos (ONS) descrito por EPCglobal emplea mecanismos DNS para encontrar la información asociada a los códigos de productos electrónicos.

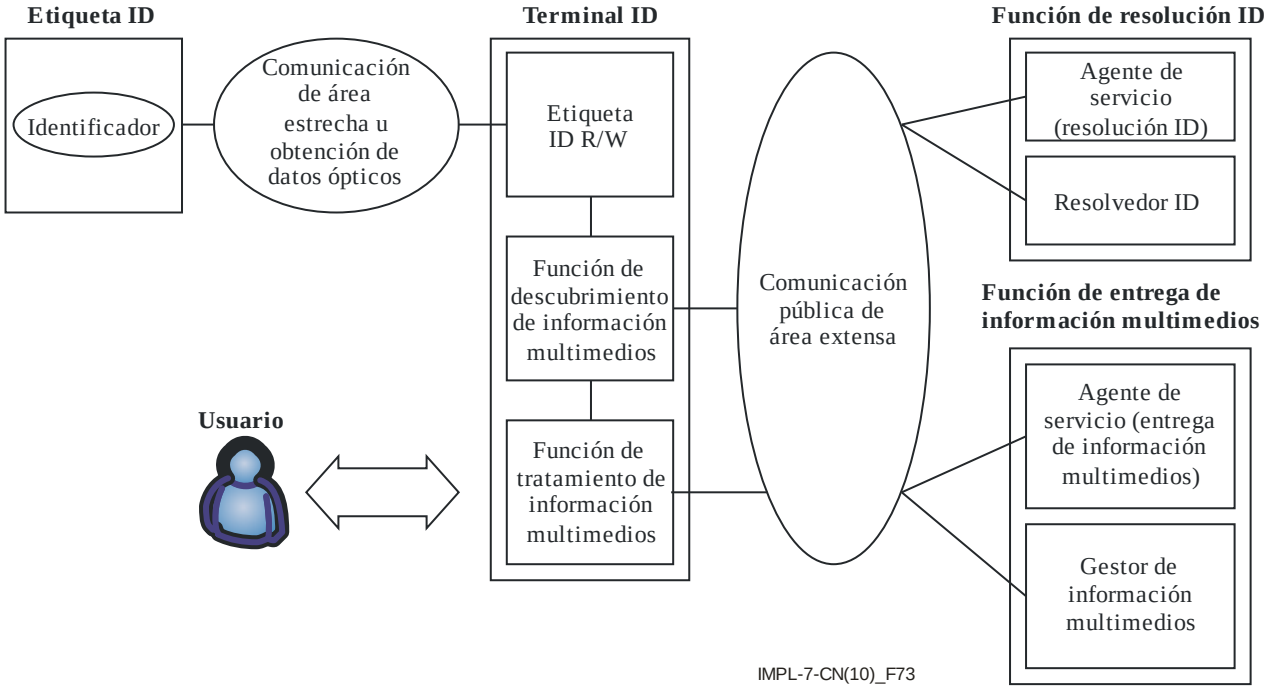

Figura 6 – Arquitectura funcional para el acceso a información multimedios obtenida mediante identificación por etiqueta (Recomendación UIT-T H.621)

Además, la Recomendación UIT-T X.1255 [79] https://www.itu.int/rec/T-REC-X.1255-201309-I/en proporciona un marco para el descubrimiento de la información de gestión de identidades que se ha reconocido en la Resolución de la Conferencia de Plenipotenciarios de la UIT sobre la lucha contra la falsificación de las telecomunicaciones y de la información y de los dispositivos de las tecnologías de comunicación.

7.5 Identificación automática y captura de datos (AIDC)

7.5.1 Códigos de barras

Los códigos de barras se utilizan a menudo para identificar productos. Tienen formas muy variadas desde los códigos de barras de código universal de producto (UPC) que están presentes en los supermercados a los códigos de barras matriciales (2D). Se pueden falsificar con facilidad y los falsificadores pueden copiarlos.

Figura 7 – Ejemplo de código de barras lineal

La Figura 7 muestra un ejemplo de código de barras lineal.

UPC ISO/CEI 15420 [80]

Código de código de barras 39 ISO/CEI 16388 [81]

Código de código de barras 128 ISO/CEI 15417 [82]

Figura 8 – Ejemplo de código de barras matricial (bidimensional)

La Figura 8 muestra un ejemplo de código de barras matricial (bidimensional):

Codablock F ISO/CEI 15417+

PDF 417 ISO/CEI 15438 [83]

Maxicode ISO/CEI 16023 [84]

Código QR ISO/CEI 18004 [85]

Matriz de datos ISO/CEI 16022 [86]

Los códigos de barras se pueden emplear para codificar un número de serie. Por ejemplo, DIN 66401 [87] define una marca de identificación única (UIM) constituida por un símbolo matricial (ISO/CEI 16022 o ISO/CEI 18004) y un identificador de datos único (de conformidad con ANSI MH10.8.2 [88] y el símbolo "+" según ANSI/HIBC 2.3 [89]). Se trata de una aplicación normalizada para marcar artículos pequeños en el ámbito de la electrónica y de la sanidad, por ejemplo. Resultan particularmente adecuados para la marcación directa usando chorro de tinta o laser así como para la impresión de etiquetas.

En la norma ISO 28219 [53] se especifican los requisitos para el etiquetado de artículos y la marcación directa de productos con códigos de barras lineales y matriciales. Los requisitos para el diseño de etiquetas de códigos de barras lineales y 2D para el empaquetado de productos se especifican en la norma ISO 22742 [54] y los de las etiquetas para el envío, transporte y recepción en la norma ISO 15394 [55].

7.5.2 RFID

La RFID permite etiquetar objetos y almacenar información en las etiquetas que se leen utilizando tecnología inalámbrica de corto alcance. Las especificaciones para la RFID incluyen la identificación de objetos, las características de las interfaces aéreas y los protocolos de comunicación de datos.

La norma ISO/CEI 15963 [56] especifica cómo se asignan identificadores únicos a las etiquetas de radio frecuencia (RF). Las etiquetas RF tienen un identificador asignado por el fabricante del circuito integrado – el ID de etiqueta. El ID de etiqueta (TID) se puede usar como un identificador único de artículo (UII) cuando la etiqueta está adherida a algún elemento o cuando el UII puede almacenarse en una parte separada de la memoria en la etiqueta. El UII en este caso podría ser un EPC especificado por EPCglobal.

La Figura 9 muestra el formato de identificación de etiqueta de ISO/CEI 15963.

Clase de atribución (AC)	Número de registro del editor del TID	Número de serie
8 bits	Tamaño definido por el valor de AC	Tamaño definido por el valor de editor de AC y TID

Figura 9 – Formato de identificación de etiqueta de ISO/CEI 15963

La clase de atribución indica la autoridad que asigna los números – el editor de TID. Los fabricantes de tarjetas de circuitos integrados pueden registrarse para asignar identificadores únicos siguiendo el esquema de la norma ISO/CEI 7816-6 [90] o el esquema del American National Standards Institute INCITS (Comité internacional para normas de tecnología de la información), también pueden hacerlo los fabricantes de etiquetas para contenedores y aplicaciones de transporte siguiendo los procedimientos de la norma ISO 14816 [91]. Los identificadores de EPCglobal son conformes al esquema de ISO/CEI 15963 como clase GS1.

La Figura 10 muestra las 10 clases de editores de TID.

Valor AC	Clase	Tamaño del identificador de editor de TID	Tamaño del número de serie	Autoridad de registro (del número de registro del editor de TID)
000xxxxx	INCITS 256	Véase ANSI INCITS 256 [92] & 371.1 [93]	Véase ANSI INCITS 256 y 371.1	autoid.org
11100000	ISO/CEI 7816-6	8 bits	48 bits	APACS (UK Payments Administration)
11100001	ISO 14816	Véase NEN	Véase NEN	NEN (Netherlands Standardization Institute)
11100010	GS1	Véase ISO/CEI 18000-6 Type C [94] & ISO/IEC 18000-3 Modo 3 [95]	Véase ISO/CEI 18000-6 Type C & 18000-3 Modo 3	GS1

11100011	ISO/CEI 7816-6	8 bits	48 bits	APACS (incluye el tamaño de la memoria y el encabezamiento de TID ampliado)
Valores restantes	Reservado			Reservado

Figura 10 – Clases de editores de TID únicos

Una de las primeras aplicaciones de la RFID fue la identificación de animales. La ISO completó una norma que define la estructura de un código de identificación RFID para animales (ISO 11784 [96]). La norma complementaria ISO 11785 [97] describe cómo se lee esta información de etiqueta.

La ISO ha procedido a definir un conjunto completo de especificaciones para la gestión de artículos: las normas ISO/CEI 15961 hasta 15963 describen el protocolo de datos común y los formatos de identificador aplicables a la serie de normas ISO/CEI 18000 [98] que describen las interfaces aéreas en diversas frecuencias. Se precisan especificaciones separadas para las diferentes bandas de frecuencias porque la frecuencia de funcionamiento determina las características de la capacidad de comunicación, es decir, la gama de funcionamiento, o si la transmisión se ve afectada por la presencia de agua.

La norma ISO/CEI 29167-1 [57] define la arquitectura para la gestión de la seguridad y de los archivos para las normas sobre interfaces aéreas ISO/CEI 18000. Se definen los mecanismos de seguridad que dependen de la aplicación y una etiqueta puede soportar todos o parte de ellos. Un interrogador de etiqueta RFID puede acceder a la información sobre los mecanismos de seguridad soportados por una etiqueta y a más información como el algoritmo de encriptación y la longitud de la clave empleada.

La norma ISO/CEI TR 24729-4 [58] incluye las directrices de implementación para que los diseñadores de sistemas evalúen las posibles amenazas a la seguridad de los datos en la comunicación entre la etiqueta y el lector de etiquetas, junto con una descripción de las contramedidas adecuadas para garantizar la seguridad de los datos de etiqueta.

Las aplicaciones de la cadena de suministro de la RFID (con partes que aplican a los contenedores de transporte, artículos de transporte retornables, unidades de transporte, empaquetamiento de productos y etiquetado de productos) se especifican en las normas ISO 17363 a 17367 [99] a [103]; ISO 18185 [104] describe cómo se puede utilizar la RFID para seguir los movimientos de un contenedor de transporte. La ISO también ha elaborado especificaciones de pruebas de calidad de funcionamiento y de conformidad.

El emblema de la RFID especificado en la norma ISO/CEI 29160 [105] puede utilizarse como una etiqueta en los productos para indicar que disponen de una etiqueta RFID. Véase la Figura 11.

Figura 11 – Ejemplo de emblema RFID especificado en ISO/CEI 29160

EPCglobal es la filial de GS1 que elabora especificaciones para el uso de códigos de productos electrónicos. EPCglobal ha generado una serie de normas que incluyen especificaciones para la codificación de datos de etiquetas, protocolos de interfaz, protocolos de lector y servicios de información y de denominación de objetos. La Figura 12 muestra una visión general de la serie de normas de EPCglobal.

Los principales elementos de la serie de normas de EPCglobal son los siguientes:

- La norma sobre datos de etiquetas (TDS) de EPC define algunos esquemas de identificación y describe cómo se codifican estos datos en las etiquetas y también cómo se codifican de forma que sean adecuados para su uso en la red de sistemas EPC.
- En la norma EPC sobre traducción de datos de etiquetas (TDT) figura una versión legible por una máquina de los formatos de datos EPC que se puede utilizar para validar identificadores EPC y traducir entre varias representaciones de los datos.
- Los protocolos de etiqueta son interfaces aéreas de RFID. En la "Gen 2" un lector envía información a una etiqueta modulando una señal de radiofrecuencia en la gama 860-960 MHz. Las etiquetas son pasivas en el sentido de que reciben energía de la señal transmitida por el lector. Este protocolo de interfaz aérea se ha incluido en la serie de especificaciones ISO/CEI 18000 como de Tipo C en la Parte 6. La interfaz aérea de alta frecuencia funciona en 13,65 MHz. Este protocolo es retrocompatible con la norma ISO/CEI 15693 [106].
- Un cliente emplea el protocolo de lectura de bajo nivel (LLRP) para controlar un lector a nivel de funcionamiento del protocolo aéreo y proporciona una interfaz entre el software de la aplicación y los lectores (el protocolo de lectores (RP)).
- Los lectores descubren clientes mediante los procedimientos especificados en la norma sobre descubrimiento, configuración e inicialización (DCI).
- La norma sobre gestión de lectores (RM) se emplea para verificar el estado de funcionamiento de los lectores RFID. Se basa en el uso del sencillo protocolo de gestión de redes (SNMP) definido por el Grupo Especial sobre Ingeniería de Internet (IETF).
- La norma sobre eventos de capa de aplicación (ALE) facilita un medio para que los clientes obtengan datos EPC filtrados. Esta interfaz proporciona independencia entre los componentes de infraestructura que obtienen los datos EPC brutos, los componentes que procesan esos datos y las aplicaciones que hacen uso de esos datos.
- La norma sobre servicios de información EPC (EPCIS) permite compartir datos EPC en y entre empresas.
- El vocabulario principal de negocio (CBV) pretende garantizar que todas las partes que intercambian datos EPCIS tengan un entendimiento común del significado de esos datos.

- La norma sobre el servicio de denominación de objetos (ONS) describe cómo se puede emplear el sistema de nombres de dominio (DNS) para obtener información asociada con un EPC concreto.
- La norma sobre perfiles de certificados de EPCglobal describe cómo se pueden autenticar entidades dentro de la red mundial de EPC. Se utilizan la red de autenticación de la Recomendación UIT-T X.509 [60] y los perfiles de infraestructura de clave pública de Internet definidos en IETF RFC 3280 [61] e IETF RFC 3279 [62].
- La norma sobre historial especifica los medios para manejar documentos electrónicos del "historial" para que se usen en aplicaciones de la cadena de suministro farmacéutica.

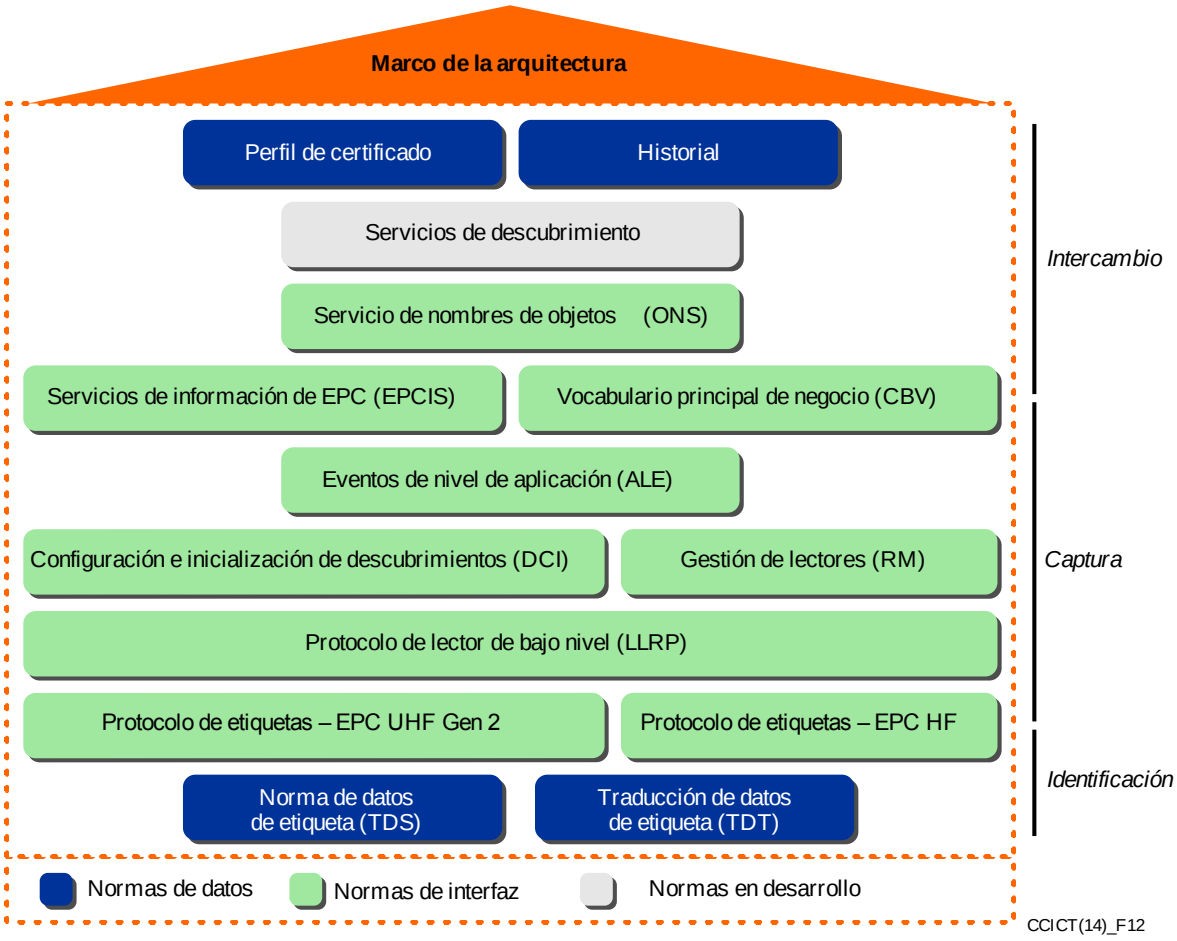

Figura 12 – Visión general de las normas de EPCglobal [59]

7.6 Impresión segura y etiquetas de holograma

Se pueden utilizar tecnologías de impresión segura para crear etiquetas a prueba de manipulaciones y las etiquetas se pueden complementar también con imágenes holográficas que son difíciles de generar. Cabe destacar, sin embargo, que los falsificadores han falsificado y copiado estos mecanismos en muchas ocasiones.

7.7 Gestión de la cadena de suministro

Mantener la seguridad de la cadena de suministro es muy importante para luchar contra las actividades de falsificación. La serie de normas ISO 28000 de la Organización Internacional de Normalización especifica los requisitos para la gestión segura de las cadenas de suministro. Estas normas aplican a organizaciones de cualquier tamaño implicadas en la fabricación, servicio,

almacenamiento y transporte por tierra, mar y aire en cualquier fase de los procesos de producción y de suministro. Están disponibles las normas siguientes:

- ISO 28000:2007, *Specification for security management systems for the supply chain*. [107]
- ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance*. [108]
- ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*. [109]
- ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*. [110]
- ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements*. [111]

Las normas ISO 28000 necesitan organizaciones para evaluar el entorno de seguridad en el que funcionan y para determinar si se han implementado medidas de seguridad adecuadas. En la Figura 13 se muestran los elementos del sistema de gestión de la seguridad.

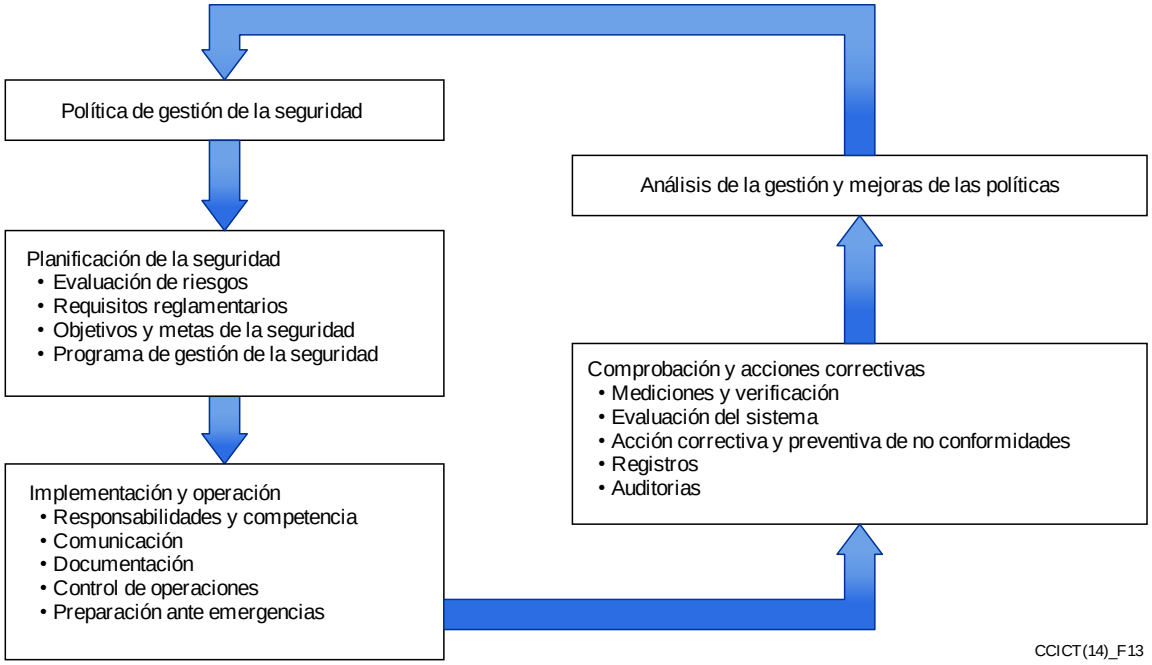

Figura 13 – Elementos del sistema de gestión de la seguridad de ISO 28000

El marco normativo SAFE [63] de la Organización Mundial de Aduanas (OMA) pretende garantizar la seguridad de las cadenas mundiales de suministro e incluye un manual que describe los factores que indican cuando un envío tiene una probabilidad elevada de contener mercancías falsificadas. El marco SAFE se basa en acuerdos entre aduanas y también en asociaciones entre aduanas y empresas de las que se benefician las empresas que cumplen las normas de seguridad de la cadena de suministro.

El Comité Técnico 107 de la CEI, cuyo ámbito de actividad es la gestión de procesos para el sector de la aviónica, ha elaborado una especificación relativa a cómo evitar el uso de componentes electrónicos falsificados, fraudulentos y reciclados [64]. Este Comité está trabajando actualmente en una especificación para la gestión de componentes electrónicos provenientes de fuentes sin franquicia para evitar que los productos falsificados se introduzcan en la cadena de suministro [65].

SAE International (originalmente la Society for Automotive Engineers) ha elaborado algunas especificaciones que pretenden concretamente evitar que se introduzcan componentes electrónicos falsificados en las cadenas de suministro de los sectores aeroespaciales y de automoción que se conocen normalmente como el sector de la electrónica. La SAE ha elaborado dos documentos destinados a aquellos que tienen que tomar decisiones de compra:

SAE AS5553 [112]: "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation"; y

SAE ARP6178 [113]: "Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors"; y una especificación para su uso por los distribuidores: SAE AS6081 [114]: "Counterfeit Electronic Parts; Avoidance Protocol, Distributors". La SAE también ha elaborado una especificación sobre pruebas: SAE AS6171 [115]: "Test Methods Standard; Counterfeit Electronic Parts".

La TC 107 de la CEI trabaja estrechamente con SAE International en relación con SAE AS5553 mediante un acuerdo de coordinación.

En la mayoría de los foros que se ocupan del problema de los productos falsificados anteriormente mencionados se ofrece asesoramiento o directrices sobre la gestión de la cadena de suministro. En general, incluyen los requisitos para la trazabilidad de los productos, su inspección y la realización de pruebas (por tres actores distintos). En 2011, el Grupo de Delitos sobre Propiedad Intelectual del Reino Unido elaboró un Conjunto de Herramientas para la cadena de suministro.

7.8 Realización de pruebas

La Comisión Electrotécnica Internacional (CEI) utiliza los siguientes programas de evaluación de la conformidad http://www.iec.ch/about/activities/conformity.htm:

- IECEE – esquema de la CEI de evaluación de la conformidad de equipos y componentes electrotécnicos;
- IECEx – Sistema de la CEI para la certificación de normas relativas a los equipos que deben usarse en atmósferas explosivas;
- IECQ – Sistema de evaluación de la calidad de la CEI para componentes electrónicos.

Estos programas de evaluación de la conformidad de la CEI se basan en certificados de terceros y utilizan sistemas en línea para facilitar información sobre certificados que pueden utilizarse a fin de identificar productos falsificados.

El IECEE utiliza el programa del organismo de certificación (CB) que se basa en el principio de reconocimiento mutuo por parte de los miembros de los resultados de las pruebas realizadas a fin de obtener la certificación o de aprobación a nivel nacional. El Boletín del CB http://members.iecee.org/iecee/ieceemembers.nsf/cb_bulletin?OpenForm constituye una base de datos para los usuarios del programa CB que contiene información sobre:

- Las normas que pueden utilizarse con este programa;
- Los organismos nacionales de certificación participantes, incluidas las categorías de productos y las normas respecto de las cuales han sido reconocidos; y
- Las diferencias nacionales para cada norma en el caso de cada país miembro.

IECEE CBTC Online es un sistema de registro de certificados de prueba en línea para organismos nacionales de certificación que también es accesible al público.

El IECEE ha establecido un equipo de trabajo para estudiar las medidas para combatir las falsificaciones (CMC-WG23, "Falsificaciones").

El sistema internacional de certificación IECEx consta de los elementos siguientes:

Programa IECEx de equipos certificados;

Programa IECEx de instalaciones de servicio certificadas;

Sistema IECEx de licencias de la marca de conformidad;

Certificación de competencias personales IECEx (CoPC).

La plataforma en línea CoC de IECEx proporciona información sobre los certificados y las licencias expedidas por estos programas.

El IECQ utiliza el Plan de Gestión de Componentes Electrónicos (ECMP) de IECQ para sistemas aviónicos y el programa de Gestión del Tratamiento de Sustancias Peligrosas (HSPM) del IECQ. Los certificados pueden obtenerse en línea.

7.9 Bases de datos

Los destinatarios de las bases de datos de las falsificaciones conocidas son los organismos encargados de velar por el cumplimiento de la ley, como los gestionados por la OMC o la Interpol, así como los consumidores. La Oficina de Información sobre Falsificaciones de la Cámara de Comercio Internacional mantiene una base de datos de estudios de caso.

7.10 Vigilancia del mercado

Se entiende por vigilancia del mercado las "actividades llevadas a cabo y medidas tomadas por las autoridades públicas para velar por que los productos cumplan los requisitos legales establecidos por la legislación pertinente y no entrañen un riesgo para la salud y la seguridad o para otros asuntos relacionados con la protección del interés público" [66].

Las actividades de vigilancia del mercado pueden permitir identificar productos falsificados, y las autoridades encargadas de la vigilancia del mercado pueden intervenir en las iniciativas encaminadas a combatir el comercio de esos productos. La UNECE recomienda que se coordinen las actividades aduaneras y las de vigilancia del mercado nacional, y que los titulares de derechos tengan la posibilidad de informar sobre toda falsificación a las autoridades encargadas de la vigilancia del mercado nacional [67].

Algunos países imponen el registro de los productos como condición para su comercialización. Por ejemplo, la Organización de Normas de Nigeria introdujo recientemente un programa electrónico de registro de productos para intentar limitar la venta de productos falsificados.

8 Organizaciones de normalización

Las principales organizaciones internacionales de normalización que se ocupan de cuestiones pertinentes para la lucha contra las falsificaciones son la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (CEI).

En 2009, la ISO creó un comité técnico encargado de elaborar las especificaciones relativas a las herramientas para la lucha contra la falsificación (ISO TC 246). Dicho comité preparó una especificación sobre los criterios de desempeño de las soluciones de autenticación que se emplean para combatir la falsificación de bienes materiales (ISO 12931) [48]. Esta especificación tiene por fin mejorar la confianza de los consumidores, reforzar la seguridad de las cadenas de suministro y ayudar a las autoridades públicas a formular unas políticas que prevengan, disuadan y castiguen. Aunque el ISO TC 246 ya no está vigente, el ISO TC 247 permitirá seguir trabajando en este ámbito.

El ISO TC 247, "Medidas y mecanismos de control para combatir el fraude", aborda la normalización es la esfera de la detección, la prevención y el control del fraude en la identidad, financiero, en los productos u otras formas de fraude económico y social. Este comité es el autor de la norma de orientación de la ISO sobre la compatibilidad de los identificadores de objeto para luchar contra la falsificación, ISO 16678 [116]: "Orientaciones para una identificación compatible de los objetos y sistemas de autenticación conexos para disuadir la falsificación y el comercio ilícito". Este nuevo proyecto gira alrededor de la utilización masiva de los números de serie para

identificar productos a partir de una base de datos, a fin de determinar su grado de autenticidad. Esta norma internacional tiene como objetivo hacer realidad un mecanismo de identificación de los objetos fiable y seguro que evite la introducción de objetos ilegales en el mercado. Los productos que disponen de un número de serie pueden autentificarse a lo largo de la cadena de fabricación y distribución, e incluso cuando han llegado al consumidor.

La ISO reconoció que las falsificaciones y la piratería afectan a un amplio abanico de bienes de consumo, entre otros ropa, calzado, medicamentos, automóviles y recambios de automóviles, alimentos y bebidas, cosméticos, películas y música, productos eléctricos, dispositivos de seguridad y piezas de aeronaves. Entre las cuestiones que preocupan específicamente al consumidor cabe destacar los riesgos para la seguridad y la salud, los aspectos vinculados al rendimiento del producto, la usabilidad/la idoneidad, la accesibilidad, la protección de datos, la pérdida de puestos de trabajo, los el daño económico y los vínculos con la delincuencia organizada. http://www.iso.org/iso/copolco_priority-programme_annual-report_2012.pdf

El Comité Técnico Mixto ISO/CEI ISO/IEC JTC 1/ SC 31 trabaja en técnicas de identificación automática y adquisición de datos. El Comité se compone de siete grupos de trabajo, sobre las cuestiones siguientes:

- GT1 sobre la portadora de datos;
- GT2 sobre la estructura de los datos;
- GT4 sobre la identificación por radiofrecuencia para la gestión de elementos;
- GT5 sobre sistemas de localización en tiempo real;
- GT6 sobre identificación y gestión de elementos móviles (MIIM);
- GT7 sobre consideraciones de seguridad para la gestión de los elementos.

El Comité Europeo de Normalización (CEN) también trabaja en tecnologías de identificación automática y adquisición de datos en el seno del CT 225.

Muchas organizaciones nacionales de normalización han establecido comités análogos a los comités técnicos de la ISO/CEI. Por ejemplo, el Instituto Alemán de Normalización ha creado el DIN NA 043-01-31, que trabaja en técnicas de identificación automática y adquisición de datos [68] y el DIN NA 043-01-31-04 UA, sobre la identificación por radiofrecuencia para la gestión de elementos.

El CEI TC 107 sobre gestión de procesos para sistemas aviónicos trabaja en la prevención de las falsificaciones.

Además, SAE International está elaborando especificaciones para evitar la utilización de componentes electrónicos falsificados en industrias de tecnología punta, y el GS1 ha elaborado un conjunto de especificaciones sobre identificación de elementos y gestión de la cadena de suministro.

9 Directrices para luchar contra las falsificaciones

Son varias las organizaciones que, desde distintos puntos de vista (el de los fabricantes y los distribuidores, el de los gobiernos y sus organismos encargados de velar por el cumplimiento de la ley y el de los consumidores), han presentado las directrices para luchar contra los productos falsificados.

En el Foro para la Lucha contra la Falsificación pueden encontrarse prácticas óptimas para fabricantes de equipos originales, distribuidores y fabricantes de componentes [69]. Estas directrices incluyen:

- acudir directamente al fabricante o a un distribuidor autorizado o, si no fuera posible, a una fuente local del mercado gris;
- insistir en la obtención de pruebas documentales de la autenticidad del producto cuando se recurra a fuentes del mercado gris;

- reforzar la coordinación entre el producto y la gestión del ciclo de vida de los componentes;
- velar por que se desechan los productos defectuosos o dañados una vez han sido utilizados; y
- mejorar la trazabilidad del producto mediante la utilización de indicadores únicos y de mecanismos de control de la documentación.

El Components Technology Institute Inc. (CTI) ha diseñado un Programa para Evitar Componentes Falsificados (CCAP-101, por sus siglas en inglés) [70] para la certificación de distribuidores independientes de componentes electrónicos, en el que se detallan una serie de requisitos que han de permitir a los distribuidores detecta y evitar el envío a sus clientes de componentes falsificados. Este programa de certificación, que prevé la realización de pruebas eléctricas, tiene por fin cumplir los objetivos que se enumeran en la especificación SAE AS5553.

Asimismo, la Independent Distributors of Electronics Association (IDEA) ha elaborado una especificación para llevar a cabo inspecciones que permitan reducir el número de productos falsificados (IDEA-STD-1010A) [117] así como una especificación sobre gestión de la calidad (IDEA-QMS-9090) [118].

La Hoja de Ruta sobre IP de la CCI incluye recomendaciones relativas a las medidas que pueden adoptar empresas y gobiernos relativas a la protección de la propiedad intelectual en sentido amplio, incluida la lucha contra la falsificación y la piratería. En particular, la CCI insta a los gobiernos a redoblar sus esfuerzos para velar por el cumplimiento de la normativa en materia de propiedad intelectual dado que, "desafortunadamente, los recursos gubernamentales que se destinan a la lucha contra la piratería y la falsificación suelen ser inadecuados a la vista de las dimensiones del problema".

La OCDE ha observado que el mercado de los productos falsificados y pirateados puede dividirse en un "mercado primario", en el que los consumidores creen que los productos son auténticos, y un "mercado secundario" en el que los compradores adquieren conscientemente productos falsificados o pirateados ya que lo que su interés principal es dar con productos a buen precio. Sin embargo, una persona que no tenga el menor reparo en comprar una camisa o un bolso falsificados, puede no estar interesada en adquirir un medicamento o un aparato eléctrico falsificado. La lucha contra las falsificaciones en uno y otro mercado requiere estrategias diferentes, de modo que es necesario saber en qué mercado se sitúa un producto concreto.

Es posible luchar de manera eficaz contra la falsificación de productos en el mercado primario, por ejemplo mediante campañas de información en las que se destaquen los peligros asociados a la compra de productos falsificados; en el caso del mercado secundario, sin embargo, puede ser necesario imponer sanciones más contundentes.

El Conjunto de Herramientas para la cadena de suministro del Grupo de Delitos sobre Propiedad Intelectual del Reino Unido [71] tiene por objetivo concienciar sobre el problema de los productos falsificados que se introducen en las cadenas de suministro legítimas de las empresas, y ofrece una serie de pautas para proteger los activos que incluyen elementos de propiedad intelectual. En la Figura 14 se presenta una panorámica general del proceso a través del cual una empresa puede reducir el riesgo de que un producto falsificado se introduzca en su cadena de suministro.

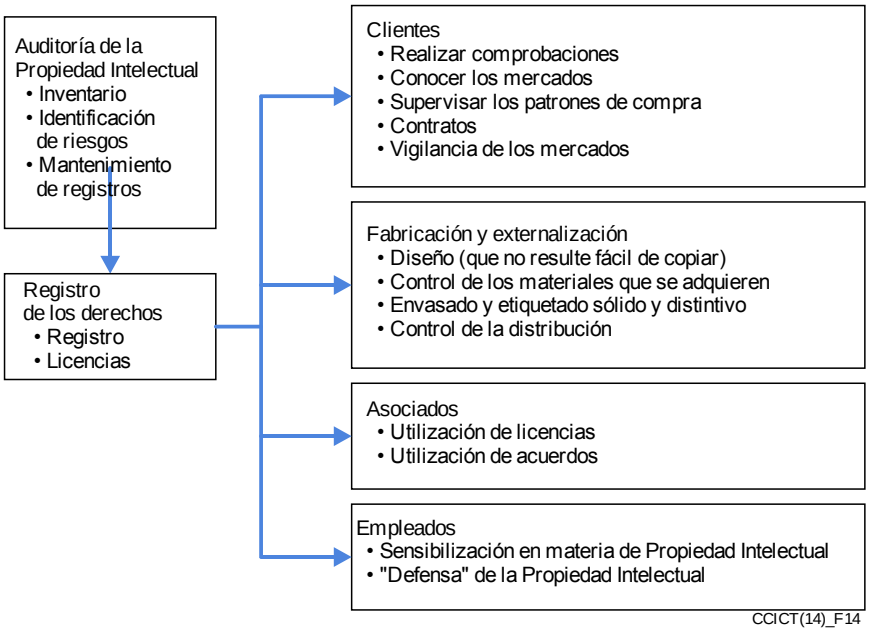

Figura 14 – Protección de los derechos de propiedad intelectual (adaptado a partir de la Herramienta del Grupo de Delitos sobre Propiedad Intelectual del Reino Unido [71])

El MMF ha elaborado una Guía de Recursos para los Gobiernos en la que se proponen distintas medidas, entre otras:

- introducción de cambios en los marcos legal y reglamentario para limitar la activación de dispositivos falsificados en redes de telecomunicaciones;
- restricciones a la importación de dispositivos móviles y accesorios que no cumplan las normas del sector o que no estén en consonancia con el marco legal y reglamentario del país;
- establecimiento de las alianzas y las soluciones necesarias a escala mundial entre la industria y los gobiernos para la validación de productos originales por parte de autoridades, consumidores y el canal de venta;
- desarrollo de unas soluciones tecnológicas armonizadas e innovadores que limiten la posibilidad de activar en las redes de telecomunicaciones dispositivos móviles falsificados; y
- promoción de las normas encaminadas a mejorar las características de seguridad (como los números únicos de identificación individual) que disuaden a las empresas implicadas de fabricar productos falsificados y otros productos ilegales.

Este enfoque va necesariamente más allá de las medidas tradicionales de control de la aplicación y pretende conseguir realmente el bloqueo de estos dispositivos a fin de que no puedan utilizarse en las redes. Pese a todo, las medidas de control de la aplicación, las campañas de sensibilización y la vigilancia de los mercados seguirán siendo elementos importantes, y los fabricantes de teléfonos móviles continuarán trabajando con las autoridades nacionales siempre que sea posible.

10 Conclusiones

La falsificación es un problema creciente que afecta a un amplio abanico de productos. En el sector de las TIC, los teléfonos móviles constituyen uno de los productos principales objeto de falsificación. Cada año se venden unos 250 millones, lo que representa entre un 15% y un 20% del

mercado mundial. Aparte de las evidentes repercusiones económicas para los fabricantes de productos genuinos (devaluación de la marca, pérdida de ingresos, infracción de la marca y de los derechos de autor, competencia desleal), para los distribuidores autorizados y gobiernos (evasión de impuestos, coste adicional para garantizar el cumplimiento de la legislación nacional, la necesidad de reaccionar ante los peligros para la seguridad pública y la pérdida de empleo), también conllevan peligros para la salud, la seguridad y la privacidad del consumidor, para la seguridad pública y tiene efectos negativos para los operadores de red (debido a la menor calidad del servicio (QoS), los posibles problemas de interferencia y de compatibilidad electromagnética (CEM) y la perturbación de la red). La mayoría de estos teléfonos móviles falsificados se producen en un país de Asia y es de este país de donde proceden la mayor parte de los componentes electrónicos falsificados como resultado del reciclaje en el sector informal de residuos electrónicos procedentes de países desarrollados, según ha determinado el Comité del Senado sobre las Fuerzas Armadas en la audiencia sobre componentes electrónicos falsificados en la cadena de suministros de sistemas de defensa [9]. Es evidente que queda mucho por hacer para determinar las fuentes de equipos falsificados y reaccionar antes de su exportación al resto del mundo.

Ya existen instrumentos jurídicos para luchar contra la falsificación, pero su aplicación sigue siendo deficiente. En su informe de 2008, la OCDE llega a la conclusión de que "la magnitud y los efectos de la falsificación y la piratería son tan importantes que obligan a gobiernos, empresas y consumidores a tomar medidas contundentes y continuas. A este respecto es fundamental una aplicación más eficaz, ya que es necesario fomentar el apoyo de los ciudadanos para combatir la falsificación y la piratería. Aumentar la cooperación entre gobiernos y con la industria sería conveniente y facilitaría la recopilación de datos".

Los gobiernos se han implicado más en este asunto y muchos están realizando campañas de sensibilización, ofreciendo asesoramiento y persiguiendo más rigurosamente a los infractores, como en el caso de China recientemente. Los gobiernos no sólo tienen que velar por el cumplimiento de la normativa sobre DPI, sino también aplicar el Convenio de Basilea a fin de garantizar que una vez llegado al final de su vida útil, el equipo usado se manipula de manera inocua para el medio ambiente, en lugar de utilizarse en la economía sumergida de falsificación. Se deben adoptar prácticas éticas de reciclaje a escala mundial.

Los gobiernos quizá también deseen vincular las actividades de vigilancia del mercado con las de las autoridades aduaneras a fin de mejorar las capacidades de detectar productos falsificados. Los equipos de TIC falsificados incautados deben considerarse residuos electrónicos y manipulares con arreglo a los mecanismos de gestión ecológica de residuos.

Las empresas e industrias afectadas por la falsificación han organizado campañas de información y presionado en defensa de sus intereses. No parece ser necesaria una mayor sensibilización acerca de los problemas de la falsificación. En EE.UU., la Ley de autorización de defensa nacional (NDAA) asigna a los contratistas la responsabilidad de detectar componentes falsificados y, en su caso, reemplazar los que detecten en sus productos.

Los consumidores tienen que ser conscientes de los peligros de comprar equipos falsificados, que quizá no sean tan seguros ni funcionen igual que los artículos genuinos. Es evidente que muchísimos organismos nacionales e internacionales, así como los fabricantes, los distribuidores y los medios de comunicación, subrayan regularmente los problemas que presentan los productos falsificados para los consumidores. No obstante, puede darse el caso de que los consumidores decidan voluntariamente comprar bienes falsificados, con independencia de las posibles consecuencias, aparentemente por su precio.

También se puede luchar contra la falsificación mediante la gestión de la vida útil del equipo, no sólo en la cadena de suministro, sino también en las fases de devolución, reutilización y reciclaje de toda la vida útil del equipo. A fin de gestionar la vida útil es necesario disponer de mecanismos para identificar y autentificar los artículos y de procedimientos para rastrearlos con seguridad. El rastreo

debe ser adecuado y suficiente para su finalidad, dado que las tecnologías de identificación automática y adquisición de datos (AIDC), como la RFID, presentan de hecho problemas considerables de privacidad al poder vincular los objetos con sus propietarios. Se debe prestar atención en los procesos normalizados a respetar la privacidad del consumidor y no facilitar la opresión de usuarios de productos TIC a través de los mecanismos de registro del identificador. También debe protegerse al consumidor contra la desconexión arbitraria de las redes.

Se puede recurrir a la tecnología de AIDC y las normas de gestión de la cadena de suministro para luchar contra la falsificación.

La lucha contra la falsificación exige la cooperación de todos los sectores industriales. Las fuerzas del orden, como las autoridades aduaneras, podrían disponer de herramientas genéricas (similares a las de detección de pasaportes y billetes falsos) así como una serie de mecanismos específicos del sector y del producto y medidas concretas con la cooperación de los sectores público y privado.

Existen en el sector de telefonía móvil varios sistemas basados en registro IMEI, que las administraciones y organismos reguladores utilizan o tienen previsto utilizar para identificar terminales móviles genuinos e importados legalmente. También existen varias iniciativas regionales para el intercambio de información sobre dispositivo móviles de origen ilícito. Tales mecanismos también pueden causar problemas a los usuarios legítimos. Por ejemplo, un extranjero que viaje a un país y luego utilice una tarjeta SIM local en su dispositivo puede quedar registrado en una lista blanca y no poder utilizar su dispositivo. Estos mecanismos pueden causar problemas de libre circulación de bienes. En otros sectores de TIC no existen este tipo de mecanismos, dada la naturaleza de los productos y la estructura de las industrias.

Aun cuando algunos países han desarrollado soluciones satisfactorias basadas en IMEI para disuadir la proliferación de teléfonos móviles falsificados, otros, especialmente los países en desarrollo, siguen experimentando grandes dificultades para encontrar una solución eficaz contra los dispositivos falsificados. Hoy en día, las soluciones disponibles en algunos países se basan en bloquear los teléfonos móviles con números IMEI no válidos en sus redes, bloquear la utilización de equipo no homologado por el regulador, o bloquear la importación ilícita de estos dispositivos, o bien tomar otras medidas de sensibilización del consumidor, de aplicación de la ley y de modificación de la legislación a escala nacional.

Las principales organizaciones de normalización internacionales han abordado temas relacionados con la lucha contra la falsificación. No existe hoy por hoy una Recomendación de la UIT disponible que, por ejemplo, compare los diferentes sistemas de lucha contra la falsificación, describa un marco pertinente y examine el rendimiento e interoperatividad a escala mundial. La UIT y otros interesados pertinentes tienen funciones esenciales que cumplir en el fomento de la coordinación entre las partes interesadas para identificar maneras de afrontar esta cuestión a escala internacional y regional. Además, se ha encargado a la UIT que realice las acciones necesarias para prevenir o detectar la alteración y/o duplicación de identificadores exclusivos de dispositivos.

En el presente Informe Técnico se tratan exclusivamente temas relativos a la lucha contra la falsificación, como su definición, sus repercusiones, los convenios de DPI y su observancia, los foros antifalsificación de la industria, las medidas para luchar contra la falsificación y las organizaciones que se encargan de este asunto. A fin de ayudar a los organismos reguladores a proteger al consumidor, a los operadores y a los gobiernos contra los efectos negativos de los dispositivos falsificados, la UIT debería estudiar más detalladamente este asunto.

11 Implicación de la UIT

En la Resolución 177 de la Conferencia de Plenipotenciarios de la UIT de 2010 (PP-10) se "invita además a los Estados Miembros y a los Miembros de Sector a tener presentes los marcos jurídico y reglamentario de otros países relativos a los equipos que afectan negativamente a la calidad de la

infraestructura y a los servicios de telecomunicaciones de esos países, reconociendo, en particular, las inquietudes de los países en desarrollo en relación con la falsificación de equipos" [72].

En la Resolución 79 de la CMDT-14, "Función de las telecomunicaciones/tecnologías de la información y la comunicación en la gestión y lucha contra la falsificación de dispositivos de telecomunicaciones/tecnologías de la información y la comunicación", y en la Resolución COM5/4 de la PP-14, "Lucha contra la falsificación de dispositivos de telecomunicaciones/tecnologías de la información y la comunicación" se encarga a la UIT que estudie el problema de la falsificación de equipos de TIC.

La Comisión de Estudio 11 (CE 11) estudia este problema en el marco de la Cuestión 8 y la UIT celebró un taller sobre la "lucha contra dispositivos falsificados y de baja calidad" en Ginebra el mes de noviembre de 2014. http://www.itu.int/en/ITU-T/C-I/Pages/WSHP_counterfeit.aspx.

Las Comisiones de Estudio 16 y 17 del UIT-T han preparado Recomendaciones relativas a la identificación y autentificación de objetos.

La Comisión de Estudio 5 (CE 5) del UIT-T se encarga de estudiar las metodologías de diseño para reducir el impacto ambiental de la utilización de las TIC mediante mecanismos tales como el reciclaje.

El Director de la TSB ha constituido un Grupo ad hoc (GAH) sobre DPI: http://www.itu.int/en/ITU-T/ipr/Pages/adhoc.aspx para estudiar la política de patentes, directrices sobre marcas y derecho de autor del software, y otras cuestiones afines. Este Grupo se viene reuniendo desde 1998. La UIT y la OMPI también han organizado de consuno simposios sobre temas tales como los nombres de dominio plurilingües en 2001 y sobre "solución de controversias en la encrucijada de las tecnologías de la información y la comunicación y la propiedad intelectual" en 2009: http://www.wipo.int/amc/en/events/workshops/2009/itu/index.html. La UIT también organizó una mesa redonda en 2012 a fin de proporcionar un lugar de encuentro neutro para la industria, los organismos de normalización y los reguladores, donde deliberar acerca de si las actuales políticas de patente y prácticas existentes en la industria responden adecuadamente a las necesidades de los diversos interesados. http://www.itu.int/en/ITU-T/Workshops-and-Seminars/patent/Pages/default.aspx. Hasta la fecha este Grupo no ha abordado el tema de la falsificación.

Es innegable el papel que tiene la UIT en la resolución del problema de la falsificación de equipos de TIC.

En el informe de la CE 1 del Sector de Desarrollo de las Telecomunicaciones de la UIT (UIT-D) titulado regulación y protección del consumidor en el contexto de la convergencia (marzo de 2013), preparado en el marco de la Resolución 64 de la Conferencia Mundial de Desarrollo de las Telecomunicaciones de la UIT (Hyderabad, 2010), se indica que la protección de los innovadores, creadores y consumidores contra la falsificación y piratería derivada de la distribución en línea (y cada vez más transfronteriza) de bienes y servicios, supone un reto para los organismos reguladores.

Según las directrices para países en desarrollo sobre la creación de laboratorios de pruebas y evaluación de la conformidad en diferentes regiones, publicado por el Sector de Desarrollo de las Telecomunicaciones de la UIT en mayo de 2012, los Estados Miembros indicaron que los equipos falsificados están agravando los problemas de conformidad e interoperatividad http://www.UIT.int/UIT-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf. Se ha observado que "la sospecha del dumping comercial de productos que no se ajustan a las normas establecidas y no han superado las pruebas necesarias en otros países es una causa adicional de preocupación, al igual que la importación y distribución de productos falsificados. Un componente fundamental de la respuesta que se ha de dar a estas preocupaciones es la creación de un régimen de homologación sólido y de una serie de laboratorios de prueba que trabaje basándose en un conjunto de normas técnicas, un régimen de realización de

pruebas y una capacidad de ensayo, con el fin de aprobar y controlar las tecnologías de la comunicación que se están implantando en el mercado, con el respaldo de un sistema de control, auditoría y cumplimiento de las normas. Si no se establecen previamente unos requisitos técnicos, un régimen de homologación y unos laboratorios de prueba en el país o región en cuestión, el mercado queda en gran medida desprotegido". Las pruebas y la interoperatividad pueden verse gravemente limitada si se aplican a un mismo producto múltiples normas de diferentes organismos. Es preciso reconocer que aunque parezca atractivo, un régimen de pruebas por sí solo no generará probablemente ningún cambio real de la situación a la hora de resolver el problema de la falsificación.

Cabe señalar asimismo que la falsificación es cada vez más sofisticada y que algunos productos falsificados pueden ser conformes con determinados requisitos técnicos y ser interoperativos con productos genuinos. Así, los productos falsificados pueden ser conformes con una serie de normas técnicas pertinentes y pasar las pruebas de conformidad e interoperatividad. En este caso, sólo el titular de la marca puede diferenciar con exactitud los productos falsificados de los genuinos realizando una evaluación del producto.

El problema de la falsificación de equipos de TIC se examinó en el taller regional de la UIT sobre reducción de la brecha de normalización (BSG) para la Región de África y los Estados Árabes (Argelia, 26-28 de septiembre de 2011) y se preparó una directiva para fomentar la compartición de información a nivel regional por medio de una base de datos de productos falsificados. http://www.itu.int/ITU-T/newslog/ITU+Regional+Workshop+On+Bridging+The+Standardization+Gap+For+Arab+And+Africa+Regions+Interactive+Training+Session+And+Academia+Session.aspx.

El Grupo Asesor de Normalización de las Telecomunicaciones (GANT) del UIT-T subrayó, en su reunión de información sobre evaluación de la conformidad y la interoperatividad (Ginebra, 13 de enero de 2012) y el Foro de la UIT sobre conformidad e interoperatividad para las Regiones de África y los Estados Árabes (Túnez, 5-7 de noviembre de 2012) la conclusión de la Región Árabe de que el equipo falsificado es un problema difícil, especialmente en el mercado de teléfonos móviles, y que es necesaria la cooperación mundial a este respecto. http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/Presentations/Session5/CI%20Forum%202012_Tunis_AAlDin_S5_4.pdf], [http://www.itu.int/dms_pub/itu-t/oth/06/5B/T065B00000E0005PPTE.pptx.

El problema del robo de dispositivos móviles, del mercado gris y de los dispositivos falsificados, así como su incidencia en la industria, los operadores, los gobiernos y los usuarios, se examinó en la reunión de Asociaciones de reguladores organizada por el Sector de Desarrollo de las Telecomunicaciones de la UIT (Sri Lanka, Colombo, 1 de octubre de 2012) de conformidad con la Resolución 48 (Rev. Hyderabad, 2010) "Fortalecimiento de la cooperación entre organismos reguladores de las telecomunicaciones", en la que se pide a la UIT que organice, coordine y facilite la realización de actividades encaminadas a promover el intercambio de información entre organismos reguladores y las asociaciones de reglamentación sobre asuntos clave de reglamentación a nivel internacional y regional. Representantes de 10 asociaciones reguladoras regionales, comprendidas ARCTEL-CPLP, AREGNET, ARTAC, EMERG, FRATEL, REGULATEL, OCCUR, FTRA, SATRC y APT, destacaron las medidas regionales que podría ser sumamente eficaces a este respecto, tales como:

- el intercambio de bases de datos con listas negras de GSM y CDMA mediante la firma de acuerdos bilaterales o multilaterales;
- la conformidad de la industria con las recomendaciones en materia de seguridad relativas a la reprogramación de la duplicación de la IMEI o el número electrónico de identificación de serie del fabricante;

- el establecimiento de mecanismos reguladores fiscales y/o aduaneros que garanticen un mayor control sobre los terminales importados, evitando la salida o la reexportación de terminales móviles robados y/o sus componentes;
- el desarrollo de campañas para sensibilizar a la población sobre la importancia de denunciar el robo y la pérdida de sus terminales móviles.

Muchas asociaciones regionales describieron sus experiencias sobre este particular y reconocieron que es un problema crucial que se ha de resolver en cooperación con la industria y los operadores. La reunión de asociaciones de reguladores adoptó la recomendación de que la UIT, en colaboración con la Asociación GSM, lleve a cabo estudios sobre la cuestión del robo de móviles, el mercado gris y la falsificación de dispositivos y formule orientaciones y recomendaciones. http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/FinalReport_RA12.pdf.

12 Referencias

[1] *The Economic Impact of Counterfeiting and Piracy*, OECD, June 2008.

[2] http://www.oecd.org/sti/ind/44088872.pdf

[3] http://www.icc-ccs.org/icc/cib

[4] *Estimating the global economic and social impacts of counterfeiting and piracy*. http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Global%20Impacts%20-%20Final.pdf

[5] *Intellectual Property Rights Fiscal Year 2100 Seizure Statistics U.S. Customs and Border Protection*. http://www.ice.gov/doclib/iprcenter/pdf/ipr-fy-2011-seizure-report.pdf

[6] http://www.havocscope.com/counterfeit-hp-printing-supplies

[7] http://www.spotafakephone.com/

[8] IDC February 2012 http://www.idc.com/getdoc.jsp?containerId=prUS23297412

[9] http://www.gpo.gov/fdsys/pkg/CRPT-112srpt167/pdf/CRPT-112srpt167.pdf

[10] *Defence Industrial Base Assessment: Counterfeit Electronics*, January 2010 http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-count

[11] http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf HR 1540 SEC. 818

[12] *In WIPO Intellectual Property Handbook* http://www.wipo.int/edocs/pubdocs/en/intproperty/489/wipo_pub_489.pdf

[13] UK IP Toolkit 2009.

[14] http://www.wipo.int/treaties/en/ip/paris/trtdocs_wo020.html

[15] http://www.wipo.int/treaties/en/ip/washington

[16] www.wcoipm.org y http://ipmpromo.wcoomdpublications.org/

[17] vacío

[18] http://www.unece.org/trade/wp6/SectoralInitiatives/MARS/MARS.html

[19] https://www.gov.uk/government/publications/annual-ip-crime-report-2013-to-2014

[20] http://www.aca.go.ke

[21] http://www.iccwbo.org/advocacy-codes-and-rules/bascap/welcome-to-bascap/

[22] http://www.iccwbo.org/bascap/id7608/index.html

[23] http://www.pasdirectory.com

[24] http://www.iccwbo.org/bascap/id42204/index.html

[25] http://www.iccwbo.org/policy/ip/id2950/index.html

[26] https://www.iacc.org

[27] http://www.ascdi.com/

[28] http://www.anticounterfeitingforum.org.uk

[29] http://archive.basel.int/convention/basics.html

[30] http://www.ier.org.tw/smm/6_PAS_141_2011_Reuse_Of_WEEE_And_UEEE.pdf

[31] http://www.bbc.co.uk/panorama/hi/front_page/newsid_9483000/9483148.stm

[32] http://www.bbc.co.uk/news/world-europe-10846395

[33] *Recycling – From E-Waste to Resources*, UNEP, 2009.

[34] Directive 2002/96/EC.

[35] BSI PAS141:2011, *Reuse of used and waste electrical and electronic equipment* (UEEE and WEEE). Process Management Specification (March 2011) http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030245346

[36] http://www.numberingplans.com/?page=analysis&sub=imeinr

[37] IMEI Allocation and Approval Process, Version 7.0, GSMA, 31 October 2013.

[38] http://www.gsma.com/imei-database

[39] http://www.c4dlab.ac.ke/wp-content/uploads/2014/04/VAT-Report_TKO.pdf

[40] Annual Report of the National Commission for the State Regulation of Communications and Informatization for 2012. http://www.nkrzi.gov.ua/images/upload/142/3963/4b2c475b68c147860c36a6e1fc2a3e47.pdf

[41] GS1 EPC Tag Data Standard 1.6, 9 September 2011. http://www.gs1.org/sites/default/files/docs/epc/tds_1_6-RatifiedStd-20110922.pdf

[42] ISO/IEC 15459, *Unique identifiers*.

Part 1:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 1: Individual transport units*.

Part 2:2006, *Information technology – Unique identifiers – Registration procedures*.

Part 3:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 3: Common rules.*

Part 4:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 4: Individual products and product packages*.

Part 5:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 5: Individual returnable transport items (RTIs)*.

Part 6:2014, *Information technology – Automatic identification and data capture techniques – Unique identification – Part 6: Groupings*.

Part 8:2009, *Information technology – Part 8: Grouping of transport units*.

[43] ISO 6346:1995, Freight containers – Coding, identification and marking.

[44] ISO 3779:2009, Road vehicles – Vehicle identification number (VIN) – Content and structure.

[45] ISO 10486:1992, *Passenger cars – Car radio identification number (CRIN)*.

[46] ISO 2108:2005, *Information and documentation – International standard book number (ISBN)*.

[47] ISO 3297:2007, *Information and documentation – International standard serial number (ISSN)*.

[48] ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.

[49] http://www.uidcenter.org/learning-about-ucode

[50] Recomendación UIT-T X.668 (2008) | ISO/IEC 9834-9:2008, *Tecnología de la información – Interconexión de sistemas abiertos – Procedimientos para la operación de autoridades de registro de interconexión de sistemas abiertos: Registro de arcos de identificadores de objetos para aplicaciones y servicios que utilizan la identificación basada en etiquetas.*

[51] Recomendación UIT-T F.771 (2008), *Descripción y requisitos del servicio de acceso a las informaciones multimedios según identificación basada en etiquetas*.

[52] Recomendación UIT-T H.621 (2008), *Arquitectura del sistema de acceso a las informaciones multimedios según identificación basada en etiquetas*.

[53] ISO 28219:2009, *Packaging – Labelling and direct product marking with linear bar code and two-dimensional symbols*.

[54] ISO 22742:2010, *Packaging – Linear bar code and two-dimensional symbols for product packaging*.

[55] ISO 15394:2009, *Packaging – Bar code and two-dimensional symbols for shipping, transport and receiving labels*.

[56] ISO/IEC 15963:2009, *Information technology – Radio frequency identification for item management – Unique identification for RF tags*.

[57] ISO/IEC 29167-1:2014, *Information technology – Automatic identification and data capture techniques – Part 1: Security services for RFID air interfaces*.

[58] ISO/IEC TR 24729-4:2009, *Information technology – Radio frequency identification for item management – Implementation guidelines – Part 4: Tag data security*.

[59] http://www.gs1.org/gsmp/kc/epcglobal

[60] Recomendación UIT-T X.509 (2012) | ISO/IEC 9594-8:2014, *Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[61] IETF RFC 3280 (2002), Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[62] IETF RFC 3279 (2002), Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

[63] http://www.wcoomd.org

[64] IEC/TS 62668-1 ed2.0 (2014), *Process management for avionics – Counterfeiting prevention – Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components*.

[65] IEC/TS 62668-2 ed1.0 (2014), *Process management for avionics – Counterfeit prevention – Part 2: Managing electronic components from non-franchised sources*.

[66] Adapted from Market Surveillance Regulation EC no 765/2008, art 2 (17), http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2009/WP6_2009_13e_final.pdf

[67] Recommendation M. on the: *Use of Market Surveillance Infrastructure as a Complementary Means to Protect Consumers and Users against Counterfeit Goods*. http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf

[68] http://www.nia.din.de/gremien/NA+043-01-31+AA/en/54773446.html

[69] http://www.anticounterfeitingforum.org.uk/best_practice.aspx

[70] http://www.cti-us.com/CCAP.htm]

[71] http://www.ipo.gov.uk/ipctoolkit.pdf

[72] http://www.itu.int/ITU-D/tech/NGN/ConformanceInterop/PP10_Resolution177.pdf

[73] Establishing Conformity and Interoperability Regimes – Basic Guidelines (ITU, 2014).

[74] Guidelines for developing countries on establishing conformity assessment test labs in different regions, ITU, 2012: www.itu.int/ITU-D/tech/ConformanceInteroperability/ConformanceInterop/Guidelines/Test_lab_guidelines_EV8.pdf.

[75] IEC 62321:2008, *Electrotechnical products – Determination of levels of six regulated substances (lead, mercury, cadmium, hexavalent chromium, polybrominated biphenyls, polybrominated diphenyl ethers).*

[76] Recommendation ITU-T E.164 (2010), *The international public telecommunication numbering plan*.

[77] ISO/IEC 15962:2013, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: data encoding rules and logical memory functions*.

[78] ISO/IEC 15961:2004, *Information technology – Radio frequency identification (RFID) for item management – Data protocol: application interface.*

[79] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[80] ISO/IEC 15420:2009, *Information technology – Automatic identification and data capture techniques – EAN/UPC bar code symbology specification*.

[81] ISO/IEC 16388:2007, *Information technology – Automatic identification and data capture techniques – Code 39 bar code symbology specification*.

[82] ISO/IEC 15417:2007, *Information technology – Automatic identification and data capture techniques – Code 128 bar code symbology specification*.

[83] ISO/IEC 15438:2006, *Information technology – Automatic identification and data capture techniques – PDF417 bar code symbology specification*.

[84] ISO/IEC 16023:2000, *Information technology – International symbology specification – MaxiCode*.

[85] ISO/IEC 18004:2006, *Information technology – Automatic identification and data capture techniques – QR Code 2005 bar code symbology specification*.

[86] ISO/IEC 16022:2006, *Information technology – Automatic identification and data capture techniques – Data Matrix bar code symbology specification*.

[87] DIN 66401 (2010), *Unique Identification Mark (UIM).*

[88] ANSI MH10.8.2-2010, *Data Identifier and Application Identifier Standard*.

[89] ANSI/HIBC 2.3-2009, *The Health Industry Bar Code (HIBC) Supplier*.

[90] ISO/IEC 7816-6:2004, *Identification cards – Integrated circuit cards – Part 6: Interindustry data elements for interchange.*

[91] ISO 14816:2005, *Road transport and traffic telematics – Automatic vehicle and equipment identification – Numbering and data structure.*

[92] ANSI INCITS 256-2007, *Radio Frequency Identification (RFID).*

[93] ANSI INCITS 371.1-2003, *Information technology – Real Time Locating Systems (RTLS) Part 1: 2.4 GHz Air Interface Protocol*.

[94] ISO/IEC 18000-6:2013, *Information technology – Radio frequency identification for item management – Part 6: Parameters for air interface communications at 860 MHz to 960 MHz General*.

[95] ISO/IEC 18000-3:2010, *Information technology – Radio frequency identification for item management – Part 3: Parameters for air interface communications at 13,56 MHz*.

[96] ISO 11784:1996, *Radio frequency identification of animals – Code structure.*

[97] ISO 11785:1996, *Radio frequency identification of animals – Technical concept*.

[98] ISO/IEC 18000 (All Parts), *Information technology – Radio frequency identification for item management.*

[99] ISO 17363:2013, *Supply chain applications of RFID – Freight containers*.

[100] ISO 17364:2013, *Supply chain applications of RFID – Returnable transport items (RTIs) and returnable packaging items (RPIs).*

[101] ISO 17365:2013, *Supply chain applications of RFID – Transport units*.

[102] ISO 17366:2013, *Supply chain applications of RFID – Product packaging*.

[103] ISO 17367:2013, *Supply chain applications of RFID – Product packaging*.

[104] ISO 18185 (All Parts), *Freight containers – Electronic seals*.

[105] ISO/IEC 29160:2012, *Information technology – Radio frequency identification for item management – RFID Emblem*.

[106] ISO/IEC 15693, *Identification cards – Contactless integrated circuit cards – Vicinity cards*.

[107] ISO 28000:2007, *Specification for security management systems for the supply chain*.

[108] ISO 28001:2007, *Security management systems for the supply chain – Best practices for implementing supply chain security assessments and plans – Requirements and guidance*.

[109] ISO 28003:2007, *Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems*.

[110] ISO 28004-1:2007, *Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles*.

[111] ISO 28005-2:2011, *Security management systems for the supply chain – Electronic port clearance (EPC) – Part 2: Core data elements*.

[112] SAE AS5553 (2013), *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*.

[113] SAE ARP6178 (2011), *Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors*.

[114] SAE AS6081 (2012), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors*.

[115] SAE AS6171 (2010), *Test Methods Standards; Counterfeit Electronic Parts*.

[116] ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.

[117] IDEA-STD-1010A (2006), *Acceptability of Electronic Components Distributed in the Open Market*.

[118] IDEA-QMS-9090 (2013), *Quality Management System Standard*.

Glosario

AC	Clase de atribución (*allocation class*)
ADI	Identificador aeroespacial y de defensa (*aerospace and defence identifier*)
AIDC	Identificación automática y adquisición de datos (*automatic identification and data capture*)
ALE	Evento de la capa de aplicación (*application layer event*)
AWP	Lugar de trabajo automático (*automated working place*)
CB	Órgano de certificación (*certification body*)
CBV	Vocabulario básico de negocios (*core business vocabulary*)
cc	Código de clase (*class code*)
CD	Disco compacto (*compact disc*)
CDMA	Acceso múltiple por división de código (*code division multiple access*)
CDR	Registro de llamadas detallado (*call detail record*)
CEIR	Registro central de identidad de equipos (*central equipment identity register*)
CIPS	Sistema integral de protección de la información (*comprehensive information protection system*)
CoPC	Certificado de competencias personales (*certification of personnel competencies*)
DB	Base de datos (*DataBase*)
DCI	Detección, configuración e instalación (*discovery, configuration and initialisation*)
DNS	Sistema de nombres de dominio (*domain name system*)
DVD	Disco versátil digital (*digital versatile disc*)
EIR	Registro de identidad de equipos (*equipment identity register*)
EMC	Compatibilidad electromagnética (*electromagnetic compatibility*)
EPC	Código de producto electrónico (*electronic product code*)
EPCIS	Servicio de información EPC (*EPC information service*)
GDTI	Identificador mundial de tipo de documento (*global document type identifier*)
GIAI	Identificador mundial de activos individuales (*global individual asset identifier*)
GID	Identificador general (*general identifier*)
GII	Programa de implante IMEI genuino (*genuine IMEI implant programme*)
GINC	Número de identificación mundial para expedición (*global identification number for consignment*)
GLN	Número mundial de ubicación (*global location number*)
GRAI	Identificador mundial de activos recuperables (*global returnable asset identifier*)
GSIN	Número mundial de identificación de envío (*global shipment identification number*)
GSM	Sistema mundial de comunicaciones móviles (*global system for mobile communications*)
GSRN	Número mundial de relación de servicio (*global service relation number*)
GT	Grupo de Trabajo

GTIN	Número mundial de artículo de comercio (*global trade item number*)
HF	ondas decamétricas (*high frequency*)
ic	código de identificación (*identification code*)
IC	circuito integrado (*integrated circuit*)
ICT	Tecnología de la información y la comunicación (*information and communication technology*)
ID	Identificación (*identification*)
IMEI	Identidad internacional de equipos móviles (*international mobile equipment identity*)
IP	Propiedad intelectual (*intellectual property*)
IP	Protocolo Internet (*Internet protocol*)
IPM	Interfaz público-miembros (*interface public-members*)
IPR	Derechos de propiedad intelectual (*intellectual property rights*)
ISBN	Número internacional de libro normalizado (*international standard book number*)
ISSN	Número internacional de serie normalizado (*international standard serial number*)
IT	Tecnología de la información (*information technology*)
LLRP	Protocolo de lector de nivel bajo (*low level reader protocol*)
LTE	Evolución a largo plazo (*long-term evolution*)
ME	Equipo móvil (*mobile equipment*)
MEID	Identidad del equipo móvil (*mobile equipment identity*)
MIIM	Identificación y gestión de elemento móvil (*mobile item identification and management*)
MRA	Acuerdo de reconocimiento mutuo (*mutual recognition agreement*)
MSC	Centro de conmutación móvil (*mobile switching centre*)
MSISDN	Red digital de servicios integrados al abonado móvil (*mobile subscriber integrated services digital network*)
NIR	Radiación no ionizante (*non-ionizing radiation*)
OID	Identificador de objetos (*object identifier*)
ONS	Servicio de denominación de objetos (*object naming service*)
QoS	Calidad del servicio (*quality of service*)
RF	Radiofrecuencia (*radio frequency*)
RFID	Identificación por radiofrecuencia (*radio frequency identification*)
RM	Gestión del lector (*reader management*)
RoHS	Restricción de sustancias peligrosas (*restriction of hazardous substances*)
RP	Protocolo de lectura (*reader protocol*)
RUIM	Módulo extraíble de identidad de usuario (*removable user identity module*)
SFP	Proveedor de características de seguridad (*security features provider*)
SGLN	Número mundial de ubicación con o sin extensión (*global location number with or without extension*)

SGTIN	Número mundial serializado de artículo de comercio (*serialized global trade item number*)
SIM	Módulo de identidad de abonado (*subscriber identity module*)
SLDc	código de dominio de segundo nivel (*second level domain code*)
SMD	Dispositivo montado en la superficie (*surface-mounted device*)
SMS	Servicio de mensajes cortos (*short message service*)
SNMP	Protocolo sencillo de gestión de red (*simple network management protocol*)
SS7	Sistema de señalización Nº. 7 (*signalling system No. 7*)
SSCC	Código serie de contenedor de envío (*serial shipping container code*)
TAC	Código de atribución del modelo (*type allocation code*)
TC	Comité técnico (*technical committee*)
TDS	Norma de datos de etiquetas (*tag data standard*)
TDT	Traducción de datos de etiquetas (*tag data translation*)
TID	ID de etiqueta (*tag ID*)
TLDc	Código de dominio de nivel superior (*top level domain code*)
TV	Televisión (*TeleVision*)
UHF	ondas decimétricas (*ultra high frequency*)
UII	Identificador único del artículo (*unique item identifier*)
UIM	Marca del identificador único (*unique identification mark*)
UMTS	Sistema universal de telecomunicaciones móviles (*universal mobile telecommunications system*)
UPC	Código universal del producto (*universal product code*)
URL	Localizador uniforme de recursos (*uniform resource locator*)
USB	Bus serie universal (*universal serial bus*)

Anexo A

Sistemas para la identificación de dispositivos móviles falsificados

Como se ha descrito anteriormente en este Informe Técnico, la falsificación de los dispositivos móviles es un asunto de gran preocupación y se han emprendido numerosas iniciativas para limitar la difusión de los dispositivos móviles falsificados. Algunos de los esquemas iniciales buscaban asegurar que se importaran los dispositivos móviles de acuerdo con los procedimientos legales, (que no fueran de contrabando), y se utilizaron posteriormente para dar seguridad sobre la autenticidad de los dispositivos no falsificados. Estos esquemas también comparten muchas características con las iniciativas diseñadas específicamente para afrontar el problema de la falsificación a través de la autentificación de un identificador único (el IMEI).

Las secciones siguientes presentan ejemplos de las medidas tomadas por autoridades nacionales y a escala regional.

A.1 Ejemplos de las medidas tomadas por administraciones y reguladores nacionales

A.1.1 Azerbaiyán

El Sistema de Registro de Dispositivos Móviles (MDRS) http://www.rabita.az/en/c-media/news/details/134 se creó en el Centro de Computación e Información (ICC) del Ministerio de Comunicaciones y Tecnologías de la Información, de acuerdo con las "Reglas de Registro de los Dispositivos Móviles" aprobadas en la Decisión número 212 del Consejo de Ministros de la República de Azerbaiyán, de fecha 28 de diciembre de 2011.

El objetivo del registro de los dispositivos móviles es evitar la importación de dispositivos de baja calidad y de origen desconocido, que no cumplen con las normas técnicas exigidas como la limitación de la emisión de radiaciones electromagnéticas nocivas, e incrementar el reconocimiento y competitividad de las empresas fabricantes. El sistema de registro impide la utilización de los dispositivos móviles perdidos/robados, o importados ilegalmente en el país.

Desde el 1 de marzo de 2013, los operadores móviles introducen diariamente los números IMEI de los dispositivos móviles utilizados en Azerbaiyán en un sistema de base de datos central. El Ministerio de Comunicaciones y Tecnologías de la Información ha informado de que 12 millones de dispositivos GSM se han registrado después de la puesta en servicio del MDRS. Unos 300 000 dispositivos que no cumplen las normas están autorizados a seguir funcionando con sus números actuales de teléfono móvil pero ningún nuevo equipo que no cumpla con las normas podrá funcionar en el país. http://www.mincom.gov.az/media-en/news-2/details/1840

Los números IMEI de todos los dispositivos móviles utilizados en la red antes del 1 de mayo de 2013, se han considerado registrados y pueden operar libremente en las redes. Después de la puesta en servicio del Sistema de Registro, el número de IMEI de cada móvil importado en el país para uso privado (con una tarjeta SIM de uno de los operadores móviles del país) debe ser registrado en el plazo de 30 días después de su conexión a la red. Esta regla no se aplica en el caso de los dispositivos móviles en itinerancia que utilizan una tarjeta SIM suministrada por un operador extranjero.

Los abonados pueden determinar la legalidad de sus dispositivos, con sus números IMEI, mediante una página web especial (imei.az) o con mensajes SMS.

El sistema de base de datos central se creó en el Centro de Computación e Información (ICC) del Ministerio de Comunicaciones y Tecnologías de la Información y, simultáneamente, los operadores móviles instalaron también los equipos que se sincronizan con la base de datos central. Los programas del MDRS fueron realizados por especialistas locales.

A.1.2 Brasil

SIGA – Sistema Integrado de Gestión de Dispositivos

La Reglamentación del servicio móvil de la Agencia Nacional de Telecomunicaciones de Brasil (Anatel) determina que los operadores solo pueden autorizar, en sus redes, los dispositivos certificados por Anatel y que los usuarios deben utilizar exclusivamente estos dispositivos (Artículo 8, IV y Artículo 10, V de la Reglamentación del servicio móvil, aprobada por la Resolución 477/2007[9]). Sobre esta base, Anatel obligó a los operadores móviles brasileños a desarrollar conjuntamente una solución tecnológica para frenar la utilización de los dispositivos móviles no certificados, falsificados o con el número de IMEI clonado.

El plan de actuación, propuesto por los operadores para cumplir con esta obligación, definió, entre otros puntos, las líneas maestras de la solución tecnológica, unos posibles criterios basados en usuarios reales para minimizar el efecto sobre la población, los criterios para los nuevos usuarios una vez lanzada la solución para que únicamente los dispositivos que cumplen con la reglamentación de Anatel puedan acceder a la red, los criterios para los usuarios móviles con el fin de evitar cualquier inconveniente a los clientes y los usuarios extranjeros, y unas campañas de publicidad para los usuarios móviles.

Anatel aprobó el Plan de actuación que considera los aspectos técnicos y reglamentarios, en 2012. La solución se nombró SIGA (Sistema Integrado de Gestión de Dispositivos) y su desarrollo se está realizando sobre la base de las consideraciones técnicas siguientes:

- solución centralizada, realizada conjuntamente por todos los operadores móviles brasileños;
- solución integrada con los operadores de plataformas móviles;
- solución automatizada, que permite la introducción de la información con una intervención humana reducida;
- escalable y con un crecimiento y una complejidad ampliables;
- dinámica y flexible, con reglas que se puedan justar a lo largo del tiempo;
- compuesta de múltiples fuentes de información como, entre otros, los registros de datos de llamada (CDR), los sistemas de gestión de los operadores, incluido la utilización de bases de datos internacionales según convenga;
- eficiente para poder realizar las acciones necesarias para frenar la utilización de los dispositivos ilícitos;
- capaz de minimizar los posibles impactos sobre los usuarios finales normales;
- fiable y segura.

Actualmente, ABR Telecom[10], una asociación técnica creada en forma de empresa mixta de la mayoría de los operadores de telecomunicaciones brasileños, para desarrollar, desplegar y explotar soluciones técnicas centralizadas para el mercado brasileño de las telecomunicaciones, realiza la explotación técnica del SIGA.

En este proyecto existe una fuerte interacción entre todas las partes involucradas para asegurar el éxito de SIGA: Anatel, las autoridades aduaneras, la Asociación de Operadores (SindiTelebrasil), los operadores, los fabricantes de equipos, la Unión de Fabricantes (ABINEE) y ABR Telecom. Además, el problema es complejo pues involucra todas las áreas de un operador, varios actores del mercado y los usuarios finales; es necesario discutir profundamente cada una de las acciones.

---

9 http://legislacao.anatel.gov.br/resolucoes/2007/9-resolucao-477

10 http://www.abrtelecom.com.br

SIGA se encuentra en funcionamiento en las redes de los operadores desde marzo de 2014, recogiendo la información necesaria para diagnosticar la cantidad de dispositivos del mercado que no cumplen la reglamentación brasileña, para que todas las partes involucradas puedan definir las acciones necesarias para garantizar que estos dispositivos falsificados, que no cumplen las normas o no autorizados sean excluidos de la red, con un impacto mínimo para los usuarios.

Una de las posibles acciones para alcanzar este objetivo, actualmente en debate, es la creación de una base de datos de casos previos con todos los casos de funcionamiento (relación única de un terminal y de sus usuarios) que se autorizan a seguir funcionando en la red, pero que bloquea el acceso a la red de cualquier terminal nuevo irregular. En este sentido, los efectos sobre los usuarios se reducen considerablemente y la base de datos de casos previos desaparecería con la sustitución de los terminales.

Es importante, además, incluir en la discusión las entidades que representan al usuario, y elaborar un plan de comunicaciones sólido antes de realizar cualquier actuación con repercusiones directas sobre los usuarios (como pueden ser el bloqueo o la suspensión de un dispositivo).

En este sentido, los operadores, Anatel y la Unión de Fabricantes están elaborado conjuntamente el plan de comunicación de SIGA; todas estas entidades deben implementar el plan, en un esfuerzo conjunto, sobre todos los canales del consumidor (como publicidad, facturas de operadores, centros de llamada) para mostrar a los usuarios las ventajas de comprar terminales legales y certificados y el riesgo que asumen cuando utilizan terminales falsificados, o que no cumplen las normas, en el escenario brasileño.

La información detallada de los aspectos técnicos de este Proyecto se puede conseguir directamente de la Agencia Nacional de Telecomunicaciones (Anatel) de la administración brasileña.[11]

A.1.3 Colombia

En 2011, el Ministerio de Información y de Tecnologías de la Comunicación publicó el Decreto 1630 para establecer mecanismos que permitiesen controlar la publicidad y venta de dispositivos terminales, tanto nuevos como usados, y crear dos tipos de bases de datos centralizadas: una con el registro de los números IMEI de los dispositivos terminales declarados como perdidos o robados y evitar su utilización y activación, y otra base de datos con el registro de los números IMEI de los dispositivos terminales legalmente importados o fabricados en el país, y asociados a un número de identificación del propietario o abonado.

La Ley 1453, del 24 de junio de 2011, sobre la Seguridad de los Ciudadanos prevé penas de 6 a 8 años de prisión para los que falsifiquen, reprogramen, vuelvan a etiquetar o modifiquen el IMEI de los dispositivos móviles y para los que activen dispositivos denunciados como perdidos. Además los equipos modificados deben ser confiscados. http://www.gsma.com/latinamerica/wp-content/uploads/2012/05/Final-CITEL-Resolution-on-Handset-Theft.pdf

Estas iniciativas se han tomado para controlar la venta y la utilización de dispositivos móviles robados pero pueden también tener repercusiones sobre la utilización de productos falsificados.

A.1.4 Egipto

En 2008, la Autoridad Nacional de Reglamentación de las Telecomunicaciones (NTRA) estableció un departamento de seguimiento del mercado para apoyar sus actividades de homologación. Se aprobó un sistema en 2010 para combatir el uso de dispositivos terminales móviles falsificados en Egipto. Este sistema utiliza la base de datos de números IMEI de GSMA (GSMA IMEI DB) para proporcionar una actualización semanal de las listas blancas de los IMEI-TAC, y de la base de datos de IMEI de un Registro Central de la Identidad de los Equipos (EIR). Esta solución está pensada para frenar la utilización de los teléfonos móviles con un número de IMEI ilegal, falso, inválido o

[11] prre@anatel.gov.br

clonado, combatir los robos de los teléfonos móviles, y afrontar los problemas de salud y de seguridad que se plantean.

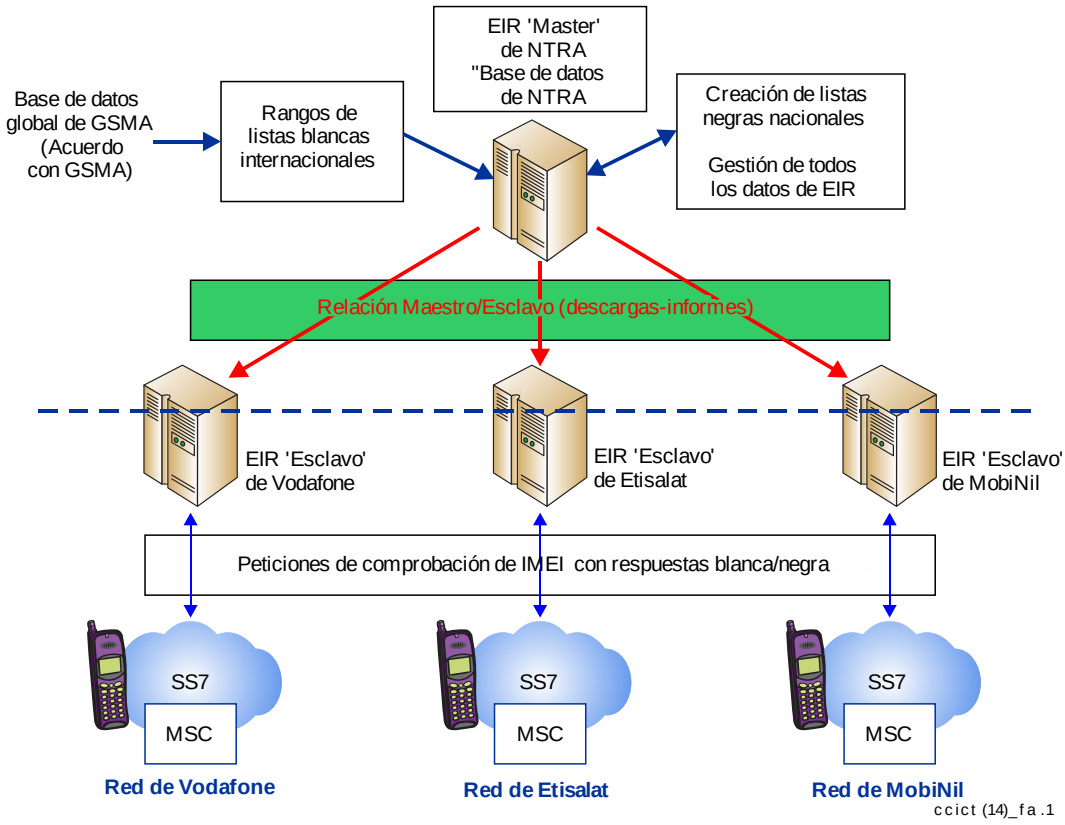

Figura A.1 – Solución de base de datos de IMEI del EIR central en Egipto

De acuerdo con los datos de la NTRA, existían 3,5 millones de teléfonos móviles con el código IMEI ilegal 13579024681122, 250 000 teléfonos con números IMEI clonados, 500 000 teléfonos con falsos IMEI, 350 000 con el número de IMEI con todo 0, y 100 000 sin código IMEI. http://www.itu.int/ITU-D/tech/events/2012/CI_ARB_AFR_Tunis_November12/CI_Forum_Tunis_2012_Report.pdf

En febrero de 2010, la NTRA anunció que los tres operadores móviles del país bloquearían, en el mercado egipcio, los servicios de todos los usuarios anónimos y de los teléfonos celulares sin número IMEI (http://www.cellular-news.com/tags/imei). http://www.cellular-news.com/story/42911.php

A.1.5 Indonesia

Las condiciones para la importación de teléfonos celulares en Indonesia se endurecieron en enero de 2013, con el establecimiento de procedimientos técnicos y requisitos normalizados, restricciones en la distribución y los puertos, controles previos al envío y la obligación de realizar un registro previo de los números IMEI antes de la importación. El Decreto número 81/2012 del Ministerio de Industria y el Decreto número 82/2012 del Ministerio de Comercio especifican estos requisitos. http://trade.ec.europa.eu/doclib/docs/2013/september/tradoc_151703.pdf

A.1.6 Kenya

A.1.6.1 Introducción

De acuerdo con la Agencia contra la Falsificación (ACA) de Kenya, la competencia desleal entre los productos falsificados y los auténticos le supone a las empresas (fabricantes locales, inversores e innovadores) una pérdida anual de ingresos estimada en 50 000 millones de chelines (aproximadamente 596 millones de dólares), y provoca una amenaza de cierre o de traslado para muchas empresas. Las pérdidas para el gobierno y la economía, derivadas de la falsificación, se estiman en más de 19 000 millones (aproximadamente 227 millones de dólares) en evasiones de impuestos.
http://www.aca.go.ke/index.php?option=com_docman&task=doc_download&gid=20&Itemid=471

Los artículos más afectados son los medicamentos, la electrónica, los CD y los programas informáticos pirateados, las bebidas alcohólicas, los teléfonos móviles y los recursos agrarios.

La Ley de Información y Comunicaciones de Kenya, en el capítulo 411A, creó la Comisión de Comunicaciones de Kenya, para conceder licencias y reglamentar los servicios de información y de comunicaciones. La Sección 25 de esta Ley encarga a la Comisión conceder, sujetas a las condiciones necesarias, las licencias para la explotación de los sistemas y la prestación de los servicios de telecomunicaciones. Uno de los requisitos de las licencias es la homologación de los equipos de telecomunicaciones para asegurar su compatibilidad con las redes de comunicaciones públicas. En este contexto, el Reglamento 3 de la Reglamentación de los Servicios de Información y Comunicaciones (importación, homologación, y distribución de equipos de comunicaciones) de Kenya, del año 2010, exige que todos los teléfonos móviles sean homologados por la Comisión antes de su conexión a las redes públicas.
http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf

La esencia del proceso de homologación es fundamentalmente proteger el público contra los efectos indeseables de los dispositivos telefónicos móviles falsificados y/o de baja calidad que representen riesgos técnicos, económicos, para la salud y para la seguridad. En la sección A.1.6.2, figura información adicional sobre los retos asociados con los teléfonos móviles falsificados para la industria de las TIC. Un teléfono móvil que no tiene el número IMEI internacional correcto no puede ser homologado

Por las razones anteriores, la utilización de los dispositivos móviles falsificados debe ser eliminada. Se ha ido realizando, sin embargo, con el respeto a los intereses de todas las partes, y con unas actividades sobre varias fases que han llevado a la fecha de corte del 30 de septiembre de 2012.

Con el objetivo de asegurar que se consideran los intereses y las preocupaciones de todos las partes, la Comisión organizó en octubre de 2011 una serie de consultas abiertas para tratar los retos que provocan los teléfonos móviles falsificados en la industria y en toda la economía, con los actores del sector de las TIC, varias agencias gubernamentales y otros interesados en el tema de los teléfonos móviles falsificados. En estas consultas, se acordaron varios puntos de acción concretos sobre el asunto.

Entre otras acciones, se acordó el lanzamiento, por la Comisión, de una campaña de concienciación pública para asegurar que los usuarios conocen los efectos negativos de los dispositivos falsificados; la creación de un sistema para que el público pueda determinar si el teléfono móvil que tiene es auténtico; la puesta en funcionamiento de sistemas para bloquear los terminales falsificados en las redes públicas; y la prestación de servicios de soporte a los clientes.

Otra acción significativa es el aumento de la vigilancia y de las medidas contra los dispositivos móviles falsificados por todas las agencias relevantes del gobierno. Se ha establecido un sistema de verificación de los teléfonos móviles, con acceso a la base de datos de GSMA para permitir que los

usuarios verifiquen la validez de sus teléfonos introduciendo el IMEI. Además, se ha implementado un sistema para el bloqueo de los terminales falsificados en las redes móviles.

Como resultado de las actuaciones descritas, 1,89 millones de terminales falsificados fueron excluidos, después del 30 de septiembre de 2012, en Kenya.

A.1.6.2 Eliminación de los teléfonos móviles falsificados

1) Antecedentes

a) Implementación del sistema de registro de la identidad de los equipos

En la actualidad, la utilización del móvil en Kenya es una necesidad, y no un lujo. Ello se puede observar en el número creciente de abonados en el país, que alcanza los 29,2 millones aproximadamente. Sin embargo, un reto asociado con la introducción de los servicios de comunicaciones móviles es el robo de los teléfonos móviles, y también el aumento del número de delitos cometidos con la ayuda de teléfonos móviles, que ponen en riesgo la seguridad.

Cuando aparecieron estas amenazas en 2001, la Comisión organizó una serie de consultas con los operadores móviles con licencia existentes, con el objetivo de encontrar una solución duradera para al problema. Mientras tanto, la Organización para las Comunicaciones de África oriental (EACO), adoptó una resolución que, entre otros aspectos, pedía a los organismos reguladores y a los operadores de la región que realizaran consultas sobre la manera más adecuada de controlar el robo de los teléfonos móviles en la región.

En estas consultas, se observó que una funcionalidad de las redes móviles, llamada Registro de identidad del Equipo (EIR), ofrecía un mecanismo para resolver la cuestión del robo de los teléfonos móviles. El EIR puede controlar el número único de Identidad internacional del equipo móvil (IMEI) de cada teléfono que accede a la red móvil y mantener un registro del mismo, y enviar esta información donde las autoridades lo necesitan.

A tal efecto, se estableció un memorándum de entendimiento (MoU) entre todos los operadores móviles para la implementación del sistema EIR y facilitar también la implementación futura del sistema a escala regional. Además se observó que la existencia de teléfonos móviles falsificados con, en muchos casos, IMEI duplicados y/o falsos, lleva a la situación de que cuando se persigue y desactiva un teléfono móvil utilizando el sistema EIR, se pueden presumiblemente desactivar varios teléfonos móviles más con IMEI iguales.

En este contexto, la razón de luchar contra la presencia de teléfonos móviles falsificados en el mercado apareció antes de la implementación completa del sistema EIR y su éxito dependerá de la erradicación de los teléfonos móviles falsificados según se propone internacionalmente.

b) Creación del marco legal/reglamentario para los teléfonos móviles.

i) Marco legal y reglamentario

Desde la perspectiva de la industria de las comunicaciones, la Sección 25 de la Ley de Información y Comunicaciones de Kenya ofrece, en el Capítulo 4IIA, el marco legal y reglamentario para los teléfonos móviles. Las licencias concedidas de acuerdo con esta Ley incluyen una condición que exige a los titulares de las licencias ofrecer los servicios exclusivamente a los usuarios que utilizan aparatos homologados.

Por otro lado, los Reglamentos de Información y Comunicaciones de Kenya de 2010 (importación, homologación y distribución de los equipos de comunicaciones) exigen que se homologuen todos los terminales. Es importante observar que, de acuerdo con los requisitos de homologación de la Comisión, no es posible homologar un teléfono móvil GSM sin un IMEI adecuado o con un IMEI falsificado. En consecuencia, todos los teléfonos móviles sin un IMEI adecuado o con un IMEI clonado son, en

esencia, ilegales y su utilización es, por lo tanto, una violación de la Ley de Información y Comunicaciones.

ii) Reciente Directiva de la Comisión y la respuesta de los operadores

En Mayo 2011, la Comisión indicó a todos los operadores de redes móviles que debían excluir de sus redes, a partir del 30 de septiembre de 2011, todos los terminales falsificados. Esta Directiva estaba de acuerdo con el espíritu y la letra de los estatutos que gobiernan el sector de las comunicaciones.

2) Consultas a la industria

Al recibir la directiva, los actores de la industria móvil contestaron con peticiones de revisión de la directiva, haciendo referencia a un gran número de usuarios que utilizan teléfonos móviles con IMEI idénticos o falsos. Además, los operadores temían que la desconexión de un número estimado de más de dos millones de terminales falsificados, tuviese consecuencias negativas sobre sus ingresos.

La Comisión creó un comité abierto para asegurar la implementación de la directiva con las mínimas interrupciones de servicio, compuesto principalmente por los representantes de los operadores móviles, los ministerios y agencias del gobierno relevantes, los fabricantes de equipos, los vendedores y de la sociedad civil.

El objetivo de las series de consultas entre los representantes de la industria de las TIC y varias agencias del gobierno, ha sido también afrontar los retos que plantean los teléfonos móviles falsificados sobre la industria y la economía en general. La Asociación GSM (GSMA) observó que Kenya es uno de los países con gran mercado de teléfonos móviles robados en Europa o falsificados. Desde su experiencia en la gestión de este tema a escala internacional, la GSMA ha contribuido significativamente y ha aconsejado el proceso en Kenya con varias intervenciones técnicas. Las consultas han contribuido a realizar acciones de soporte a la iniciativa.

Entre estas acciones fueron claves, el lanzamiento por la Comisión de una campaña de información pública para asegurar que los abonados conocieran los efectos negativos de los dispositivos falsificados, y el compromiso de los fabricantes de teléfonos móviles para la creación de un sistema que el público pudiera utilizar para determinar si su teléfono móvil es auténtico o no. Además, los operadores de red establecieron sistemas para bloquear los teléfonos móviles en sus redes y ofrecer servicios de soporte a los abonados, y las agencias del gobierno, sistemas para aumentar la vigilancia y tomar medidas contra los teléfonos móviles falsificados.

La puesta en funcionamiento de un sistema de verificación de los teléfonos móviles con acceso a la base de datos de GSMA para permitir a los abonados verificar la autenticidad de sus teléfonos móviles mediante la introducción del IMEI, se realizó para coincidir con la campaña de información a los consumidores. http://www.cofek.co.ke/CCK%20Letter%20to%20Cofek%20-%20Counterfeit%20phone%20switch-off%20threat.pdf

A.1.7 Rwanda

El Organismo Regulador de Servicios Públicos de Rwanda (RURA) anunció un plan para eliminar la importación de dispositivos móviles falsificados en el país a partir de 2013 sin bloquear los que ya se estaban utilizando:

http://www.newtimes.co.rw/news/views/article_print.php?i=15290&a=64650&icon=Print. Rwanda está afrontando también un reto de teléfonos falsificados que reencaminan las llamadas realizadas a los códigos abreviados armonizados EACO: 100 (servicio de cliente), 101 (recarga en Tanzania) y 102 (consulta de saldo en Tanzania) al número 112 (emergencias, policía). Ha sido necesario que el RURA reasignara temporalmente un nuevo código abreviado al servicio de información del cliente. http://www.eaco.int/docs/19_congress_report.pdf

A.1.8 Sri Lanka

En marzo de 2013, la Comisión de Reglamentación de las Telecomunicaciones de Sri Lanka (TRCSL) solicitó declaraciones de interés para "Diseñar, desarrollar, e instalar un registro central de identidad de equipos (CEIR) para las redes móviles de Sri Lanka".
http://www.trc.gov.lk/images/pdf/eoi_ceir_07032013.pdf

Con el objetivo de limitar el mercado de teléfonos móviles falsificados, desalentar el robo de teléfonos móviles y proteger los intereses de los consumidores, TRCSL quiere implementar un registro central de identidad de equipos (CEIR) conectado con los EIR de todos los operadores móviles. El CEIR actúa como un sistema central para que todos los operadores de red compartan las listas negras de terminales móviles y que los dispositivos incluidos en una lista negra de una red no puedan funcionar en las otras redes, incluso cambiando el Módulo de identificación del abonado (SIM) en el dispositivo.

De acuerdo con los requisitos del TRCSL, el CEIR debe asegurar las siguientes funciones:

i) El CEIR debe tener la capacidad de mantener la base de datos de IMEI de todos los dispositivos registrados en las redes móviles.

ii) El CEIR debe poder identificar los números IMEI tales como:
   a) IMEI no asignados;
   b) IMEI nulos, duplicados o todo ceros.

iii) La base de datos del CEIR debe contener la información siguiente de los dispositivos que se hayan registrado en cualquier red móvil de Sri Lanka:
   a) IMEI;
   b) estado del IMEI (blanco, gris, negro);
   c) fecha de creación del registro;
   d) fecha de la última actualización del registro;
   e) número de modelo del dispositivo;
   f) causa del estado del IMEI (inválido, robado, clonado, valido).

iv) El CEIR debe poder bloquear los servicios a los abonados con dispositivos registrados con números IMEI inválidos o incluidos en la lista negra.

v) El CEIR debe poder identificar el modelo, la versión y otra información del dispositivo.

vi) El CEIR debe permitir la creación de un nuevo registro en la base de datos de IMEI, cuando se activa una nueva cuenta de abonado.

vii) El CEIR debe poder suministrar la información actualizada de la base de datos de las listas locales negras/grises/blancas de los operadores para prevenir el clonado entre las redes y mantener la información actualizada.

viii) El CEIR debe actualizar periódicamente la base de datos de IMEI con la información más reciente de las asignaciones válidas de IMEI, utilizando los métodos más eficaces disponibles.

ix) El CEIR debe tener la capacidad de identificar números IMEI falsificados mediante su comparación con los IMEI suministrados por GSMA.

x) El CEIR debe de ser compatible con todos los equipos de red e interfaces pertinentes de los operadores móviles.

xi) La base de datos del CEIR debe soportar un método flexible de introducción de los datos (por medio de una introducción manual de los datos o ficheros planos con actualizaciones de rangos de IMEI).

xii) El CEIR debe realizar una comprobación del formato del IMEI para verificar si su formato y rango son válidos.

A.1.9 Turquía

En 2006, el Organismo de Tecnologías de la Información y la Comunicación (ICTA) de Turquía estableció un registro central de identidad de equipos (CEIR) para prevenir la utilización de teléfonos no registrados, las pérdidas de impuestos, la competencia desleal en el sector y el pirateo, y automatizar los procesos de importación. La infraestructura se estableció para limitar los dispositivos importados ilegalmente, y desconectar de la red móvil los dispositivos robados, perdidos, de contrabando o con números IMEI clonados.

https://www.icta.mu/mediaoffice/publi.htm

Figura A.2 – Estructura del registro central de identidades de equipos

La Ley de las Comunicaciones por Radiofrecuencia ha categorizado los números IMEI de la siguiente manera:

- Lista blanca: números IMEI de dispositivos registrados y cuya información de identidad electrónica no se ha modificado.
- Lista negra: números IMEI que pertenecen a la categoría de dispositivos perdidos o robados, o cuya información de identidad electrónica se ha modificado. Se ha pedido a los operadores de telecomunicaciones que corten las comunicaciones móviles de estos dispositivos.
- Lista gris: números IMEI que no pertenecen ni a la lista blanca ni a la lista negra pero cuyas comunicaciones están autorizadas. Los operadores deben analizar los detalles de las llamadas de estos dispositivos y deben informar al ICTA. Los operadores de telecomunicaciones deben notificar también a los abonados, con un mensaje de texto, que sus dispositivos no están incluidos en la lista blanca.
- Lista blanca de números emparejados: números IMEI clones del número RDSI de abonado móvil (MSISDN) de los dispositivos de abonados que han depositado una tasa de inscripción. También se incluyen los dispositivos que formalizan un contrato de abono con un operador de telecomunicaciones y están en Turquía, con el número MSISDN, durante un periodo de tiempo.

Según el Informe anual de 2010 del ICTA, el número de IMEI legalmente registrados, a final de 2010, ascendía a 131 836 847, y a 14 308 239 el número de IMEI incluidos en la lista negra por ser dispositivos robados, perdidos, clonados o de contrabando.
https://www.icta.mu/mediaoffice/publi.htm

A.1.10 Uganda

La Comisión de Comunicaciones de Uganda (UCC) ha empezado la implementación de un proyecto http://ucc.co.ug/data/mreports/18/0/ELIMINATION%20OF%20COUNTERFEIT%20MOBILE%20PHONES.html que busca la eliminación gradual de los teléfonos móviles falsificados del mercado de Uganda. Un estudio certificado por la UCC indica que el 30% aproximadamente de los teléfonos móviles del mercado de Uganda son falsificados. El estudio también indica que el estado pierde aproximadamente 15 000 millones de schilling (aproximadamente 5 400 millones USD a fecha de noviembre de 2014) de los ingresos de las tasas de los vendedores de teléfonos móviles ilegales o falsificados.
http://www.monitor.co.ug/Business/Commodities/Survey+finds+30++of+Ugandan+phones+fake/-/688610/1527408/-/elvou8z/-/index.html

En diciembre de 2012, la UCC publicó el documento consultivo "Calendario y distribución de tareas para la eliminación de los teléfonos móviles falsificados"
http://www.ucc.co.ug/files/downloads/Counterfeit%20phones%20Consultative%20Document.pdf
que define el proyecto y sus cuatro fases de implementación de la manera siguiente:

FASE 1: Verificación de los teléfonos móviles

Durante esta fase, los consumidores podrán comprobar el estatus de sus teléfonos utilizando una o ambas aplicaciones, por Internet o SMS.

Se aconseja a los consumidores comprobar inmediatamente la legitimidad de sus teléfonos utilizando una de estas opciones.

FASE 2: Denegación del servicio a los teléfonos nuevos falsificados

Durante esta fase, se debe denegar el servicio en todas las redes a los teléfonos móviles nuevos falsificados que no se hayan registrado anteriormente en alguna de las redes. La fecha propuesta para la implementación de esta fase era el 31 de enero de 2013.

FASE 3: Desconexión de todos los teléfonos móviles falsificados

Durante esta fase, se deben desconectar todos los teléfonos móviles, incluidos los que se hayan registrado anteriormente en alguna de las redes. La fecha propuesta para la implementación de esta fase era el 1 de julio de 2013.

FASE 4: Consolidación del Proyecto:

Durante esta fase, la Comisión debe estudiar la información del proyecto y su implementación, y los temas relativos a la gestión de los residuos electrónicos y la clonación de IMEI. Las propuestas de estudio de varios temas durante esta fase se están analizando todavía.

A.1.11 Ucrania

A.1.11.1 Introducción

En 2008, el problema inmediato y más acuciante que se debía afrontar era la introducción de terminales móviles de contrabando que representaba un 93-95% del mercado. Una parte considerable de estos terminales de origen desconocido no cumplían con las normas ucranianas, por sus características técnicas o por su seguridad. La Ley "sobre los recursos de radiofrecuencia de Ucrania" encargó a la Comisión nacional para la reglamentación estatal de las comunicaciones e informatización (NCCIR) imponer nuevas medidas para proteger el mercado de Ucrania contra los terminales móviles de baja calidad, no autorizados, o importados ilegalmente.

La NCCIR definió un procedimiento reglamentario para la importación de los terminales móviles. En la parte técnica del procedimiento de importación, se creó el Sistema de información automatizado para el registro de los terminales móviles en Ucrania (AISMTRU) puesto en funcionamiento por el Centro estatal de Ucrania de radiofrecuencia (UCRF) en 2009. En consecuencia, las importaciones ilegales de terminales móviles se redujeron de forma espectacular, no representando más de un 5-7% del mercado en 2010, y siguieron disminuyendo en los años siguientes.

Los números IMEI se utilizan en Ucrania para crear una base de datos de los dispositivos importados legalmente en Ucrania. Se mantienen las siguientes listas: una "lista blanca" de los dispositivos importados legalmente, una "lista gris" de los dispositivos con un estado no confirmado y una "lista negra" de los dispositivos a los que se deniega el servicio. Se proporcionan accesos, con los niveles de privilegios adecuados, a las autoridades regulatorias y aduaneras, a los operadores y al público en general

El AISMTRU realiza las siguientes funciones:

- automatización del procesamiento de las solicitudes de los importadores para completar los procedimientos reglamentarios definidos para el registro y la utilización de los equipos terminales en las redes de telecomunicaciones;
- prevención de la importación ilegal "gris" de terminales móviles en el territorio de Ucrania;
- lucha contra el robo de teléfonos móviles;
- automatización del proceso del UCRF e incremento de la eficacia de las relaciones entre el UCRF y los actores del mercado de terminales;
- identificación de los números IMEI clonados y bloqueo de los terminales con números IMEI clonados.

La sección A.1.11.2 contiene información detallada sobre el AISMTRU:

La legislación de Ucrania prohíbe la venta de terminales móviles con números IMEI no registrados en el AISMTRU. El componente central del AISMTRU es la base de datos general, que mantiene las listas "blancas", "grises" y "negras" de los números IMEI de los terminales móviles. Cuando se realiza la conexión y se registra un terminal por primera vez en la red de uno de los operadores móviles, éste reenvía automáticamente el número IMEI del terminal a la base de datos central. AISMTRU comprueba los números que no están presentes en la lista "blanca", identifica los teléfonos móviles falsificados e incorpora el correspondiente número IMEI a la lista "gris". Todos los propietarios de los respectivos terminales reciben un aviso por SMS y deben confirmar el origen legal de su terminal en los 90 días siguientes a su entrada en la lista "gris".

Los números IMEI de los terminales robados se incorporan a la lista "negra" bajo petición legal de un organismo y hacen inútil el robo de terminales. El mismo procedimiento se sigue en el caso del bloqueo del terminal a petición de los propietarios de teléfonos perdidos. Los operadores de las redes no prestan servicio a los terminales de la lista "negra".

El objetivo de proteger al consumidor se consigue con la implementación de la herramienta para la verificación de la legalidad de un terminal móvil antes de su compra. Cualquier cliente puede verificar el estado del número IMEI del terminal, enviando un SMS con el IMEI al número 307 de cobertura nacional o utilizando el portal de Internet del UCRF. El tiempo requerido para la comprobación no supera los diez segundos.

La puesta en funcionamiento del AISMTRU asegura un mercado legal de terminales y ha reducido de manera espectacular la importación "gris" (ilegal) de terminales móviles en Ucrania. La cuota de los terminales móviles importados ilegalmente se ha reducido desde un 93-95% en 2008 a un 5-7% en 2010 y los años siguientes. En Ucrania, un ingreso de más de 500 millones USD se ha transferido al presupuesto del estado en el periodo 2010-2012, de las tasas de importación de los

terminales móviles, comparados con 30 millones USD aproximadamente durante los tres años anteriores. El mercado ucraniano de terminales móviles está compuesto en su mayoría por terminales móviles que cumplen con las características técnicas requeridas para su utilización en Ucrania.

A.1.11.2 Sistema de información automatizado para el registro de los terminales móviles en Ucrania (AISMTRU)

A.1.11.2.1 Antecedentes

El rápido desarrollo de los servicios de comunicaciones móviles (celulares) prestados por los operadores y la prevalencia significativa de este tipo de servicios de telecomunicaciones en Ucrania, han llevado al rápido crecimiento del mercado de los terminales móviles y, en consecuencia, a un incremento de las importaciones de estos productos.

Un "terminal móvil" significa un teléfono móvil o cualquier otro equipo de usuario final de una red de telecomunicaciones, que tenga un número internacional de identidad IMEI y pueda ser identificado en una red con la utilización de ese número.

En 2008, existía una situación crítica en el mercado de los terminales móviles de Ucrania: un 93-95% de los productos del mercado eran importaciones "grises" o, más sencillamente, contrabando. Además, una mayoría de estos productos eran copias de teléfonos móviles de marca, de origen desconocido y cuyas características técnicas y de seguridad no cumplían las normas ucranianas. Varias medidas regulatorias del mercado no consiguieron cambiar esta situación y no se fabricaban terminales en Ucrania.

Fue entonces cuando la Ley "sobre los recursos de radiofrecuencia de Ucrania" encargó al organismo regulador independiente, la Comisión Nacional para la reglamentación estatal de las comunicaciones e informatización (NCCIR), imponer nuevas medidas para proteger el mercado ucraniano contra los terminales móviles de baja calidad, no autorizados o importados ilegalmente.

A.1.11.2.2 Objetivos

Para controlar la importación, venta y utilización de los terminales, la NCCIR definió los siguientes objetivos:

1) Proteger el mercado ucraniano contra los terminales móviles de baja calidad, que pueden ser no autorizados o peligrosos para la salud.
2) Asegurar la calidad adecuada de los servicios móviles de comunicaciones.
3) Resolver el problema del robo de teléfonos móviles, especialmente entre los niños.
4) Combatir la importación ilegal y la utilización de terminales móviles en el mercado ucraniano.

Se definieron los procedimientos para la importación y utilización de equipos móviles considerando los objetivos anteriores. Estos procedimientos se han incorporado a los siguientes documentos oficiales: el procedimiento para la importación de equipos electrónicos de radiofrecuencia y dispositivos radiantes y el procedimiento para la utilización de los equipos electrónicos y dispositivos radiantes en Ucrania.

A.1.11.2.3 Procedimientos de importación

Las autoridades aduaneras controlan la importación de los equipos de radiofrecuencia con los siguientes requisitos:

- disponibilidad de un documento sobre la conformidad de los equipos de radiocomunicaciones con los reglamentos técnicos;

- conformidad con el Registro de equipos electrónicos de radiofrecuencia y dispositivos radiantes, autorizados para su utilización en Ucrania en las bandas de frecuencias de uso común;
- ausencia del Registro de equipos electrónicos de radiofrecuencia y dispositivos radiantes, cuya utilización se ha prohibido en Ucrania en las bandas de uso común.

Los números IMEI, comunicados por el importador a el UCRF, se procesan e introducen en la "lista blanca" de la base de datos general de números IMEI. Para el registro de los identificadores internacionales de los equipos terminales importados legalmente en Ucrania, el Servicio estatal de aduanas de Ucrania suministra a el UCRF, diariamente, el extracto de las declaraciones de aduanas (en formato electrónico) de las importaciones de material electrónico de radiofrecuencia.

El Sistema de información automatizado para el registro de los terminales móviles en Ucrania (AISMTRU) fue creado y puesto en funcionamiento por el Centro estatal de frecuencias de radiofrecuencia (UCRF) el 1 de julio de 2009, como implementación técnica del procedimiento reglamentario de importación.

De acuerdo con la Ley de "Confirmación de la conformidad" de Ucrania, los organismos acordados por el Regulador (NCCIR) deben certificar la conformidad de los equipos terminales.

A.1.11.2.4 Funciones del AISMTRU

Las funciones del AISMTRU se han definido en el párrafo A.1.11.1:

- automatización del procesamiento de las solicitudes de los importadores;
- prevención de la importación ilegal "gris" de terminales móviles en el territorio de Ucrania;
- lucha contra el robo de teléfonos móviles;
- automatización del proceso del UCRF e incremento de la eficacia de las relaciones entre el UCRF y los actores del mercado de terminales;
- identificación de los números IMEI clonados y bloqueo de los terminales con números IMEI clonados.

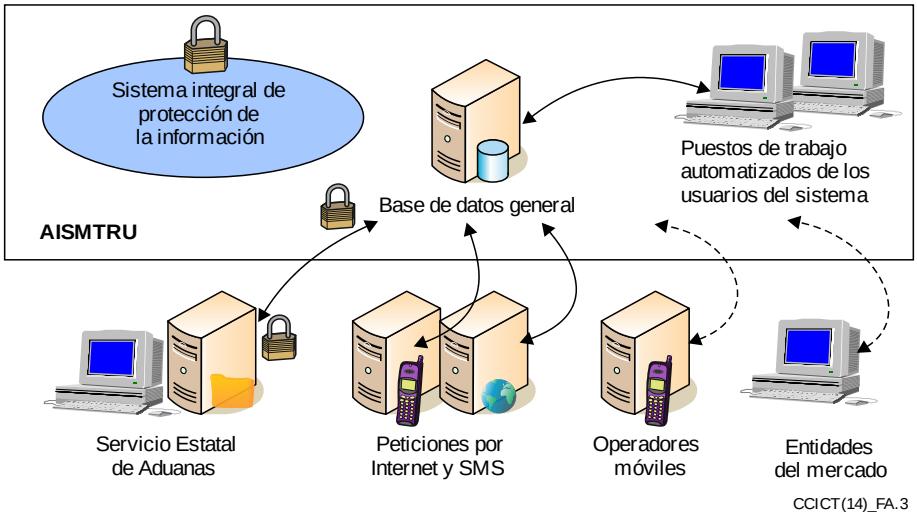

Figura A.3 – Funciones del AISMTRU

A.1.11.2.5 Autorización

De acuerdo con la legislación vigente, las siguientes entidades están autorizadas para utilizar el sistema AISMTRU:

- el Centro estatal de Ucrania de radiofrecuencias (UCFR);

- la Comisión Nacional para la reglamentación estatal de las comunicaciones e informatización (NCCIR);
- los operadores móviles;
- el Servicio estatal de aduanas;
- el Ministerio del Interior;
- los compradores y usuarios de los terminales móviles; y
- los importadores.

A.1.11.2.6 Base de datos general de IMEI

El componente principal del AISMTRU es la base de datos general de números IMEI, que mantiene tres listas conocidas como:

- "Lista blanca": registro de los números IMEI de los terminales importados legalmente en Ucrania.
- "Lista gris": un registro de la base de datos general que contiene los números IMEI de los terminales no incorporados a la "lista blanca" o la "lista negra" en el momento de su primer registro en la red de telecomunicaciones.
- "Lista negra": un registro de los números IMEI de los terminales cuya utilización está prohibida en las redes de los operadores (terminales perdidos o robados, terminales cuyo origen legal no se ha confirmado después de 90 días desde su incorporación a la "lista gris").

El subsistema de mantenimiento de la base de datos general de IMEI ofrece a los usuarios autorizados por el UCRF una herramienta para la introducción de datos en la "lista blanca". Las listas "gris" y "negra" se generan automáticamente. Los usuarios autorizados del UCRF tienen un derecho limitado para cambiar el estado de los números IMEI en las listas "blanca" y "negra".

Cada acción de un usuario autorizado por el UCRF debe ser confirmada con la firma digital electrónica de un usuario individual.

El subsistema dispone de una función de importación de datos para incorporar los datos de los importadores de terminales y de los operadores móviles al registro de números IMEI.

Mediante el procesamiento de los datos de la "lista blanca" y de los datos de los operadores, los importadores y del servicio de aduanas, es posible crear y mantener los registros de las listas "grises" y "negras".

La primera fase de la puesta en funcionamiento del sistema resolvió dos objetivos:

1) La protección del mercado de Ucrania contra el uso de los terminales móviles no autorizados de baja calidad y que pueden ser peligrosos para la salud de los usuarios.
2) La prevención de la importación de terminales móviles y su utilización en el mercado de Ucrania.

Posteriormente, se desarrolló un sistema para alcanzar todos los objetivos, incluido el de desmotivar el robo de terminales, especialmente de los niños.

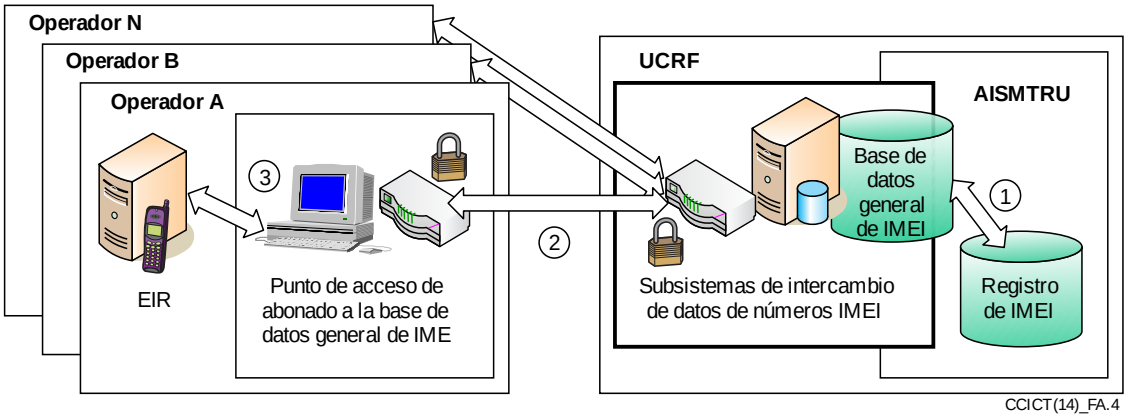

Figura A.4 – EIR y base de datos general de IMEI

En una segunda etapa, se implementó un subsistema para intercambiar los números IMEI de las listas "blanca", "gris" y "negra" entre el AISMTRU y los operadores móviles nacionales. Hasta ese momento, el intercambio de números IMEI se realizaba en modo manual.

Por otro lado, se implementaron los subsistemas de intercambio de datos para informar al Ministerio del Interior de los terminales perdidos/robados y con el servicio de aduanas para la comunicación de la información sobre los terminales importados.

Para asegurar una relación activa con el AISMTRU, los operadores y el UCRF han proporcionado:

- el mantenimiento del registro de identidades de equipos (EIR);
- puntos de acceso de abonado a la base de datos general de IMEI (punto de abonado);
- un canal para la actuación entre el punto de abonado y el EIR;
- una aplicación de certificados de firma digital para los usuarios autorizados.

El sistema del AISMTRU, sincroniza el trabajo de los EIR de los operadores celulares (móviles) y la base de datos general de IMEI, y posibilita el intercambio automático de las listas de números IMEI entre los EIR de las redes de los operadores móviles y la base de datos general de IMEI. De esta manera, el número IMEI de cada terminal, después de su registro en la red del operador, aparece en AISMTRU y se comprueba en la base de datos general.

Actualmente, el servidor de sincronización soporta tanto el modo manual como automático, para la conexión con los EIR de los operadores.

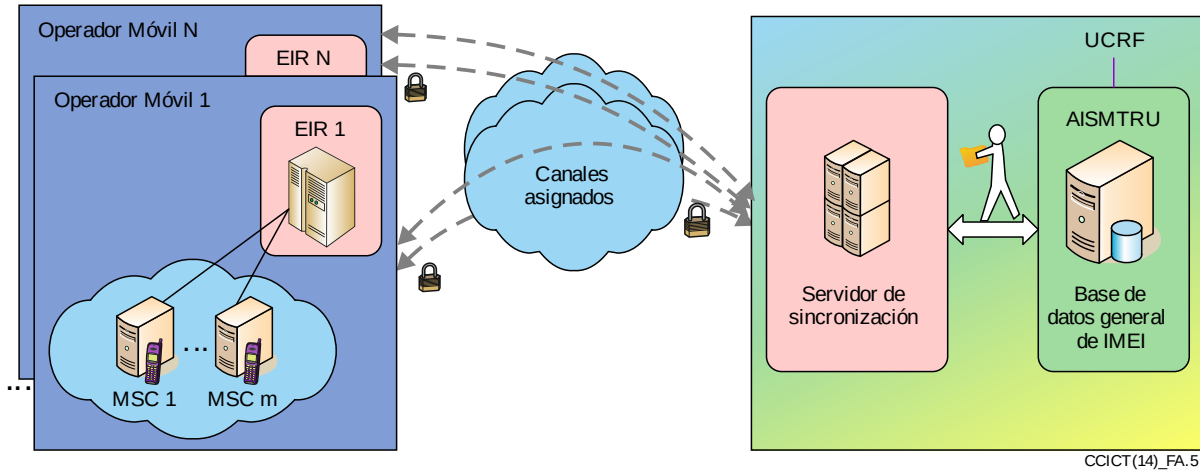

Figura A.5 – Servidor de sincronización

A.1.11.2.7 Funcionalidades

Las funcionalidades del sistema incluyen:

- utilización de las normas de la industria para el almacenamiento y la transferencia de datos (intercambio de datos);
- seguridad garantizada de los datos y del sistema completo;
- utilización de la norma nacional de firma digital para asegurar la integridad y el no repudio en todas las etapas del procesado de datos en el sistema;
- estructura modular del sistema;
- operación 24 horas al día los 7 días de la semana (24x7).

A.1.11.2.8 Seguridad de los datos

El Sistema integral de protección de la información (CIPS) del AISMTRU cumple los requisitos de la legislación vigente y ha sido aprobado con las conclusiones positivas del examen realizado por la autoridad gubernamental competente.

El CIPS asegura:

- el control del acceso restringido a la información confidencial;
- la identificación de los riesgos para la seguridad de la información de acceso restringido transferida, procesada y almacenada en el sistema;
- la protección de la confidencialidad, la integridad y la disponibilidad de la información de acceso restringido frente a accesos no autorizados;
- la prevención de las fugas de información en el paso por un entorno no seguro;
- la protección de la información tecnológica contra los accesos no autorizados, la destrucción, la alteración o el bloqueo.

La seguridad y la fiabilidad se aseguran con:

- la utilización de medios fiables de firma digital electrónica para asegurar la autenticidad e integridad de la información, la autorización y la autentificación de los usuarios autorizados;
- la implementación de la firma digital electrónica de acuerdo con las normas nacionales de Ucrania;
- la disponibilidad de un sistema de duplicación y de recuperación;
- el mantenimiento de un registro de seguridad (registro de todas las acciones de usuario y los eventos del sistema).

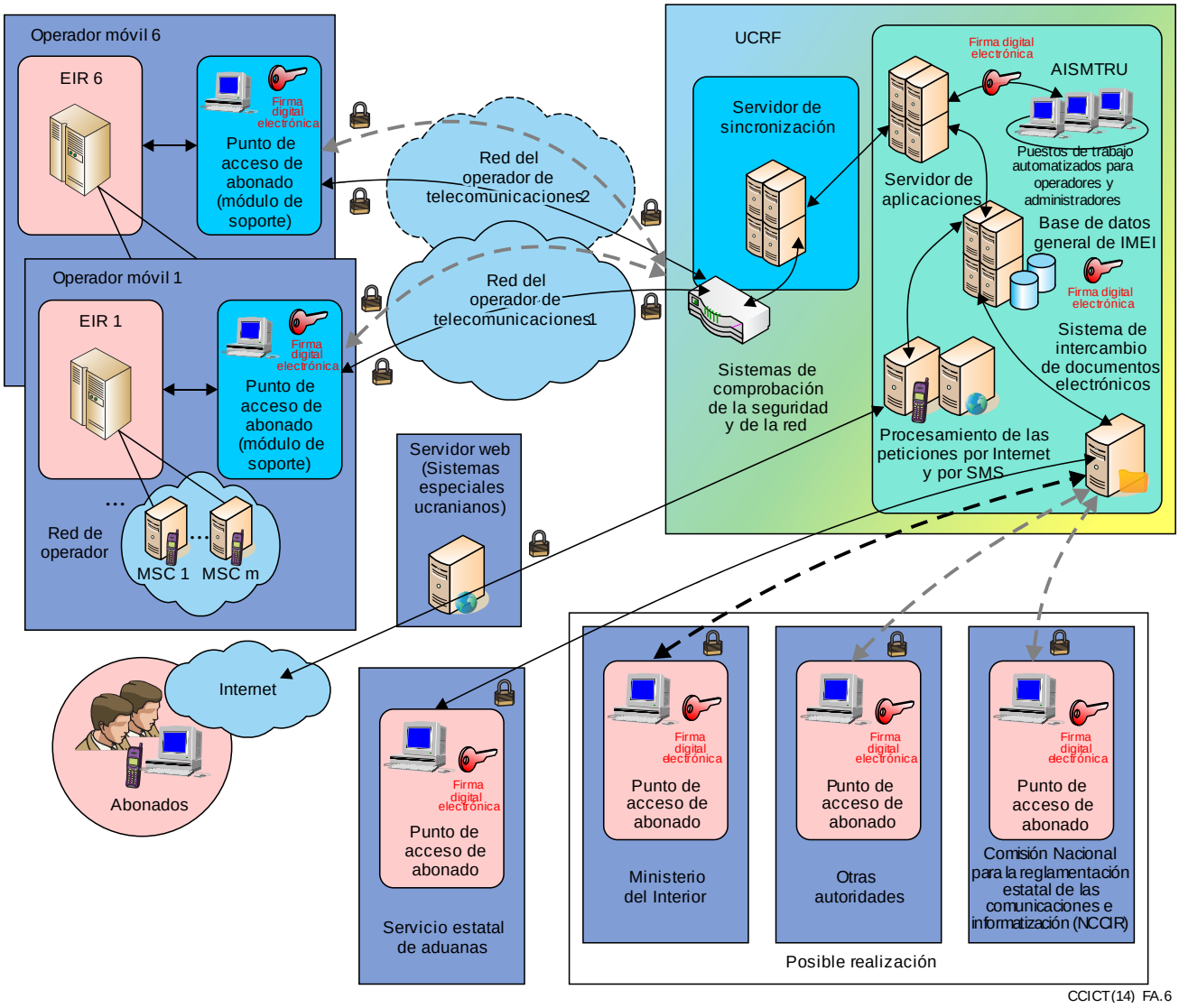

Figura A.6 – Sistema integral de protección de la información (CIPS) del AISMTRU

A.1.11.2.9 Efectos de la puesta en funcionamiento del sistema

1) Protección del consumidor

Cualquier comprador puede verificar la legalidad de un terminal móvil antes de su compra en Ucrania. Puede realizarse mediante la utilización del portal de Internet del UCRF o enviando un SMS con el IMEI por comprobar al número 307, común para todos los operadores móviles. Después de unos segundos, se obtiene una respuesta con el estado del IMEI enviado en la base de datos general de IMEI.

De esta manera, se protege el mercado ucraniano frente a los terminales que no cumplen con los requisitos de utilización especificados en Ucrania.

La legislación vigente ucraniana prohíbe la utilización de terminales móviles con números IMEI no registrados en la base de datos general de IMEI.

2) Lucha contra el robo de terminales

Los números IMEI de los terminales robados se incorporan a la "lista negra" bajo petición legal de un organismo y hacen inútil el robo de terminales.

El mismo procedimiento se sigue en el caso del bloqueo del terminal a petición de los propietarios de teléfonos perdidos.

3) Supresión de las importaciones ilegales

Durante la primera conexión a la red de cualquier operador, la red registra el terminal de manera inmediata. En el momento previsto (por lo noche), el operador móvil envía los números IMEI de los terminales conectados a su red (salvo los que están en itinerancia internacional) a la base de datos general de IMEI del AISMTRU.

AISMTRU identifica los números IMEI que no están incluidos en la "lista blanca" de la base de datos general de IMEI. Estos números IMEI se registran en la "lista gris". Todos los propietarios de los terminales reciben por SMS un aviso del posible bloqueo del terminal a los 90 días.

Al final del periodo de 90 días, el número IMEI es transferido de la "lista gris" a la "lista negra". Los terminales de la "lista negra" no son atendidos por los operadores (rechazo en el registro de red, salvo para las llamadas de emergencia al número 112). Una conexión a cualquier otra red de operador no cambia el estado "gris" o "negro" del terminal

Al recibir por SMS el aviso de la entrada en la "lista gris" y del límite de 90 días del servicio, el propietario puede dirigirse al UCRF para presentar una confirmación de la importación legal del terminal. El personal del UCRF revisa la petición del propietario y, en caso de confirmarse la importación legal, transfiere el código IMEI de la "lista gris" a la "lista blanca". Después de este procedimiento, los operadores prestan servicio al terminal sin límite de tiempo.

Sin embargo, hasta el momento no se desconectan los terminales de la "lista negra", debido a la falta de un instrumento legal.

El UCRF dispone de un centro de llamadas para atender las peticiones de los usuarios de terminales móviles sobre el estado del número IMEI y la importación de terminales.

4) Legalización del mercado de terminales en Ucrania

- La importación "gris" (ilegal) de terminales móviles en Ucrania ha caído de forma espectacular. La cuota de los terminales legalmente importados aumentó hasta el 93-95% en 2010 (frente al 7,5% en 2008).
- Se han ingresado más de 500 millones USD en el presupuesto del estado, en el periodo 2010-2012, provenientes de las tasas de importación de los terminales móviles, comparado con 30 millones USD aproximadamente durante los tres años anteriores.
- El mercado ucraniano de terminales móviles está compuesto principalmente de terminales móviles que cumplen con las características técnicas requeridas para su utilización en Ucrania.
- La base de datos general de IMEI del AISMTRU tiene registrados 140 865 260 números IMEI de terminales móviles a fecha de 30 de abril de 2013.
- El AISMTRU recuperó la inversión en siete meses solamente, con los pagos de los importadores recibidos por el UCRF.

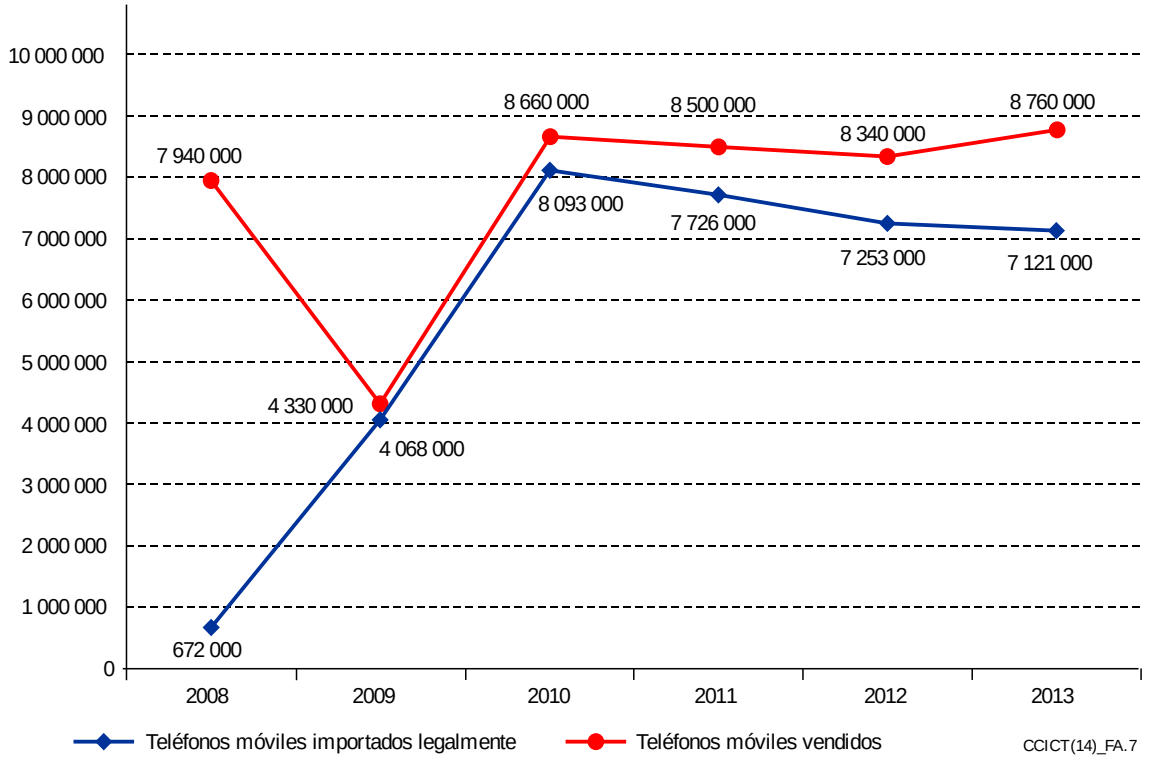

Figura A.7 – Efectos de la puesta en funcionamiento del AISMTRU en Ucrania

A.1.12 Emiratos Árabes Unidos (EAU)

Las leyes de telecomunicaciones en los Emiratos Árabes Unidos prohíben la utilización, la venta, la compra, la distribución y la publicidad de los dispositivos móviles falsificados. La Autoridad de Reglamentación de las Telecomunicaciones (Telecommunications Regulatory Authority, TRA) ha tomado todas las medidas necesarias para asegurar el cese completo de la venta y la utilización de estos dispositivos en los EAU. Se envían avisos y multas a los involucrados en la venta de teléfonos móviles falsificados y, en algunos casos, se podría llegar a retirar las licencias, cuando no se cumplen los reglamentos.

En 2011, la TRA lanzó una campaña http://www.uaeinteract.com/docs/TRA_urges_against_use_of_fake_cell_phones/47437.htm para informar y desalentar la utilización de los teléfonos móviles falsificados en los EAU, y anunció que a partir del 1 de enero de 2012, se dejaría de prestar servicio en la red móvil de telecomunicaciones de los EAU a todos los teléfonos móviles con un número IMEI fraudulento. La TRA publicó anuncios en los diarios avisando a la gente de la prohibición de los teléfonos falsificados.

Mientras que estas medidas pretendían dejar obsoleta la utilización de dispositivos móviles fraudulentos, los contratos de servicio no se han visto afectados y siguen funcionando normalmente al pasar a utilizar dispositivos telefónicos móviles legítimos. Al mandar un SMS con el número IMEI del dispositivo móvil al número 8877, los usuarios pueden recibir la respuesta de un operador sobre el estado del dispositivo móvil. Los prestadores de servicio se ponen en contacto inmediatamente con los usuarios de dispositivos móviles falsificados y los teléfonos no homologados deben ser desconectados de todos los servicios de telecomunicaciones, incluidos llamadas, mensajes de texto e Internet.

La TRA alertó de que los dispositivos móviles fraudulentos podían ser perjudiciales para la salud de los usuarios y alentó a todos los usuarios a adoptar las medidas adecuadas en la compra de los dispositivos móviles. De acuerdo con la TRA, los teléfonos móviles falsificados son particularmente propensos a las pérdidas y a las explosiones de las baterías, liberando productos altamente corrosivos y venenosos. La baja calidad también significa que los niveles de radicación

no se controlan, las baterías tienden a descargarse más rápidamente y la señal de recepción es generalmente mucho más débil.

Un objetivo principal de la TRA era la eliminación de los dispositivos móviles falsificados en los EAU y la educación del público en general y de los vendedores sobre los riesgos de su utilización. La TRA reconocía también que la falsificación y el pirateo tenían un gran impacto sobre la economía y los derechos de la propiedad intelectual, pero los teléfonos móviles eran también dispositivos de baja calidad que habían sido fabricados sin los controles y las pruebas adecuados.

A.2 Ejemplos de medidas conjuntas tomadas a escala regional

A.2.1 Comisión Interamericana de Telecomunicaciones (CITEL)

La Asamblea General de la Organización de Estados Americanos (OEA) estableció la Comisión Interamericana de Telecomunicaciones (CITEL) con el objetivo de promocionar el desarrollo de las telecomunicaciones y las TIC en las Américas. Los 35 estados son miembros, junto con más de 100 Miembros Asociados de la industria de las TIC.

El Comité Consultivo Permanente I (CCP.I: Telecomunicaciones) de la CITEL recomendó en 2009 a los Estados Miembros "que consideren la creación de bases de datos como parte de un programa integral contra la falsificación y el fraude" (Informe Final de la reunión 15 del CCP.I de la CITEL, 2 de octubre de 2009) y en diciembre de 2011 el CCP.II (Radiocomunicaciones incluyendo radiodifusión) inició el estudio de las medidas tomadas por las administraciones con respecto a la utilización de los teléfonos móviles falsificados.

El CCP.II decidió solicitar a las Administraciones que proporcionaran información "sobre las acciones y medidas reglamentarias y administrativas tomadas o planificadas con respecto a los teléfonos celulares falsos, falsificados y de baja calidad, y sus efectos negativos sobre los usuarios y operadores, incluyendo la interferencia, niveles de radiaciones no ionizantes (NIR) y el uso de componentes químicos peligrosos o prohibidos" (Informe Final de la reunión 18 del CCP.II de la CITEL, 22 de diciembre de 2011, Decisión 121).

La CITEL también ha considerado el problema del robo de los teléfonos móviles y los dos Comités Consultivos Permanentes han aprobado un cierto número de resoluciones relacionadas con estos temas.

El CCP.II aprobó la Resolución 73, en septiembre de 2011, sobre el "establecimiento de una alianza regional contra el hurto de equipos terminales móviles". Esta Resolución solicitaba al PCC.I considerar "que la CITEL promueva el establecimiento de medidas conjuntas de los Estados Miembros para restringir, en cualquier país de la región, la activación de estos equipos terminales móviles hurtados y adopte recomendaciones concretas dirigidas a los operadores para que utilicen los recursos que brinda la tecnología y se abstengan de permitir la conexión a sus redes de equipos cuyo origen no esté plenamente identificado, estableciendo una alianza regional contra el hurto de estos equipos" (Informe Final de la reunión 17 del CCP.II, 6 de septiembre de 2011, Resolución 73).

El CCP.I respondió casi inmediatamente con la aprobación de una resolución sobre "Medidas regionales contra el hurto de equipos terminales móviles" (Informe Final de la reunión 19 del CCP.I de la CITEL del 20 de septiembre de 2011, Resolución 189). Esta resolución observa la naturaleza internacional del problema pues cuando un país concreto toma medidas contra el robo de dispositivos, los dispositivos móviles se envían a otros países y, en consecuencia, existe la necesidad de tomar medidas a escala regional. Además de las medidas relativas a los teléfonos perdidos o robados, la Resolución 189 también insta a los Estados Miembros a "que consideren incluir en sus marcos regulatorios la prohibición de la activación y uso de los IMEI o el número de serie electrónico del fabricante de equipos reportados como hurtados, extraviados *o de origen*

ilegal, provenientes de bases de datos nacionales, regionales o internacionales" (las cursivas son del editor).

El Anexo de la Resolución 189 incorpora medidas complementarias como "estudiar la viabilidad de implementar controles a la comercialización local de equipos terminales móviles hurtados y su conexión a las redes" y "promover el establecimiento de mecanismos regulatorios, fiscales y/o aduaneros que garanticen la importación de equipos terminales móviles y/o repuestos de procedencia legitima, y que estén homologados conforme al marco normativo de cada país miembro, así como controles aduaneros que impidan la salida o reexportación de los equipos terminales móviles y/o repuestos, producto de hurto".

El CCP.I aprobó una recomendación sobre "Medidas regionales para el intercambio de información de equipos terminales móviles con reporte de hurto, robo o pérdida y recuperación" en 2012 (Informe Final de la reunión 20 del CCP.I de la CITEL, 10 de junio de 2012, Recomendación 16) que también incluyó los terminales "de origen ilegal". Se invita "a los Estados Miembros de la CITEL a implementar acciones e iniciativas nacionales, regionales e internacionales con el fin de que los proveedores de servicios de telecomunicaciones móviles intercambien información de terminales móviles robados, hurtados, extraviados o de origen ilegal a través de las diferentes plataformas existentes y operativas para las diferentes tecnologías de acceso para combatir los mercados informales, promoviendo la cooperación entre los países y garantizando los principios de la seguridad ciudadana y derechos del usuario final". También se alerta a los países miembros que deben "considerar además la creación de una plataforma de base de datos para el intercambio de información de los terminales móviles robados, hurtados, extraviados o de origen ilegal usando el identificador de equipo móvil (Mobile Equipment Identifier, MEID) empleado en los equipos usados por la tecnología del acceso múltiple por división de código (Code Division Multiple Access, CDMA), de EV-DO, de CDMA/4G de modalidad doble (dual mode CDMA/4G) y de RUIM (Removable User Identity Module, RUIM) que emplean muchas otras redes".

El CCP.I ha aprobado también la creación de una "carpeta técnica" sobre "Terminales móviles robados, hurtados y/o extraviados" (Informe Final de la reunión 23 del CCP.I de la CITEL, 10 de octubre de 2013, Resolución 217).

En mayo de 2014, la CITEL aprobó la Resolución 222 (XXIV-14) "*Fortalecimiento de medidas regionales para combatir la difusión de dispositivos móviles falsificados, subestandars y no homologados*".

Como resultado, se estableció un Grupo de correspondencia para "debatir las medidas regionales para combatir la difusión de dispositivos móviles falsificados, subestandars y no homologados, compartir información, experiencias y las mejores prácticas técnicas y reglamentarias con los Estados Miembros relacionados con el tema, y con el objetivo de desarrollar recomendaciones y directrices que se puedan implementar en la Región de las Américas".

En agosto de 2014, se aprobó el plan de trabajo de este Grupo de correspondencia e incorporó en el ámbito de la Relatoría sobre el control de fraude, prácticas antirreglamentarias en telecomunicaciones y medidas regionales contra el hurto de equipos terminales móviles con el siguiente mandato:

1) Elaborar una definición de que se entiende para los siguientes términos: dispositivos móviles falsificados, subestandars y no homologados.

2) Evaluar el alcance y carácter del problema de los dispositivos móviles falsificados, subestandars y no homologados.

3) Promover el intercambio de información y experiencias entre miembros de la CITEL respecto de las medidas tomadas para combatir el comercio y uso de dispositivos móviles falsificados, subestandars y no homologados.

4) Documentar las mejores prácticas de todo el mundo para combatir el comercio y uso de dispositivos móviles falsificados, subestandars y no homologados.

5) Proponer la creación de carpetas técnicas, recomendaciones y/o resoluciones de la CITEL encarando las medidas técnicas y reglamentarias para combatir el comercio y uso de dispositivos falsificados, subestandars y no homologados en la Región de las Américas.

6) Finalizar el trabajo e informar sobre los resultados obtenidos a la Relatoría sobre control de prácticas antirreglamentarias en telecomunicaciones y medidas reglamentarias contra el hurto de equipos terminales móviles.

A.2.2 Comunidad de África Oriental (East African Community, EAC)

África Oriental pierde más de 500 millones USD de ingresos por las imitaciones de productos http://www.trademarkea.com/ea-loses-huge-sums-of-money-in-counterfeit-products/. Los productos baratos y de baja calidad, suministrados por comerciantes y fabricantes, locales o extranjeros copian los nombres y los diseños de grandes marcas conocidas en el envoltorio.

De acuerdo con el Protocolo de Mercado Común, aprobado por la EAC en 2010, solamente la colaboración puede vencer a los productos falsificados y su comercio.

La Organización para las Comunicaciones de África Oriental (EACO), es un organismo regional que reúne los organismos reguladores, postales, de telecomunicaciones y de radiodifusión de los cinco Estados Miembros de la EAC (Kenya, Tanzanía, Rwanda, Burundi, y Uganda). La EACO consideró el problema de la invasión de teléfonos móviles falsificados en la región y aprobó una iniciativa común en 2012.

El Grupo Especial sobre numeración de la EACO (Comisión de Comunicaciones de Kenya (CCK), Organismo Regulador de las Comunicaciones de Tanzanía (TCRA), el Organismo Regulador de Servicios Públicos de Rwanda (RURA), la Agencia para la Regulación y el Control de las Telecomunicaciones de Burundi (ARCT), Comisión de Comunicaciones de Uganda (UCC)) recomendó en mayo de 2012 el desarrollo de una base de datos nacional y la adopción de los procedimientos para la verificación de los teléfonos móviles para proteger a los usuarios, las empresas y las redes de los efectos de las falsificaciones (Informe del Grupo Especial sobre numeración de la EACO para 2011-2012).

En el decimonoveno Congreso de la EACO en 2012, se informó del estado de las implementaciones de los registros de identidades de equipos (EIR) en la región y se describieron algunos de los problemas identificados http://www.eaco.int/docs/19_congress_report.pdf:

- clonado o ausencia del número de identidad internacional del equipo móvil (IMEI);
- falta de información de los consumidores sobre los peligros asociados con la utilización de equipos falsificados y falta de conocimiento de la manera de verificar si un equipo es genuino;
- falta de información de los comercios y revendedores sobre los problemas asociados con la venta de productos baratos de baja calidad; y
- el alto coste de la implementación.

Con el objetivo de superar estos retos, se propusieron las siguientes soluciones:

- lanzamiento de campañas de información para los consumidores y los vendedores locales;
- creación de una licencia para todos los vendedores y revendedores;
- mejora de los procedimientos de homologación;
- establecimiento de bases de datos de los equipos; y
- exigencia del registro de la tarjeta SIM.

A.2.3 Asociación de los Reguladores de Comunicaciones y Telecomunicaciones de la Comunidad de Países de Lengua Portuguesa (ARCTEL-CPLP).

La Asociación de los Reguladores de Comunicaciones y Telecomunicaciones de la Comunidad de Países de Lengua Portuguesa (ARCTEL-CPLP) tiene miembros de Angola, Brasil, Cabo Verde, Guinea-Bissau, Mozambique, Portugal, Santo Tomé y Príncipe y Timor Oriental (http://www.arctel-cplp.org). En el Simposio Mundial de Reguladores de la UIT de 2012, ARCTEL-CPLP presentó las iniciativas regionales contra el robo de móviles, el mercado de importación ilegal y los dispositivos falsificados. https://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR12/RA12/pdf/Batista3_ARCTEL_Session3_mobilerobbery.pdf

ARCTEL-CPLP propuso la extensión a escala regional de la solución tradicional (los sistemas de bases de datos de listas negras nacionales) para:

- compartir las bases de datos de listas negras de GSM y CDMA mediante acuerdos bilaterales o multilaterales;
- establecimiento de mecanismos reglamentarios fiscales y/o de aduanas para asegurar un mayor control de la importación de teléfonos móviles y prevenir la reexportación;
- acuerdo de la industria con las recomendaciones de seguridad contra la reprogramación o el clonado de número IMEI o del número de serie electrónico de identificación del fabricante;
- creación de campañas de información para sensibilizar a la población de la importancia de denunciar los robos y la pérdida de los dispositivos móviles.