Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Q.5051

(03/2020)

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

Lucha contra la falsificación y el robo de dispositivos TIC

Marco para luchar contra la utilización de dispositivos móviles robados

Recomendación UIT-T Q.5051

RECOMENDACIONES UIT-T DE LA SERIE Q

CONMUTACIÓN Y SEÑALIZACIÓN, Y MEDICIONES Y PRUEBAS ASOCIADAS

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

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

Recomendación UIT-T Q.5051

Marco para luchar contra la utilización de dispositivos móviles robados

Resumen

En la Recomendación UIT-T Q.5051 se propone un marco compuesto de requisitos y una amplia gama de medidas de amplio alcance cuya adopción y aplicación se recomienda para luchar contra el robo de dispositivos móviles y la reutilización de los robados.

El aumento de las funciones y capacidades disponibles en los dispositivos móviles ha acrecentado la importancia y utilización de estos dispositivos en la vida cotidiana de las personas durante los últimos años. Un efecto colateral cuya intensificación también se ha observado en algunos países, es el robo de estos dispositivos con ánimo de lucro, no sólo como consecuencia de la venta de los propios equipos sino también por la utilización ilegal de la información que se guarda en ellos.

Para responder a esta problemática, se necesitan iniciativas encaminadas a disuadir del robo de dispositivos móviles y la reutilización de los robados y a proteger los datos del consumidor que se guardan en estos dispositivos frente a su utilización ilegal. Es habitual que los dispositivos robados en un país, donde pueden haberse desplegado medidas para frenar la utilización de dispositivos robados, se vendan en otros países o en otras regiones donde no se hayan adoptado medidas de control similares. Por ese motivo resulta crítico para el éxito de tales iniciativas que se coordinen entre los gobiernos y los operadores que pretenden luchar contra el robo de dispositivos móviles y la reutilización de los robados en un entorno mundial, y que intercambien información. De lo contrario, existe el riesgo de que se facilite accidentalmente el comercio ilegal transfronterizo de dispositivos robados.

Cabe señalar que la mayor parte de las soluciones actualmente desplegadas para disuadir del robo de dispositivos y poner coto a su reutilización se basan en la existencia de listas de identificadores únicos. Para contrarrestar esas medidas los traficantes suelen manipular los dispositivos para alterar su identificador único y, en algunos casos, elegir identificadores utilizados en dispositivos legales. De este modo se pueden volver a colocar los equipos en el mercado y conectarlos a las redes móviles.

En esta tesitura, muchos países se han comprometido no sólo a luchar contra la utilización de dispositivos móviles robados, sino también a evitar que se reintegren a la red dispositivos con identificadores únicos reprogramados sin autorización, que suelen denominarse identificadores manipulados. Mientras tanto, los gobiernos de otros países se enfrentan al reto de dilucidar cuál es la mejor estrategia a adoptar, principalmente por falta de la experiencia técnica y los conocimientos necesarios para entender el problema y encontrar las posibles soluciones, y para elegir con conocimiento de causa las soluciones más convenientes, a la medida de sus respectivos países, para conseguir la mayor eficacia posible. En ese sentido, se necesitan directrices para responder a este reto, como se señala en la Resolución 97 de la AMNT (Hammamet, 2016).

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio	ID único*
1.0	UIT-T Q.5051	2020-03-13	11	11.1002/1000/14140

Palabras clave

Lucha contra los dispositivos móviles robados, conformidad, marco, requisitos, seguridad.

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

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

ÍNDICE

Recomendación UIT-T Q.5051

Marco para luchar contra la utilización de dispositivos móviles robados

1 Alcance

La presente Recomendación describe el marco de referencia y las necesidades que es preciso considerar para el despliegue de soluciones destinadas a luchar contra la utilización de dispositivos móviles robados.

2 Referencias

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

[UIT-T Q.5050] Recomendación UIT-T Q.5050 (2019), *Solución marco para contrarrestar la falsificación de dispositivos TIC*.

[UIT-T X.1058] Recomendación UIT-T X.1058 (2017), *Tecnología de la información – Técnicas de seguridad – Código de prácticas relativo a la protección de la información de identificación personal*.

[UIT-T X.1127] Recomendación UIT-T X.1127 (2017), *Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 usuario del dispositivo [UIT-T X.1127]: El usuario autorizado del dispositivo móvil.

3.1.2 herramienta de desactivación [b-GSMA]: Una "herramienta de desactivación" sirve para inhabilitar funciones esenciales de un dispositivo móvil. Se trata fundamentalmente de una funcionalidad del equipo móvil que, cuando se activa, por ejemplo, cuando se le envía un mensaje de un determinado formato, el móvil deja de funcionar adecuadamente y sólo pueda reactivarse o reutilizarse si el propietario del dispositivo lo autoriza.

3.1.3 teléfono móvil [b-UIT-T X-Sup.19]: Dispositivo electrónico utilizado para realizar llamadas telefónicas y enviar mensajes de texto en una amplia zona geográfica gracias al acceso radioeléctrico a redes móviles públicas, pudiendo el usuario puede estar en movimiento.

3.1.4 teléfono inteligente [b-UIT-T X-Sup.19]: Teléfono móvil con gran capacidad de cálculo, conectividad heterogénea y sistema operativo avanzado que constituye una plataforma para aplicaciones de terceros.

3.1.5 dispositivo TIC alterado [UIT-T Q.5050]: Dispositivo de tecnología de la información y la comunicación (TIC) cuyos componentes, software, identificador único y elementos están protegidos por derechos de propiedad intelectual o marcas registradas, que se ha alterado o tratado de alterar sin el consentimiento explícito del fabricante ni de su representante legal.

3.1.6 identificador único [UIT-T Q.5050]: Identificador asociado a un único dispositivo cuyo objetivo es identificarlo de forma exclusiva.

3.2 Términos definidos en la presente Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 identificador no válido: Identificador único que no se ajusta al formato definido en la normativa técnica o que no figura en la base de datos de referencia de identificadores de dispositivo distribuida por la entidad gestora responsable.

3.2.2 identificador clonado: Identificador de dispositivo válido debidamente asignado a un dispositivo por la entidad gestora responsable que está siendo utilizado por otros dispositivos diferentes.

3.2.3 identificador único fiable: Será único para cada equipo que se pretenda identificar, sólo podrá ser asignado por una entidad gestora responsable y no deberá ser modificado por terceros no autorizados.

4 Siglas y acrónimos

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

EIR Registro de identidades de equipo (*equipment identity register*)

IIP Información de identificación personal

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

IMSI Identidad internacional del abonado móvil (*international mobile subscriber identity*)

RUI Identificador único fiable (*reliable unique identifier*)

TAC Código de homologación (*type allocation code*)

5 Convenios

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

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

b) La utilización del verbo "deber" en presente o la expresión "se recomienda" indican que se trata de un requisito recomendado y que, por ende, no es absolutamente obligatorio. Su cumplimiento no es indispensable para poder declarar la conformidad.

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

6 Consideraciones generales

El aumento de las funcionalidades y capacidades disponibles en los dispositivos móviles ha acrecentado la importancia y utilización de estos dispositivos en la vida cotidiana de las personas durante los últimos años. Un efecto colateral cuya intensificación también se ha observado en algunos países, es el robo de estos dispositivos con ánimo de lucro, no sólo como consecuencia de

la venta de los propios equipos sino también por la utilización ilegal de la información que se guarda en ellos.

Para responder a esta problemática, se necesitan iniciativas encaminadas a disuadir del robo de dispositivos móviles y la reutilización de los robados y a proteger los datos del consumidor que se guardan en estos dispositivos frente a su utilización ilegal. Es habitual que los dispositivos robados en un país, donde pueden haberse desplegado medidas para frenar la utilización de dispositivos robados, se vendan en otros países o incluso en otras regiones donde tal vez no se hayan adoptado medidas de control similares. Por ese motivo resulta crítico para el éxito de tales iniciativas que se coordinen entre los gobiernos y los operadores de los diferentes países que pretenden luchar contra el robo de dispositivos móviles y la reutilización de los robados en un entorno mundial, y que intercambien información. De lo contrario, existe el riesgo de que se facilite accidentalmente el comercio ilegal transfronterizo de dispositivos robados.

En esta tesitura, muchos países se han comprometido no sólo a luchar contra la utilización de dispositivos móviles robados, sino también a evitar que se reintegren a la red móvil dispositivos con identificadores únicos reprogramados sin autorización, que suelen denominarse identificadores manipulados. Mientras tanto, los gobiernos de otros países se enfrentan al reto de dilucidar cuál es la mejor estrategia a adoptar, principalmente por falta de la experiencia técnica y los conocimientos necesarios para entender el problema y encontrar las posibles soluciones, y para elegir con conocimiento de causa las soluciones más convenientes, a la medida de sus respectivos países, para conseguir la mayor eficacia posible. En ese sentido, se necesitan directrices para responder a este reto, como se señala en la Resolución 97 de la Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT) (Hammamet, 2016).

Por consiguiente, en la presente Recomendación se describe un marco compuesto de requisitos y una amplia gama de medidas de amplio alcance cuya adopción y aplicación se recomienda para luchar contra el robo de dispositivos móviles y la reutilización de los robados.

7 Requisitos de alto nivel

Las partes interesadas deben afrontar varios retos al desplegar soluciones para luchar contra la utilización de dispositivos móviles robados. Al utilizar estas soluciones para luchar contra el robo de dispositivos móviles, los países deben tener en cuenta los requisitos expuestos en esta cláusula.

7.1 Impedir la utilización de dispositivos móviles robados por usuarios no autorizados

Es necesario implementar soluciones que permitan desactivar los dispositivos que hayan sido objeto de robo o extravío, para impedir que puedan ser utilizados por usuarios no autorizados.

Es necesario que este proceso se ejecute automáticamente cuando un usuario no autorizado intente acceder al dispositivo un cierto número de veces (por ejemplo, cuando el usuario no autorizado no consiga introducir la contraseña o el número de identificación personal (PIN, *personal identification number*) correctos tras un cierto número de intentos).

Se recomienda que este proceso pueda activarlo a distancia el usuario autorizado del dispositivo cuando lo solicite (por ejemplo, mediante la sensibilización de una herramienta de desactivación en el dispositivo extraviado/robado).

Es necesario que exista la opción de revertir la inutilización del dispositivo si el usuario autorizado lo recupera y la de restaurar los datos del usuario en el dispositivo en la medida posible.

En [UIT-T X.1127] se abordan los requisitos de seguridad y arquitecturas funcionales para las medidas antirrobo de teléfonos móviles. En esa Recomendación se describe la implementación de una herramienta de desactivación destinada a ser utilizada en caso de extravío o robo de un teléfono inteligente. Esa herramienta debe ofrecer las siguientes capacidades:

– suprimir a distancia los datos del usuario guardados en el teléfono inteligente;

– dejar el teléfono móvil inservible para un usuario no autorizado;
– impedir su reactivación, dentro de lo tecnológicamente posible, sin autorización previa del usuario autorizado;
– cancelar la desactivación del teléfono inteligente en el caso de que lo recupere el usuario autorizado y restaurar, en la medida de lo posible, los datos del usuario en el teléfono inteligente;
– rastrear la localización del dispositivo móvil perdido o robado.

Además, se recomienda enseñar a los usuarios de los dispositivos móviles cómo configurar y utilizar esta funcionalidad y denunciar el extravío/robo de dispositivos móviles a sus proveedores de servicios o instancias policiales o judiciales pertinentes, con el fin de impedir que los dispositivos puedan acceder a redes móviles y para que las autoridades competentes adopten las medidas oportunas.

7.2 Impedir que los dispositivos móviles robados accedan a la red

Es necesario implementar soluciones que impidan que los dispositivos móviles robados accedan a las redes móviles, preferiblemente mediante sistemas automáticos que puedan ser objeto de auditoría.

Es necesario que sólo las personas autorizadas, tales como el legítimo propietario del dispositivo, puedan solicitar que un dispositivo móvil robado se reintegre en todas las redes del país, o bien que se suprima de éstas.

Se recomienda elaborar un marco de políticas orientadas a impedir la utilización de los dispositivos robados en la red.

Es importante observar que los dispositivos bloqueados en las redes móviles, utilizando a sus identificadores únicos, pueden seguir teniendo acceso a redes que no verifiquen estos identificadores únicos de dispositivos móviles, tales como las redes fidelidad inalámbrica (Wi-Fi). Por ello es importante complementar esta solución con otras tales como las descritas en la cláusula 7.1.

7.3 Impedir la utilización de dispositivos móviles con identificadores únicos manipulados y/o clonados

Es necesario implementar una solución que permita identificar los dispositivos móviles cuyos identificadores hayan sido manipulados y/o clonados para distinguirlos de los dispositivos auténticos, con una precisión considerable, con el fin de adoptar medidas disruptivas, preferiblemente mediante sistemas automáticos, sin repercusión alguna sobre los dispositivos auténticos.

Es necesario que las bases de datos de referencia se integren en esta solución con el fin de identificar la información perteneciente a los dispositivos auténticos y el origen legal de los mismos. Deben utilizarse las bases de datos nacionales de registro como medio de identificación de los teléfonos importados y adquiridos legalmente y las bases de datos con identificadores atribuidos a los fabricantes y demás características de los dispositivos como fuente de información para la base de datos de referencia con el fin de facilitar la diferenciación entre los dispositivos auténticos y los manipulados.

Es necesario considerar en el marco de esta solución que los identificadores manipulados pueden enmarcarse en diferentes tipologías que deben contemplarse en el proceso de detección y control, tales como: identificadores no válidos, clonados y, en su caso, no homologados o no registrados en bases de datos nacionales de referencia.

7.4 Impedir que los dispositivos móviles robados de otros países tengan acceso a la red

Se recomienda que la legislación y los reglamentos locales faciliten la coordinación y el intercambio de información entre los gobiernos y los operadores de los diversos países para impedir la utilización de dispositivos robados con independencia del lugar donde fueron sustraídos.

Al no incentivar y facilitar el intercambio de datos a nivel internacional se deja vía libre al comercio ilegal de dispositivos robados en el ámbito internacional lo que da lugar a que los dispositivos robados en un país pudieran exportarse y venderse en otros países o regiones.

Se recomienda contar con una base de datos de dispositivos robados a la que puedan tener acceso todos los integrantes de cualquier país del mundo con el fin de denunciar los robos de dispositivos y verificar el estado de un dispositivo para abordar este problema y dar solución al mismo.

Las listas negras nacionales de dispositivos deben intercambiarse y ponerse a disposición de la comunidad mundial, y exigirse la conexión y el intercambio de los datos relativos a los dispositivos locales robados con la base de datos mundial de dispositivos robados.

7.5 Reducir la repercusión en el consumidor

En toda solución que se adopte para impedir la utilización de dispositivos móviles robados debe considerarse la repercusión en el consumidor. Cuando existan varias opciones para lograr el mismo objetivo, deberá adoptarse la de menor repercusión global en los consumidores legítimos.

Se recomienda controlar los dispositivos con identificadores no válidos que hayan sido activados recientemente en las redes, previa notificación a los usuarios, concediéndoles un plazo adecuado y suficiente para que demuestren que los han adquirido legalmente, así como para atenuar la repercusión de una súbita denegación de servicio al dispositivo o evitarla.

Se recomienda no bloquear el abono del usuario al servicio cuando se adopten medidas para controlar los dispositivos con identificadores manipulados y/o clonados.

Se recomienda realizar campañas públicas educativas y de sensibilización, que alcancen la máxima difusión posible, sobre las medidas que proceda adoptar, su objeto, sus beneficios y las alternativas y acciones que los usuarios pueden emprender si pierden sus teléfonos o se los sustraen, o si adquieren dispositivos cuyos identificadores hayan sido manipulados o clonados.

Se recomienda considerar el establecimiento de amnistías o periodos transitorios cuando se adopten medidas contra los dispositivos cuyos identificadores hayan sido manipulados y/o clonados, ya que los dispositivos que ya se estén utilizando pueden haber sido adquiridos de buena fe sin que los usuarios hayan sido conscientes de los riesgos que asumían. En el caso de que se decida no bloquear los dispositivos antiguos, deben adoptarse medidas adicionales para impedir que dichos dispositivos sean activados con nuevos usuarios.

Se recomienda establecer sistemas eficaces de recopilación de informes e información de los usuarios con el fin de proceder a la suspensión de los servicios y al bloqueo de los identificadores de los dispositivos.

Se recomienda facilitar la determinación del identificador del dispositivo a bloquear sin pedirle al usuario que lo recuerde o que lo busque, por ejemplo, investigando en el registro de llamadas la actividad del dispositivo en la red del operador en cuestión con el fin de averiguar el identificador extraviado/robado.

Se recomienda suspender los servicios de los dispositivos extraviados/robados y bloquear sus identificadores a la mayor premura posible, por ejemplo, bloqueando el dispositivo tan pronto hayan validado la solicitud correspondiente las instancias responsables de dicha acción.

Se recomienda dotar de instrumentos adecuados a todas las instancias para que pueden comprobar y verificar si un determinado dispositivo se ha bloqueado.

Se recomienda que la instancia responsable del bloqueo del dispositivo comunique al usuario cuándo se ha bloqueado aquél o, cuando se haya denegado su bloqueo, los motivos que impiden el bloqueo del dispositivo denunciado.

7.6 Protección de los datos privados del consumidor

Cuando se extravía un dispositivo o es objeto de robo, los datos privados del consumidor deben quedar protegidos. Como medida principal, se recomienda implementar mecanismos que impidan utilizar el dispositivo, incluso acceder a los datos privados que haya introducido en el mismo un usuario autorizado.

Se recomienda sensibilizar a los consumidores sobre la importancia de proteger sus datos personales y disponer de una copia de seguridad, y formarlos en el manejo de las funcionalidades que les permiten borrar a distancia la información de identificación personal (IIP) que se guarda en el dispositivo, si se lo roban.

Se recomienda que los fabricantes incluyan en todos los dispositivos nuevos, por defecto, las características especificadas en [UIT-T X.1127].

Se recomienda que las partes interesadas enseñen a los consumidores cómo configurar y utilizar esta funcionalidad.

7.7 Impedir que los dispositivos móviles robados tengan acceso a los mercados

Se recomienda que los organismos reguladores de las telecomunicaciones nacionales colaboren con otros organismos nacionales pertinentes (por ejemplo, Aduanas) para mejorar el control de los dispositivos denunciados como extraviados o robados en el propio país y en otros países.

En el marco de esta colaboración, debe contemplarse, cuando proceda, lo siguiente:

1) El acceso a las bases de datos de dispositivos robados pero también a información adicional (tal como la relativa a dispositivos no válidos o no homologados), teniendo en cuenta que se puede alterar el identificador único para eludir las bases de datos nacionales e internacionales de dispositivos robados.
2) El acceso a una base de datos mundial de identificadores atribuidos a fabricantes legítimos, con el fin de validar si la estructura de los identificadores pertenece a los dispositivos que se pretende importar.
3) El acceso a la lista de marcas y modelos de dispositivos homologados con el fin de autorizar exclusivamente la importación de los modelos de dispositivos homologados con arreglo a los reglamentos nacionales pertinentes.
4) El acceso a las bases de datos nacionales de referencia en las que se registran los identificadores de los dispositivos importados y adquiridos legalmente, como corresponda.
5) El acceso a una base de datos mundial de dispositivos robados y a una base de datos que contenga información específica de los dispositivos para poder confirmar la autenticidad de los mismos. Esta última sería de interés cuando el identificador único del dispositivo robado pudiera haber sido manipulado y reprogramado con un identificador que representase a un dispositivo diferente.

Se recomienda consultar el identificador completo en la base de datos nacional de dispositivos, con el fin de impedir la entrada de un dispositivo con un identificador que corresponda a otro dispositivo que ya haya entrado al país.

Se recomienda adoptar las medidas jurídicas oportunas contra los puntos de venta que ofrezcan dispositivos robados.

7.8 Otras consideraciones para luchar contra la manipulación de los identificadores únicos de los dispositivos móviles robados

Entre las consideraciones que pueden tenerse en cuenta para luchar contra la manipulación de los dispositivos móviles robados figuran las siguientes:

- Considerar la creación de marcos de políticas que impidan la utilización o venta en el mercado de dispositivos móviles robados.
- Impartir educación y formación sobre los aspectos técnicos del robo y la manipulación de los identificadores únicos de los dispositivos móviles.
- Considerar la implantación de controles sobre la utilización de hardware y/o software de manipulación de identificadores de dispositivos móviles.

Se recomienda establecer los fundamentos y el apoyo jurídico necesario para que las autoridades competentes puedan sancionar a quienes modifiquen, alteren, borren o manipulen identificadores de dispositivos móviles con el objetivo de eludir las medidas adoptadas para impedir la utilización de los dispositivos móviles robados en el mercado.

Se recomienda que en dicho marco jurídico se contemplen también las medidas que proceda adoptar frente a quienes ofrezcan, posean, importen o vendan hardware y/o software de manipulación de identificadores de dispositivos móviles.

Se recomienda que se eduque y se forme a las fuerzas y cuerpos de seguridad en los aspectos técnicos relativos al robo y la manipulación de identificadores únicos de dispositivos móviles, y sobre el marco jurídico que permita la persecución de estos delitos.

Se recomienda que los fabricantes de dispositivos móviles incluyan mecanismos para garantizar la fiabilidad e integridad de los identificadores únicos de dispositivos móviles.

8 Requisitos marco

Al desplegar una solución para luchar contra el robo de dispositivos móviles, se deben tener en cuenta los siguientes requisitos.

8.1 Base de datos de referencia centralizada

Se recomienda utilizar una base de datos de referencia centralizada con información de los dispositivos extraviados y robados. Así pues, para evitar que los dispositivos robados tengan acceso a cualquier red móvil, todos los operadores deberán utilizar esta base de datos. Esta base de datos deberá registrar, como mínimo, el identificador único del dispositivo robado, la fecha del robo y la entidad que introdujo esta información en la base de datos.

Se recomienda que dicha base de datos incluya otros tipos de identificadores e información que facilite la identificación y la resolución del problema de los dispositivos robados con identificadores manipulados.

Se recomienda que en esta base de datos de referencia se registre también información sobre los dispositivos importados y/o adquiridos legalmente.

Se recomienda que las instancias autorizadas tengan acceso a todas las bases de datos pertinentes.

Se recomienda implementar con carácter obligatorio la inscripción de los dispositivos. Cuando se implemente la inscripción de los dispositivos con carácter obligatorio, deberá prestarse particular atención a la vinculación de los dispositivos con la IIP, y a los efectos colaterales sobre el comercio de dispositivos móviles legales y la competencia en el mercado móvil.

Se recomienda implementar procedimientos de auditoría para verificar si se han bloqueado los dispositivos robados denunciados y si todas las partes interesadas han adoptado los procedimientos correctos.

8.2 Soporte de la red al bloqueo de dispositivos

Es necesario que las redes móviles cuenten con elementos capaces de impedir el acceso de dispositivos robados cuyos identificadores válidos se hayan incluido en la lista negra y también el de dispositivos que transmitan identificadores con un formato que no se ajuste a las normas de los identificadores únicos[1].

Se recomienda que las soluciones de bloqueo que se utilizan en las redes móviles soporten características que impidan la utilización de dispositivos con identificadores únicos clonados y por lo tanto sean capaces de distinguir los dispositivos auténticos de los clonados[2].

8.3 Identificadores únicos fiables

Se recomienda que las bases de datos de referencia que se utilicen para impedir que los dispositivos móviles robados tengan acceso a las redes móviles se basen en identificadores únicos fiables (RUI, *reliable unique identifiers*), ya que la manipulación de los identificadores únicos de los dispositivos puede afectar negativamente a la eficacia de las soluciones implementadas para retirar del mercado los dispositivos robados.

Se recomienda que los dispositivos móviles guarden[3] su identificador único en un elemento seguro del equipo y que los dispositivos implementen medidas de seguridad, dentro de lo tecnológicamente posible, para detectar la manipulación del elemento seguro o de la información guardada en éste y que, en caso de que ésta se haya producido, deje inservible el dispositivo en cuestión hasta tanto no se hayan restaurado los datos originales.

Se recomienda que la entidad de gestión responsable de estos identificadores únicos implemente un proceso de incentivación de la utilización correcta y segura de los identificadores únicos por parte de los fabricantes de los dispositivos legítimos a los que se han atribuido los identificadores.

Se recomienda que los identificadores únicos cumplan los principios de integridad (todos y cada uno de los fabricantes deben tener rangos de identificadores atribuidos por la entidad designada) y los principios de seguridad definidos por la industria (todos las medidas previstas o una combinación de éstas para implementar los identificadores de forma que resulte imposible manipularlos)[4].

Se recomienda que los gobiernos y los marcos reglamentarios nacionales apoyen los procesos implementados por la industria para hacer que se cumplan estos principios.

Es necesario que los identificadores únicos no sean reprogramables, ni siquiera durante las operaciones de mantenimiento. Si se permite que se modifiquen los identificadores después del proceso de fabricación, se puede menoscabar la seguridad de los identificadores únicos, y facilitar su manipulación por parte de un tercero no autorizado.

8.4 Estrechar la colaboración con las fuerzas y cuerpos de seguridad y otros organismos nacionales

Para limitar de manera efectiva la circulación de dispositivos robados en el mercado, es necesario establecer una estrecha colaboración entre las autoridades responsables de mantener y facilitar el

---

1 Véanse [b-3GPP TS 122.016] y [b-3GPP TS 123.003] para los dispositivos conformes con 3GPP/3GPP2.

2 Para los dispositivos conformes con 3GPP/3GPP2 que utilicen el IMEI como identificador único, el soporte de la verificación IMEI-IMSI de la red de acceso radioeléctrico a la red central puede ayudar a satisfacer esta necesidad.

3 Por ejemplo, según la definición de [b-3GPP TS 122.016], el IMEI no debe cambiarse.

4 Por ejemplo, véase [b-IMEI-SEC] para dispositivos móviles compatibles con 3GPP.

acceso a las bases de datos de referencia, los organismos nacionales de aduanas y entre estas entidades de distintos países y las partes interesadas pertinentes. Se habrá de considerar lo siguiente:

– Dado que los organismos de aduanas y otras autoridades nacionales competentes y autorizadas desempeñan un papel fundamental en la vigilancia e interceptación de productos robados, perdidos o manipulados, es importante proporcionarles los instrumentos necesarios para identificar los dispositivos robados, extraviados, manipulados e incluso los legales, tales como la Base de Datos de Referencia Centralizada.
– Deben establecerse procedimientos de fiscalización y comunicación entre las diferentes organizaciones que sean plenamente operativos. Entre ellos podría considerarse el intercambio de información pertinente, tal como la de las bases de datos de dispositivos móviles conformes con las normas nacionales, regionales o internacionales.
– El comercio ilegal de dispositivos móviles robados, puede combatirse mediante mecanismos que permitan autenticar la identidad de un determinado dispositivo con el fin de comprobar si es genuino, y si la legislación y reglamentación de ese país permite su utilización.
– Las fuerzas y cuerpos de seguridad, a tenor del marco jurídico nacional, pueden optar por no bloquear inmediatamente los dispositivos con fines de investigación, a fin de identificar el origen de los dispositivos robados que se están vendiendo en el mercado, aunque debe considerarse preferente el bloqueo de todos estos dispositivos tan pronto como sea posible, salvo que existan motivos válidos excepcionales que justifiquen el no hacerlo en casos puntuales.

Se recomienda que sean las más altas instancias gubernamentales las que definan la estrategia principal al máximo nivel con el fin de estimular la formación de alianzas y la adopción de un conjunto de medidas de amplio alcance que faciliten los compromisos y la ejecución de actividades de diferentes sectores y autoridades independientes de la industria (por ejemplo, fuerzas y cuerpos de seguridad, aduanas, comercio, etc.).

8.5 Herramientas para verificar el estado de los dispositivos móviles

Es necesario poner a disposición de los consumidores y de otras partes interesadas una herramienta de acceso público que les permita verificar el estado de los dispositivos móviles. Los consumidores y otras partes interesadas deben poder consultar, preferiblemente por Internet, si un determinado dispositivo está identificado como robado o extraviado.

Se recomienda identificar la entidad responsable del bloqueo del dispositivo en la respuesta a la consulta sobre un dispositivo (incluido el país al que se aplica el bloqueo) con el fin de evitar que el consumidor compre o adquiera un dispositivo robado así como para atender a las reclamaciones motivadas por un bloqueo improcedente o el bloqueo de un tercero provocado por un dispositivo clonado con el mismo identificador. Además, esta herramienta es importante para que el consumidor compruebe la situación del dispositivo antes de comprarlo.

Se recomienda que los minoristas y las entidades implicadas en el manejo de dispositivos verifiquen los que adquieran para asegurarse de que no se haya denunciado su extravío, robo, o la duplicación de su identificador único. Debe mantenerse un registro que permita demostrar que se ha observado la debida diligencia para impedir la compraventa de dispositivos cuyo extravío, robo, o la duplicación de su identificador único hayan sido objeto de denuncia.

8.6 Apoyo a los marcos jurídicos y reglamentarios nacionales aplicables

Se recomienda crear mecanismos que permitan identificar y bloquear en las redes móviles los dispositivos extraviados y robados, y también aquéllos cuyos identificadores únicos se hayan manipulado, siempre que sea técnicamente viable, cosa que debe comprobarse con los operadores de las redes móviles locales.

Se recomienda contar con el respaldo de los marcos jurídicos y reglamentarios nacionales aplicables, antes de implementar cualquier medida restrictiva contra los dispositivos robados con identificadores únicos manipulados y duplicados, en cuanto a:

– La restricción del acceso de los dispositivos robados a las redes de telecomunicaciones, con independencia de que las denuncias se hayan presentado en el propio país o en el extranjero.
– La restricción del acceso de los dispositivos con identificadores manipulados a las redes de telecomunicaciones.
– La restricción que prohíbe la manipulación de los identificadores únicos de los dispositivos móviles, y las consecuencias que ello acarrea.
– El establecimiento de las soluciones necesarias para que las autoridades, los consumidores y el canal de venta puedan distinguir los productos auténticos de los robados y manipulados.
– La institución de una autoridad responsable de exigir el cumplimiento de los puntos anteriores.

En este contexto, deben consultarse la legislación y los marcos reglamentarios nacionales existentes que quizá ya contemplen los aspectos considerados.

9 Marco de referencia

A continuación se ilustra en la Figura 1 una propuesta de marco de referencia, basada en los requisitos marco esbozados en la cláusula 8, para luchar contra el robo y la utilización de los dispositivos móviles robados. Conviene señalar que no todos los elementos funcionales de la Figura 1 son obligatorios y que cada país puede implementar los elementos que se ajusten a sus necesidades.

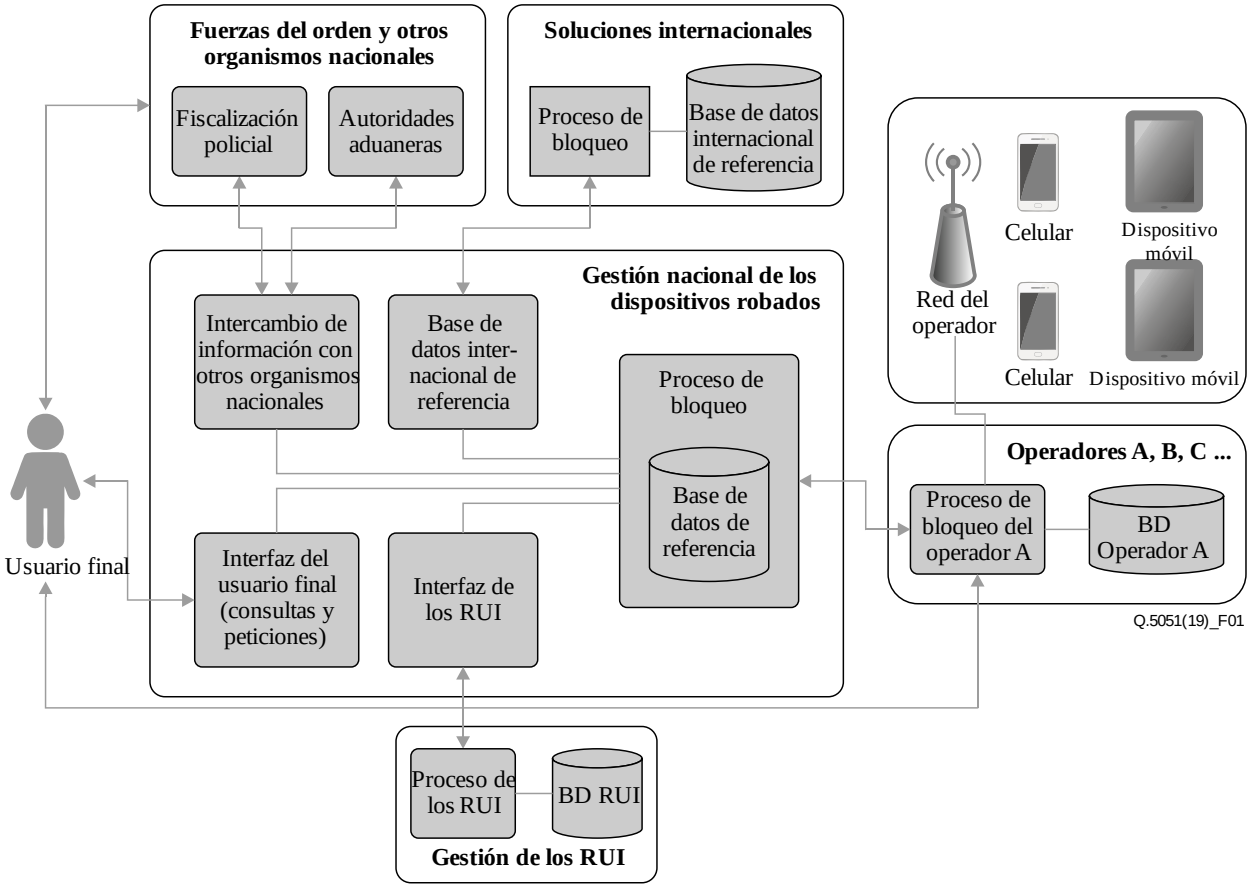

Figura 1 – Marco general propuesto

Deben combinarse diversas actividades y sistemas de información, gestionados por diferentes organizaciones, con el fin de colaborar para controlar y proporcionar información esencial para identificar y luchar contra la utilización de dispositivos móviles extraviados, robados y de aquellos cuyos identificadores no sean válidos.

Los consumidores y demás partes interesadas deben poder consultar si un cierto dispositivo está afectado por alguna restricción (robado, extraviado o con un identificador no válido).

La solicitud de bloqueo de un dispositivo robado puede presentarse a través de diferentes instancias (consumidores, fuerzas y cuerpos de seguridad, operadores móviles o directamente en el sistema central). Deben adoptarse medidas para la validación de la identidad del usuario y la titularidad del dispositivo con independencia del lugar donde se haya presentado la solicitud de bloqueo del dispositivo en uso. Para los dispositivos que no se hayan vendido a un consumidor, por ejemplo los robados en tránsito, en los comercios minoristas, etc., la denuncia legal debe venir acompañada de la solicitud de bloqueo del dispositivo.

Para que se posible limitar la circulación de dispositivos robados en el mercado, otros organismos nacionales pertinentes (por ejemplo, las fuerzas y cuerpos de seguridad y las administraciones de aduanas) deben tener la capacidad de consultar el estado de los dispositivos en todas las bases de datos de referencia y fuentes de información disponibles.

Es indispensable que se pueda intercambiar información con instituciones internacionales, ya sea con carácter bilateral o a través de una base de datos de referencia mundial.

Para garantizar la eficacia del bloqueo de los dispositivos robados en las redes móviles del país, todos los operadores deben sincronizarse con una base de datos de referencia nacional y mundial.

Es necesario que la gestión de las RUI se integre con el proceso de bloqueo de móviles robados, ya que es posible que se manipulen los identificadores únicos de ciertos dispositivos para eludir el proceso de bloqueo.

Es necesario implementar un proceso de identificación y control de dispositivos móviles con identificadores no válidos en las redes que se hayan manipulado con posterioridad al bloqueo de los dispositivos robados.

10 Características deseables

Durante el despliegue de una solución para luchar contra la utilización de los dispositivos móviles robados, los países deben tener en cuenta las características deseables expuestas en las siguientes cláusulas:

10.1 Base de datos de referencia mundial de dispositivos extraviados y robados

Como los dispositivos bloqueados pueden transportarse a diferentes países e incluso venderse a los consumidores de éstos, se recomienda utilizar una base de datos de referencia mundial para intercambiar información sobre los identificadores de los dispositivos robados y bloquearlos, con el fin de crear una lista negra de dispositivos robados en un solo punto de información que facilite el intercambio de datos y agilice el bloqueo.

Se recomienda que, con independencia de la importancia del operador, se impida a todos los dispositivos cuyos identificadores figuren en esta base de datos de referencia mundial que se conecten a una red local, a pesar de los planteamientos alternativos que se puedan considerar dependiendo del entorno específico de cada implementación (por ejemplo, proceso por lotes para la comparación de los identificadores únicos activos con los registrados en la base de datos de referencia mundial).

Es necesario que la base de datos de referencia mundial esté a disposición de las fuerzas y cuerpos de seguridad y de otros organismos gubernamentales a efectos de la tramitación de denuncias y la evacuación de consultas de grupos de identificadores con el fin de facilitar la ejecución de sus acciones legales de lucha contra el robo de dispositivos móviles.

Se recomienda verificar la exactitud de los datos relativos a los dispositivos cuyo robo se ha denunciado, antes de incluirlos en la base de datos mundial. Sólo se entregarán las listas de dispositivos robados confeccionadas por las partes mencionadas anteriormente, para su inclusión en esta base de datos mundial de dispositivos robados, cuando se hayan verificado debidamente.

Esta base de datos mundial debe ponerse a disposición de todas las partes interesadas de cualquier lugar del mundo para que puedan verificar si un determinado dispositivo ha sido denunciado como robado. El acceso a la base de datos debe poder efectuarse tanto a nivel del sistema, para las instancias que puedan bloquear los dispositivos robados, como a nivel del consumidor, para que los consumidores de cualquier país puedan comprobar si un dispositivo ha sido denunciado como robado.

La base de datos mundial debe facilitar la información adecuada, siempre que disponga de ella (por ejemplo, las características del dispositivo, el país donde se produjo el robo, la fecha del hecho, etc.). Si los identificadores del dispositivo robado aparecieran en varios países, la base de datos mundial debería facilitar dicha información en sus resultados.

Deben implementarse procedimientos que permitan a los participantes en la base de datos mundial abordar las situaciones de bloqueo improcedente (por ejemplo, bloqueo erróneo o debido a la duplicación o clonación de identificadores).

10.2 Medidas aplicables a los establecimientos que vendan dispositivos extraviados, robados o manipulados

Se recomienda que los países estudien la creación de un marco de definición de responsabilidades de los puntos de venta para que sólo pongan a la venta dispositivos homologados y en el que se señalen las consecuencias de vender dispositivos robados o con identificadores manipulados. Esto dotará a las fuerzas y cuerpos de seguridad del respaldo jurídico necesario para combatir la venta y la demanda de tales dispositivos.

También se podrían incluir en la base de datos de referencia nacional los identificadores de los dispositivos importados y vendidos legalmente. Esta base de datos podría ser de gran utilidad para una diversidad de medidas y actividades nacionales de fiscalización, por ejemplo las relativas a la importación, la venta, la utilización en las redes y la actuación de las fuerzas y cuerpos de seguridad.

Así pues, el acceso a esta base de datos de dispositivos autorizados podría ayudar a las fuerzas y cuerpos de seguridad a aplicar las medidas oportunas contra los establecimientos que vendieran al público dispositivos robados, manipulados o clonados, e incluso a identificar e interceptar productos que se hubieran importado ilegalmente.

Apéndice I

Planteamiento de la GSMA para luchar contra el robo de dispositivos móviles

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

Cada vez son más los países en los que los operadores permiten que los consumidores denuncien el robo o el extravío de dispositivos móviles. Ante una denuncia, el operador de la red móvil puede averiguar el identificador único del dispositivo, o sea la identidad internacional de equipos móviles (IMEI), y bloquear el acceso del teléfono a la red móvil. Esto se denomina inclusión en la lista negra de IMEI[5].

Un ejemplo de la utilización de la base de datos mundial es el de la comunidad de operadores móviles, que comunican sus listas negras de IMEI a la base de datos mundial de IMEI de la GSM Association (GSMA), lo que permite a los operadores intercambiar datos y bloquear dispositivos en varias redes tanto a nivel nacional como internacional.

La base de datos de IMEI de la GSMA mantiene una lista negra mundial recopilada a partir de los datos facilitados por los operadores que contribuyen a aquélla. La GSMA puede entregar información de la lista negra 24 horas al día, siete días a la semana, a los operadores que se hayan conectado con la base de datos de IMEI para descargársela y utilizarla para bloquear dispositivos en sus propias redes. Los operadores participantes seleccionan una lista de operadores de la que extraen los datos de la lista negra y de esta forma se determina hasta qué punto funciona el intercambio de datos.

Como a veces el abonado que denuncia a su proveedor de servicios la pérdida de un dispositivo móvil no puede determinar si se le ha extraviado o se lo han robado, no suele distinguirse entre ambos estados. Si el propietario encuentra el dispositivo y lo comunica a su proveedor de servicios, éste podrá desbloquear el dispositivo y suprimir su IMEI de la base de datos de IMEI de la GSMA. A continuación la GSMA enviará a los operadores conectados que hubieran descargado el registro de la lista negra original instrucciones para que eliminen el IMEI de la lista negra.

Gracias a las características de esta base de datos mundial y al interés de las diferentes partes interesadas del mercado en evitar el robo de dispositivos, la GSMA ha desarrollado un sistema que permite verificar el estado de los IMEI. Éste se conoce como Verificación de dispositivo y permite intercambiar datos e información sobre el estado de un dispositivo con asociados autorizados, entre ellos minoristas, compañías de seguros, empresas de reciclaje y fuerzas y cuerpos de seguridad.

Este sistema permite que las partes interesadas averigüen si un dispositivo ha sido objeto de denuncia por robo o extravío, obtengan el registro histórico del dispositivo de varios años y consulten la información sobre el modelo del mismo y sus prestaciones. El conocimiento de las prestaciones presenta diversas ventajas: a) ayuda a los revendedores a identificar y eliminar los dispositivos robados antes de que lleguen a formar parte de la cadena de suministro; b) confirma el verdadero modelo del dispositivo como garantía de su autenticidad y facilita el cálculo de su valor; c) disuade del robo de dispositivos porque reduce el valor de los dispositivos robados; d) confirma quién fue el operador de la red que denunció el robo o pérdida del dispositivo, lo que facilita su devolución a su propietario legítimo.

Además de los operadores de red, hay muchas otras organizaciones en el ecosistema de dispositivos móviles que pueden utilizar este servicio de Verificación de dispositivos, entre ellos: a) las empresas de reciclaje de dispositivos, los minoristas y los distribuidores que pueden utilizar estos datos para reducir la probabilidad de que entren en su flujo de reciclaje o reventa, dispositivos que hayan sido objeto de denuncia por robo o extravío; b) compañías de seguros que recurran a esta

5 Véase [b-GSMA-IMEI-Blklst].

base de datos para reducir las reclamaciones de seguros por extravío o robo de dispositivos que sean falsas o exageradas; c) las fuerzas y cuerpos de seguridad, que pueden utilizarlos en las identificaciones y para facilitar la investigación y/o devolución de los artículos robados o extraviados[6].

Se puede facilitar el acceso a la base de datos mundial de IMEI para consultar un solo identificador a otras partes interesadas, entre ellas los consumidores, mediante ofertas de servicio de instancias autorizadas, tales como las autoridades del país, que pueden establecer portales en los idiomas locales desde donde se puedan realizar consultas de IMEI. El acceso para la inscripción de identificadores en la lista negra y/o su eliminación de ésta, sólo se permite actualmente a los operadores de red que puedan identificar sin ambigüedad y acreditar los datos del IMEI de sus clientes, manteniendo de este modo la integridad de la lista negra. Se está estudiando la ampliación del acceso a la lista negra a otras instancias tales como fabricantes de dispositivos, minoristas, etc. que puedan acreditar y responder de los IMEI que se pretenda acreditar.

Los sistemas de la GSMA antes enumerados (Base de datos de IMEI y Verificación de dispositivos en cuanto al estado de su IMEI) aportan a las partes interesadas una serie de ventajas adicionales frente a las de las bases de datos nacionales que terminan fragmentándose pero que pueden crearse como fruto de la labor bilateral o multilateral de intercambio y bloqueo de identificadores de dispositivos que hayan sido objeto de denuncia por extravío o robo. Estas ventajas pueden suponer: a) la reducción del tiempo de implementación y ajuste preciso; b) la disminución de los gastos de capital (CAPEX) y de los gastos operativos (OPEX); c) la simplificación de la complejidad y el aumento de la eficacia (al existir un punto de intercambio común en vez de varios orígenes y destinos), y d) la reducción del número de copias de la información. Estos elementos se basan en las siguientes características de los sistemas mencionados: a) modularidad; b) exención de tasas de conexión para los operadores/gobiernos, y c) madurez y estabilidad de la plataforma tecnológica de la base de datos de IMEI que funciona desde 1996.

6 Véase [b-GSMA-IMEI-DevChk].

Bibliografía

[b-UIT-T X-Sup.19] Recomendaciones UIT-T de la serie X – Suplemento 19 (2013), Suplemento sobre aspectos de seguridad de los teléfonos inteligentes.

[b-IMEI-SEC] GSMA (2016), *IMEI* Security *Design Principles. Enabling stolen mobile device blocking. V4.0.* <https://imeidb.gsma.com/imei/resources/documents/IMEI-Security-Technical-Design-Principles-v4.pdf>

[b-3GPP TS 122.016] ETSI TS 122 016 V3.1.0 (2000-01), *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); International Mobile station Equipment Identities (IMEI) (3G TS 22.016 version 3.1.0 Release 1999).*

[b-3GPP TS 23.003] ETSI TS 123 003 V10.5.0 (2012-04), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003 version 10.5.0 Release 10).*

[b-GSMA] GSM Association, Official Document SG.24 (2016), *Anti-Theft Device Feature Requirements v3.0.*

[b-GSMA-IMEI-Blklst] GSMA Services, *IMEI Blacklisting*. <https://www.gsma.com/services/gsma-imei/imei-blacklisting/> (consultado por última vez el 13 de abril de 2020)

[b-GSMA-IMEI-DevChk] GSMA Services, *Device Check*. <https://www.gsma.com/services/gsma-imei/about-device-check/> (consultado por última vez el 13 de abril de 2020)

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2020