Comisión de Regulación de Comunicaciones
REPÚBLICA DE COLOMBIA

Revisión de las condiciones y criterios para la identificación de equipos terminales móviles: Etapa de control

Documento Soporte

Relaciones de Gobierno y Asesoría

Mayo de 2016

CONTENIDO

1 INTRODUCCIÓN

La estrategia del Gobierno Nacional contra el grave flagelo del hurto de equipos terminales móviles, que inició en el año 2011 con la alianza entre la industria, el sector privado y el sector público, liderado desde la Presidencia de la Republica, y mediante la cual se consensaron el tipo de medidas y acciones que eran requeridas, ha ido construyéndose sobre un conjunto integral de medidas a cargo de múltiples sectores y entidades, y las cuales han contado con la participación de los actores involucrados y de la ciudadanía en general.

Es así como la estrategia se planteó en 3 ejes: reducir las vulnerabilidades del mercado, atacar la economía criminal y educar a la ciudadanía, los cuales se desarrollaron en 7 líneas de acción, como se aprecia en la tabla 1. En estos ejes han participado la Presidencia de la Republica, el Ministerio de TIC, la Comisión de Regulación de Comunicaciones, los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM), el Administrador de la Base de Datos a cargo de los PRSTM, el Ministerio de Comercio, Industria y Turismo, el Ministerio de Defensa, la Policía Nacional, a Fiscalía, la Dirección de Impuestos y Aduanas Nacionales, así como otros actores tales como comerciantes, asociaciones de comerciantes, e importadores. En la siguiente tabla se identifican las principales acciones sobre cada eje de la estrategia, en las cuales de manera específica la CRC participó en los ejes 2, 3 y 5 de manera directa.

Tabla 1. Estrategia contra el hurto de celulares 2011 - 2015

Fuente: Elaboración CRC

Así las cosas, dentro de la estrategia nacional contra el hurto de equipos terminales móviles (ETM) la CRC expidió la Resolución CRC 3128 de 2011, por la cual se define el modelo técnico, los aspectos

operativos y las reglas para la implementación, cargue y actualización de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles (ETM) reportados como hurtados o extraviados. Desde el año 2011 los PRSTM han venido adelantando todas las medidas tecnológicas que han sido dispuestas para el apoyo a esta estrategia nacional.

Luego de varios años de implementación y adopción de medidas, el enfoque de 2015 a 2018 establecido por la Presidencia de la Republica busca fortalecer y complementar el camino recorrido, y se dirige a tres ejes fundamentales: controlar el delito, control del mercado ilegal y la construcción de confianza, como se aprecia a continuación.

Tabla 2. Estrategia enfoque 2015-2018

Control del delito	1	Facilitar la denuncia
	2	Mejora en proceso de judicialización
	3	Despliegue conjunto Fiscalía y Policía
Control del mercado ilegal	4	Fortalecimiento y control de Bases de Datos
	5	Control a sitios ilegales de comercialización
	6	Mayor control de importaciones- exportaciones
Construcción de confianza	7	Devolución de celulares

Fuente Presidencia de la Republica.

Dado que, de acuerdo con las investigaciones adelantadas por la Policía Nacional, las bandas dedicadas al hurto de ETM proceden a la modificación o alteración del Identificador Internacional del Equipo Móvil (IMEI, por sus siglas en inglés) para eludir el bloqueo en las bases de datos negativas, recurriendo al uso de números de IMEI eventualmente ya asignados a otros equipos, así como de números de IMEI con estructura y formato erróneos[1], se tiene como consecuencia la reventa y reintroducción al mercado

[1] En relación con los estándares de la industria 3GPP TS 22.016 y TS 23.003 (equivalentes a los estándares ETSI TS 122.016 y ETSI TS 123.003)

de los equipos hurtados, los cuales pueden obtener servicio en las redes móviles dado que el IMEI bloqueado fue modificando evadiendo el control de la base de dato negativa.

De otra parte, en las redes de los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) se usan equipos cuya marca y modelo no han sido homologados ante la CRC para su uso en las redes móviles del país, de conformidad con lo establecido en la Resolución CRC 4507 de 2014 y anteriores, así como también de equipos que no se registran en las bases de datos positivas, como está establecido en la Resolución CRC 3128 de 2011.

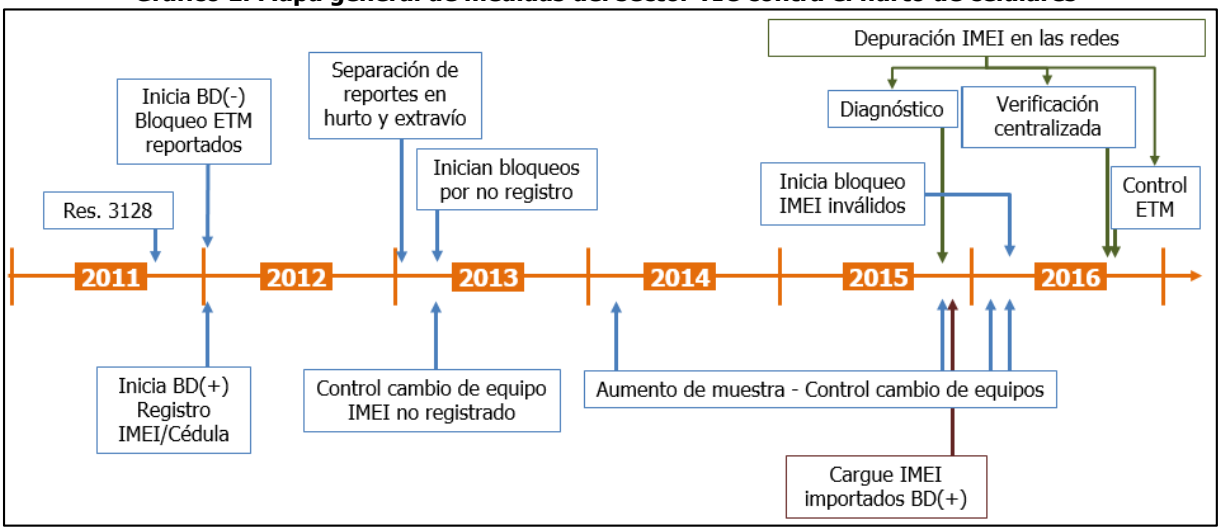
En este punto es de mencionar que de conformidad con el artículo 4, el literal h del numeral 10.2 del artículo 10, y el artículo 105 de la Resolución CRC 3066 de 2011, la cual contiene el Régimen Integral de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, si bien el usuario puede utilizar para la prestación de los servicios de comunicaciones móviles el equipo terminal de su elección, este debe encontrarse debidamente homologado y es necesario que durante su compra, el usuario se cerciore de adquirirlo en un lugar autorizado para la venta de equipos terminales móviles, de acuerdo con el listado que para el efecto publique el Ministerio de Tecnologías de la Información y las Comunicaciones en su página Web.

Así mismo, la norma en mención dispone que los proveedores de redes y servicios de comunicaciones sólo podrán exigir como condición para la activación de los equipos terminales en sus redes que dichos equipos se encuentren homologados, cuando la homologación sea obligatoria.

El sector TIC representado por el Ministerio de TIC, la CRC y los PRSTM han desarrollado el conjunto de medidas tecnológicas que requiere el control del problema. Respecto del fortalecimiento y control, las actividades se han enfocado en depurar las bases de datos y controlar la actividad de los equipos en las redes a fin de cerrar el paso a los equipos hurtados que se reintroducen al mercado por la alteración de sus sistemas de identificación. Como parte del fortalecimiento de las medidas asociadas a las bases de datos negativas y positivas, de que trata el artículo 106 de la Ley 1453 de 2011, la CRC se ha venido desarrollando las siguientes acciones frente a la necesidad de detectar y controlar el uso de ETM:

- Medidas de control aplicables a aquellos equipos que hacen cambio de SIM y no se encuentran registrados en la BDA Positiva.
- Medidas de control destinadas a equipos con IMEI inválido y que no se encuentran registrados en la BDA Positiva.
- Medidas para depuración de IMEI en las redes.

Gráfico 1. Mapa general de medidas del sector TIC contra el hurto de celulares



Fuente: Elaboración CRC

Frente a las medidas para depuración de IMEI en las redes, se incluye la implementación y puesta en operación de un proceso de verificación y control de IMEI sin formato, inválidos, duplicados, no homologados y no registrados en la base de datos positiva, a través de la realización de 3 etapas:

- La primera etapa consiste en una validación y diagnóstico preliminar, en la cual los PRSTM envían a la CRC parte de los campos de los CDR[2] de voz y datos generados en sus redes desde noviembre de 2015 y hasta abril de 2016, para que con base en su análisis y seguimiento se identifique la cantidad de IMEI inválidos, potencialmente duplicados, no homologados y no registrados en la base de datos positiva[3].
- La segunda etapa corresponde a la de verificación, modificada mediante la Resolución CRC 4937 de 2016, en la que se deben detectar de manera diaria todos los IMEI sin formato, los inválidos, los duplicados, los no homologados, y los no registrados en la BDA Positiva, con actividad en las redes móviles del país. Dicho proceso será desarrollado a través de un sistema implementado mediante 2 ciclos: uno intra red, ejecutado de manera individual por cada PRSTM, y otro inter red, implementado de manera centralizada a cargo de todos los PRSTM de manera conjunta, en el cual se realiza la recepción, procesamiento y análisis de información de los CDR de todos los PRSTM en cuanto a equipos con IMEI duplicado.
- La tercera etapa corresponde a la de control, consistente en las actividades que deberán ser ejecutadas por los PRSTM, a efectos de realizar la depuración de los equipos terminales móviles

[2] CDR (Charging Data Records): Formato de recolección de información acerca de eventos, tales como tiempo de establecimiento de una llamada, duración de la llamada, cantidad de datos transferidos, identificación del abonado llamante, etc.
[3] Los resultados iniciales de esta etapa se presentan en el numeral **¡Error! No se encuentra el origen de la referencia.** el presente documento.

que como resultado de la etapa de verificación sean detectados con IMEI sin formato, inválidos, duplicados, no homologados y no registrados en la base de datos positiva.

Teniendo en cuenta que la etapa de control entra en operación a partir del 1° de agosto de 2016, resulta necesario realizar la definición de las actividades que deberán ser ejecutadas por los PRSTM a efectos de realizar la depuración de los IMEI que se identifiquen en la etapa de verificación, con el fin de proceder a depurar las bases de datos.

Es así como este documento aborda en el segundo capítulo la revisión del contexto internacional en cuento al control de equipos terminales móviles falsificados, sub-estándar y no homologados. Posteriormente, en el segundo capítulo se muestran los resultados iniciales del proceso de validación y diagnóstico de equipos terminales móviles. Luego, en el cuarto capítulo se describe la propuesta sobre medidas a desarrollar en la etapa de control por parte de los PRSTM. Finalmente, en el quinto capítulo se presentan otras propuestas de modificación de la Resolución CRC 3128 de 2011, las cuales han sido identificadas por la CRC en el marco de desarrollo del presente proyecto regulatorio.

2 CONTEXTO INTERNACIONAL

Dado el creciente problema a nivel mundial de la proliferación de equipos terminales móviles falsificados, sub-estándar y no homologados, dentro de los cuales se incluyen aquellos que son alterados en su mecanismo de identificación para reintroducir equipos hurtados al mercado, la comunidad internacional ha tomado un conjunto de iniciativas a nivel regional y mundial, para buscar soluciones de control, las cuales se relacionan en la tabla 1.

Tabla 3. Iniciativas regionales y mundiales para combatiré equipos TIC falsificados, sub-estándar y no homologados.

Organización	Actividades relacionadas
COMISION INTERAMERICANA DE TELECOMUNICACIONES CITEL	Grupo de correspondencia para combatir terminales falsificados, sub-estándar y no homologados.
	Relatoría en control de fraude, practicas antirreglamentarias en telecomunicaciones y medidas regionales contra hurto de equipos terminales móviles.
	Creación de la carpeta Técnica sobre equipos falsificados y vínculo con estudios en UIT
	Resolución 222-2014: Desarrollar definiciones, evaluar alcance, compartir información y mejores practicas
	Decisión sep. 2015: Proponer texto base para el reporte técnico de dispositivos falsificados, discutir cómo trabajar junto con UIT.
UNION INTERNACIONAL DE TELECOMUNICACIONES UIT	Creación del grupo de estudio ITU-T SG11, Question 8.
	Resolución 188: Reconoce problema global creciente. Instruye afrontar el tema compartiendo información a nivel regional y global. Emite el Reporte Técnico Equipos Falsificados en 6 idiomas. Realiza el Evento: Combate a Equipos Falsificados.
	Reunión Ginebra, Diciembre 2015: Borrador para emitir Recomendación UIT: Marco para solución en el combato de equipos TIC falsificados, borrador de reporte técnico con las guías, mejores prácticas y soluciones. Borrador de reporte técnico sobre metodologías y casos de uso en el combate a equipos TIC falsificados. Más de 20 países y entidades participan en la elaboración de las recomendaciones.
COMISION DE TELECOMUNICACIONES DE CENTRO AMERICA COMTELCA	Taller Control de equipos falsificados, abril 2015.

Fuente: CITEL, UIT, COMTELCA.

Con el fin de ilustrar al sector y público interesado, esta Comisión considera útil incluir en el presente documento soporte la información relacionada con las prácticas y sistemas de control de equipos terminales móviles, basada en estudios realizados en los grupos de trabajo de la Comisión

Interamericana de Telecomunicaciones CITEL[4] y de la Unión Internacional de Telecomunicaciones UIT[5] sobre los equipos falsificados, sub-estándar, no homologados y los alterados/clonados, éstos últimos debido a que en varios países se integra dicho control. Colombia a través de la CRC ha participado en foros de discusión presenciales y virtuales en donde ha tenido la oportunidad de compartir experiencias y conocer el desarrollo de las cuestiones que en torno a esta problemática evolucionan a nivel internacional.

Como resultado de dichos estudios, la UIT-T publicó en noviembre de 2014 el "Informe Técnico – Equipos TIC falsificados"[6] que recopila aspectos relacionados con la definición de la problemática, sus impactos en los mercados, lo usuarios, las redes de telecomunicaciones y pérdidas financieras, así como las experiencias y mejores prácticas a nivel mundial[7].

A partir del Informe Técnico de la UIT-T, se encuentra en discusión una recomendación de la UIT[8] sobre el modelo marco de solución para combatir la falsificación de dispositivos TIC.[9]

Los estudios a la fecha han identificado algunos retos, así como similitudes entre los diferentes mecanismos de control que han adoptado los países, que se sustentan en el manejo de un identificador único de los dispositivos, que para el caso de los ETM es el IMEI, así como el uso de procedimientos y medios tecnológicos para su bloqueo.

Dado que las soluciones actuales que se están desplegando para impedir el uso de equipos falsificados también están en la capacidad de identificar dispositivos alterados/clonados, estos están siendo incluidos en el alcance del modelo marco de control bajo estudio en el borrador de recomendación de la UIT.

Otro elemento fundamental que se integra a un modelo de control como punto de partida es el proceso interno que un país desarrolle en virtud de la homologación de equipos terminales móviles, y en otros casos procesos de evaluación de conformidad, que propenden por autorizar, para el uso en las redes y mercados, los dispositivos que sean compatibles con los estándares y normas nacionales o internacionales para evitar riesgos relacionados con la salud de los usuarios y las potenciales afectaciones a los servicios y redes de telecomunicaciones.

---

[4] Grupo de Trabajo sobre Políticas y Regulación (GTPR), Relatoría sobre Control de Fraude, Prácticas Antirreglamentarias en Telecomunicaciones y medidas regionales contra el hurto de equipos terminales móviles.
[5] Grupo de Trabajo UIT-T Question 8/11.
[6] http://www.itu.int/pub/T-TUT-CCICT-2014
[7] Brasil, Ecuador, Colombia, Emiratos Árabes Unidos, Turquía, Indonesia, Egipto, Kenya, Azerbaiyán, Sri Lanka, Uganda, Ucrania.
[8] Grupo de estudio ITU-T Question 8/11.
[9] En el marco de las discusiones, se estudia la siguiente propuesta de definición respecto de un dispositivo falsificado[9] "*un producto que infringe de forma explícita las marcas, que copia los diseños de hardware o software, marcas o derechos de empaque de un producto original o auténtico. En general, también infringe los estándares técnicos aplicables nacionales y/o internacionales, los requisitos regulatorios o procesos de conformidad, los acuerdos de licencias de fabricación, u otros requisitos legales aplicables*".

2.1 Retos del modelo de control

En los grupos de estudio internacional se han identificado, entre otros, los siguientes retos:

1. Construir bases de datos fiables de identificadores de dispositivos.
   a. Se necesita de identificadores únicos y confiables (seguros)
   b. Preferible usar bases de datos de referencia[10] internacionales sumadas a las bases de datos nacionales.

2. Sistemas de identificación y verificación de identificadores para distinguir equipos genuinos y falsificados/alterados.
   a. En procesos complejos como los de importación al territorio nacional.
   b. En las acciones de las autoridades de policía una vez el producto está en el mercado.
   c. En las acciones de control en los proveedores de servicios para identificar equipos en sus redes.

3. Identificación y definición de las acciones para cada escenario.
   a. ¿Qué atacar primero?
   b. ¿Cómo afrontar los terminales clonados?

4. Acciones solo sobre los terminales que ya están en uso en las redes.
   a. ¿Cómo controlar la entrada de nuevos dispositivos falsificados o irregulares?

5. Cómo detener el uso de los equipos falsificados/alterados?
   a. Cómo distinguir entre equipos genuinos y falsificados/alterados?
   b. Cómo bloquear el IMEI de equipos clonados sin afectar el usuario del equipo legítimo?.

6. Cómo detener el ingreso al país (importación/contrabando), venta y circulación de nuevos equipos falsificados?.

7. Cómo reducir el impacto en los usuarios que ya tienen equipos falsificados/alterados en uso?
   a. Educación
   b. Aviso previo a las medidas de bloqueo
   c. Herramientas de consulta para verificación de equipos

Respecto del modelo de gestión adoptado en Colombia los retos se están afrontando de acuerdo a la siguiente descripción, y cuyas acciones obedecen a la estrategia frontal del Gobierno Nacional:

[10] Un ejemplo es la base de datos de TAC (Type Allocation Code) o código de asignación a fabricantes, la cual se administra por la Asociación de operadores GSM -GSMA-, bajo un procedimiento que es estándar en la industria a fin de asignar identificadores únicos e irrepetibles a los fabricantes, para que en cumplimiento de los estándares ETSI TS 122.016 y ETSI TS 123.003 identifiquen de manera univoca cada equipo terminal móvil que producen.

1. Bases de datos confiables:
    a. Bases de datos positivas y negativas basadas en control del IMEI como identificador internacional único. La BDA positiva no admite un mismo IMEI relacionado a más de un documento de identidad.
    b. Base de Datos de referencia para la unicidad del IMEI. Se hace uso de la base de datos de TAC y listas negativas de la GSMA.

2. Sistemas de identificación y verificación de identificadores para distinguir equipos genuinos.
    a. La BDA negativa es punto de referencia para las autoridades de policía y aduanas.
    b. BDA negativa y consulta BD GSMA para los controles de los operadores móviles sobre sus redes.

3. Identificación de escenarios a atacar:
    a. Se ha iniciado con equipos cuyo IMEI es inválido.
    b. Se gestionan equipos no registrados en bases de datos positivas.
    c. Se continuará con duplicados, no homologados, no registrados.

4. Acciones sobre terminales ya en uso.
    a. Las medidas han atendido el derecho del usaurio y plantea respecto de su registro, aviso previo y oportunidad de registro.
    b. Se controlan IMEI con actividad en las redes móviles.

5. Cómo detener el uso de equipos alterados?
    a. La estrategia de control busca soluciones teécnicas y operativas para identificar y controlar equipos no registrados, inválidos, no homologados y duplicados.

6. Cómo detener el ingreso al país de equipos alterados/falsificados y su comercialización?
    a. El Decreto 2025 busca restringir el ingreso de equipos mediante la validación previa de identificadores en bases de datos, y la prohibición de exportación de usados.
    b. Existe un esquema de autorización de comercializadores de equipos terminales a nivel nacional.

7. Cómo reducir el impacto a los usuarios?.
    a. Los PRSTM siempre dan aviso previo a las medidas de bloqueo y la razón que lo originó.
    b. Tanto comercializadores como usuarios pueden utilizar información en la web para consulta y verificación previa de equipos.
    c. Divulgación de sitios legales para adquisición de equipos.

2.2 Requisitos del modelo de control.

En los estudios adelantados en la UIT[11] se han incluido las condiciones mínimas que debiera tener un sistema que permita un control integral de terminales, el cual debería incluir:

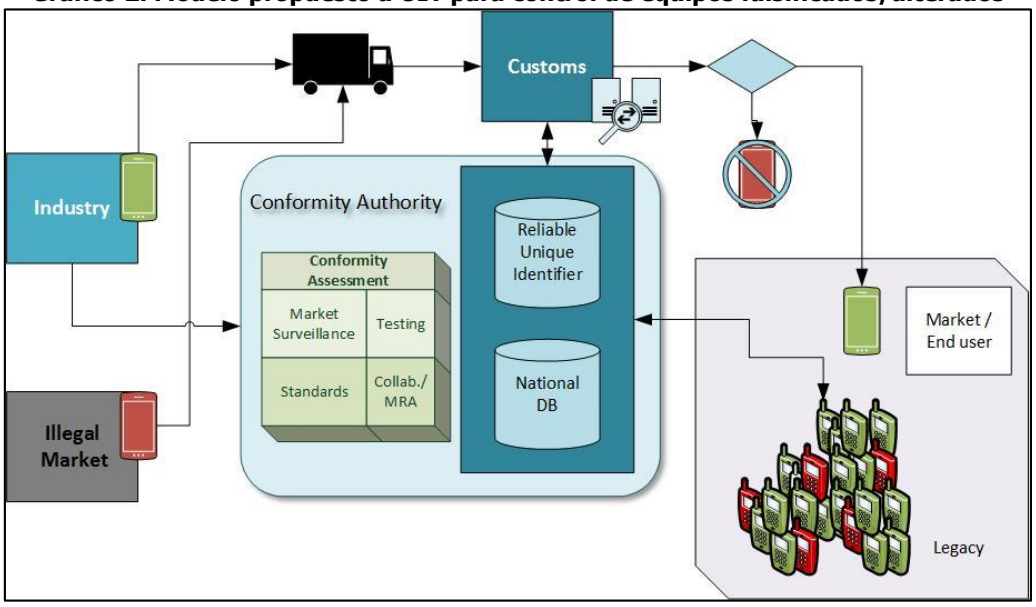
1. Identificadores únicos confiables con posibilidad de referencia en un proceso formal de asignación.
2. Proceso de evaluación de conformidad u homologación con posibilidad de consulta para verificación de usuarios, industria, proveedores de servicio.
3. Cooperación de autoridades aduaneras y entrega de herramientas y conocimientos sobre procesos de identificación y conformidad de equipos.
4. Consultas con la industria sobre alternativas y medidas a adoptar.
5. Empoderar a usuarios con información que permita conocer la condición de sus equipos.
6. Reducir el impacto a usuarios y redes de telecomunicaciones, con políticas de notificación previa, de exención de controles y de transición para equipos que ya estaban en el mercado.
7. Soporte con medidas legales y regulatorios respecto de importación, venta, circulación de equipos y medidas y acciones contra responsables de falsificación/alteración.
8. Exención regulatoria para productos que ya están en uso en el mercado.
9. Acciones de autoridades de policía y de control para el cumplimiento de procesos relacionados con falsificación, alteración, tráfico, etc., que se soporten en el marco legal y normativo.

2.3 Enfoque integral de solución[12]

Los grupos de estudio conjugaron las diferentes experiencias y medidas tomadas en diferentes países para proponer incluir en la recomendación UIT un modelo de control para afrontar la producción, circulación y uso de dispositivos falsificados/alterados/clonados, que se aprecia en el Gráfico 2.

[11] Grupo de Estudio 11 de la UIT-T, cuestión 8. Grupo de correspondencia de CITEL sobre equipos falsificados, alterados, subestandar y no homologados.
[12] Tomado del taller "WSC Workshop on Conformity Assessment". UIT, Ginebra, diciembre de 2015. Presentation "Combat of Counterfit ICT Devices, Conformity as a Tool. Joao Alexandre Zanon, Specialist ANATEL Brasil. http://www.wsccaworkshop.com/documents/

Gráfico 2. Modelo propuesto a UIT para control de equipos falsificados/alterados



Fuente: "Combat of Counterfeit ICT Devices, Conformity as a Tool", UIT WSC Workshop on Conformity Assessment. Ginebra, diciembre 2015.

Los elementos clave en el modelo propuesto son:

- Control a equipos terminales móviles que no están homologados por el regulador.
- Bloqueo a la importación ilegal de equipos falsificados.
- Creación de un registro de cada equipo terminal móvil para bloquear el uso de falsificados, basado en el registro de IMEI como identificador único y partiendo de los equipos legalmente importados.
- Empleo de "listas blancas" (equipos legalmente importados o fabricados en el país), "listas grises" (estado no confirmado, no están en "lista blanca" ni en "lista negra") y listas negras" (el servicio debe ser negado). Uso de sistema estándar de listas conocido como EIR (Registro de Identificadores de Equipos).
- Deshabilitar el uso de identificadores inválidos y no genuinos.
- Esquemas seguros de consulta sobre los registros y listas, según la necesidad y propósito de cada grupo objetivo.

Con un modelo como el representado gráficamente se aspira a:

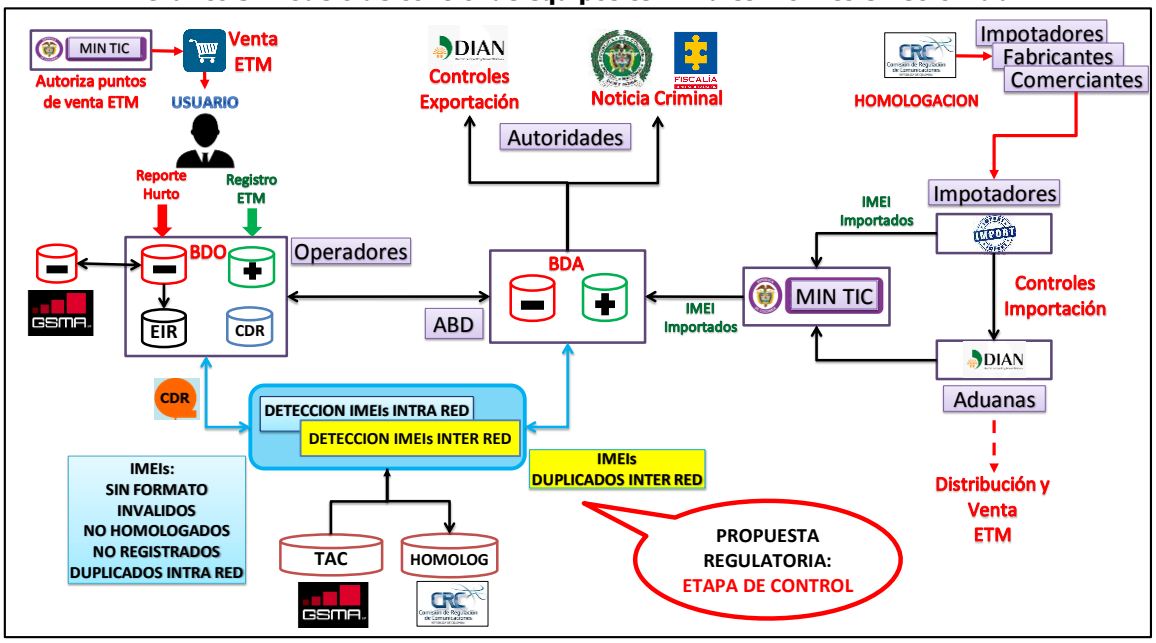
- Acciones y cooperación multinivel, bilateral y regional. Reunir las mejores prácticas internacionales y recomendaciones.
- Reducir el impacto al usuario final (usuarios de buena fe). Crucial una buena comunicación, exoneración de terminales ya en uso, pero con un tiempo para su recambio.

- Acciones integrales para combatir el problema. Política de homologación/certificación con integración de autoridades aduaneras.
- Soluciones para retirar/deshabilitar equipos falsificados/alterados del mercado.
- Bases de datos confiables de referencia para las soluciones basadas en el identificador del equipo. Identificador único seguro.

En este punto es importante señalar que gran parte de los criterios, métodos y requisitos que recopilan los estudios antes referidos, han sido adoptados en Colombia y que, de hecho, la presente propuesta regulatoria forma parte de una de las etapas de su implementación. Por lo anterior, las medidas que se están tomando por parte del Gobierno Nacional no son únicas, inexistentes o imposibles de accionar, toda vez que el esfuerzo de la comunidad internacional por estudiar y recomendar su uso y adopción proviene precisamente de experiencias y medidas que ya han sido puestas en operación en otros países y sirven de guía para los demás.

Para ilustrar lo anterior, en el Gráfico 3 se aprecia el modelo de control para Colombia que viene en construcción desde el año 2011 dentro de la estrategia de medidas integrales contra el hurto de equipos terminales móviles.

Gráfico 3. Modelo de control de equipos terminales móviles en Colombia



Fuente: Elaboración CRC

3 PROPUESTA ETAPA DE CONTROL

En primer lugar, resulta importante resaltar que el IMEI es un número que permite identificar un terminal móvil individual en una red GSM, UMTS o LTE. Este número permite a los operadores realizar las siguientes tareas:

- Habilitar la carga remota de parches y adaptaciones para evitar problemas de interoperabilidad del dispositivo.
- Gestionar la configuración de soporte y actualización remota de la base de equipos que utilizan sus usuarios.
- Apoyar estrategias de mercadeo y ventas permitiendo a los operadores identificar dispositivos específicos que pueden soportar los servicios de valor agregado.
- Determinar qué dispositivos son responsables por fallas técnicas en la red y permitir la toma de medidas correctivas.
- Detectar el fraude en una etapa temprana.
- Evitar que un teléfono robado tenga acceso a la red y sea utilizado.

Así mismo, los IMEI pueden ser usados por los fabricantes de dispositivos para:

- Probar la autenticidad de dispositivos por parte de agencias de aduanas en algunos países (ejemplo, Turquía, India)
- Facilitar la identificación del mercado gris de aparatos.
- Tomar acciones correctivas contra dispositivos que son robados de los sitios de fabricación, sitios de almacenamiento o mientras están en tránsito.
- Asignar IMEIs de prueba para la verificación de prototipos en redes reales, previo al lanzamiento al mercado.
- Permite a los operadores identificar dispositivos que pueden requerir actualizaciones de software.

Todo lo anterior se basa en el hecho que todo equipo terminal móvil debe tener un IMEI asignado, y éste debe ser un número único que permita identificar a cada equipo terminal móvil de manera individual en una red pública móvil terrestre, ya que dicho mecanismo de identificación es el principal medio para poder determinar cuáles son los equipos que cursan tráfico en la red de un operador, y está conformado por un TAC y un número serial.

Adicionalmente, en relación con el TAC, la Recomendación ETSI TS 123 003, indica que existe un procedimiento de asignación del código TAC con el fin que los fabricantes asignen de manera única un IMEI (TAC+SNR) a cada equipo móvil que producen, y es así como desde el año 2002 los actores de la industria solicitaron a la GSMA, asumir la responsabilidad de la asignación de los rangos de números IMEI y códigos TAC a los fabricantes de dispositivos móviles, para garantizar que dicho mecanismo de identificación sea único para cada equipo y que el TAC sea único para cada marca y modelo producido por los diferentes fabricantes.

En ese sentido, a través de la propuesta regulatoria presentada para comentarios del sector, se definen las medidas de control de los IMEI identificados en la etapa de verificación de equipos terminales móviles:

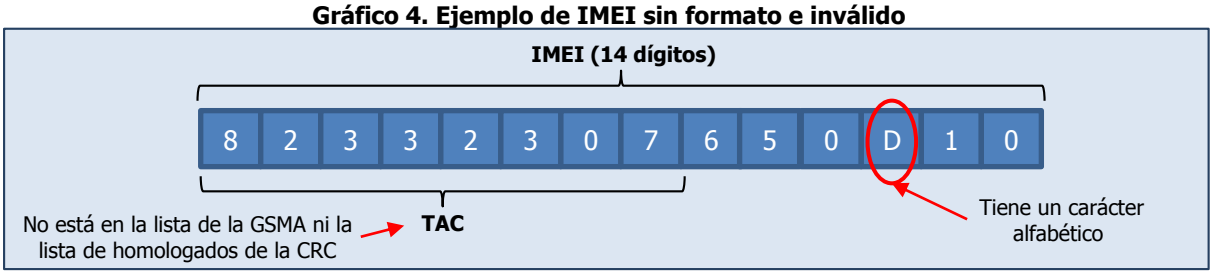
- IMEI sin formato: Los equipos no cumplen con los estándares de la industria, es decir poseen una longitud diferente o utilizan caracteres alfanuméricos; y adicionalmente pueden corresponder a equipos cuyo IMEI original ha sido alterado.
- Inválidos: De acuerdo con la definición establecida por la CRC, se entiende como aquellos que no poseen TAC asignado por la GSMA ni fueron previamente homologados por la CRC (antes de la Res. 4868 de 2016).
- No homologados: Pueden ser equipos lícitos con TAC asignado por la GSMA, pero no han sido homologados ante la CRC, o equipos cuyo IMEI ha sido alterado con un TAC asignado por la GSMA.
- Duplicados: equipos que no tiene un IMEI único en las redes, lo que va en contra de la finalidad del IMEI.
- No registrados en la BDA positiva.

Teniendo en cuenta lo anterior, en el presente capítulo se desarrolla las medidas propuesta para discusión con el sector relacionadas con la etapa de control de equipos terminales móviles, abarcando en primera instancia lo relacionado con la priorización de las medidas, en segundo término las medidas como tal, y por último, las consideraciones a tener en cuenta para el retiro de IMEI de la BDA Negativa de los nuevo tipos de reportes que se van a incluir a partir del 1° de agosto.

3.1 Priorización de las medidas de la etapa de control

Cuando se realiza la detección de un IMEI con actividad en la red de los PRSTM, este puede ser clasificado en una o más de las categorías definidas en la etapa de verificación de equipos terminales móviles: sin formato, inválido, no homologado, duplicado y no registrado en la BDA positiva. Es decir, por ejemplo, que un IMEI puede ser clasificado al mismo tiempo como sin formato[13] y como inválido[14]. Sin embargo, el control de IMEI sin formato a aplicar, en principio, debe ser más estricto que el control de IMEI inválidos (Ver Gráfico 4). En este sentido, a los IMEI sin formato se les debe aplicar únicamente el control asociado a este tipo.

Gráfico 4. Ejemplo de IMEI sin formato e inválido



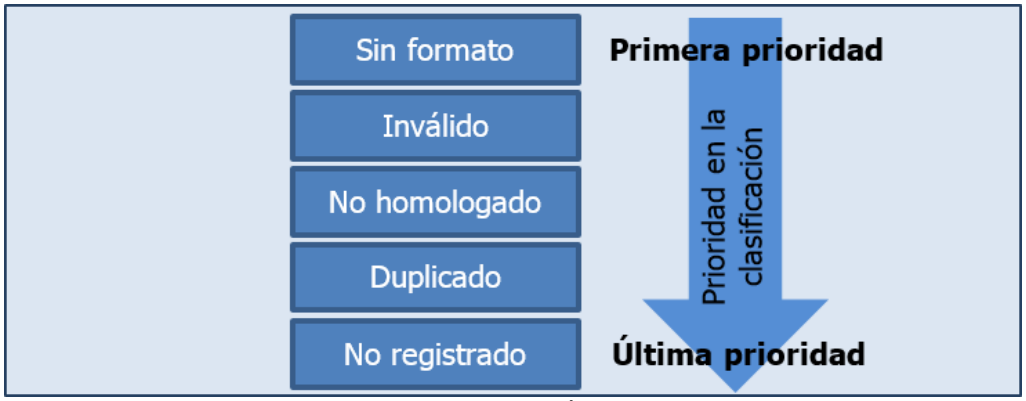
[13] Su longitud es menor a 14 dígitos o contiene caracteres alfabéticos
[14] TAC no presente en la base de datos de la GSMA ni en la lista de TAC homologados de la CRC

Fuente: Elaboración CRC

Así mismo, pueden ser detectados IMEI inválidos como duplicados al mismo tiempo, caso en el cual debería primar la condición de invalidez para aplicar medidas de control.

Teniendo en cuenta lo anterior, se propone el siguiente nivel de prioridad en la aplicación de los diferentes tipos de control.

Gráfico 5. Prioridad en la clasificación de los IMEI

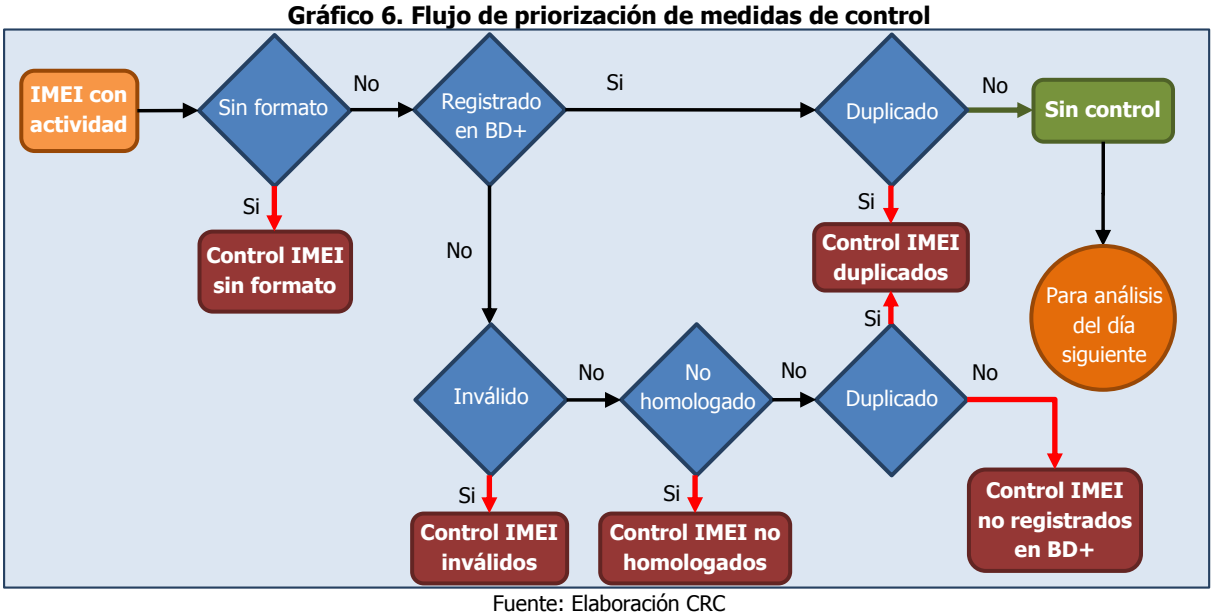


Fuente: Elaboración CRC

Por otra parte, es importante tener en cuenta que existen IMEI inválidos e IMEI no homologados que se encuentran actualmente registrados en la BDA positiva, a los cuales no se les aplicará control de inválidos ni de no homologados posterior, debido a que cumplieron oportunamente con el requerimiento de registro realizado. Por lo tanto, este tipo de IMEI deben ser excluidos de estos controles.

En el siguiente gráfico se muestra el desarrollo de una primera aproximación de la priorización en la aplicación de las medidas de control, en el cual se observa que a los IMEI registrados en la BDA positiva, únicamente se les realiza la verificación de duplicidad, mientras que a los no registrados se le aplican todas las verificaciones, siguiendo la prioridad de clasificación descrita anteriormente.

Gráfico 6. Flujo de priorización de medidas de control

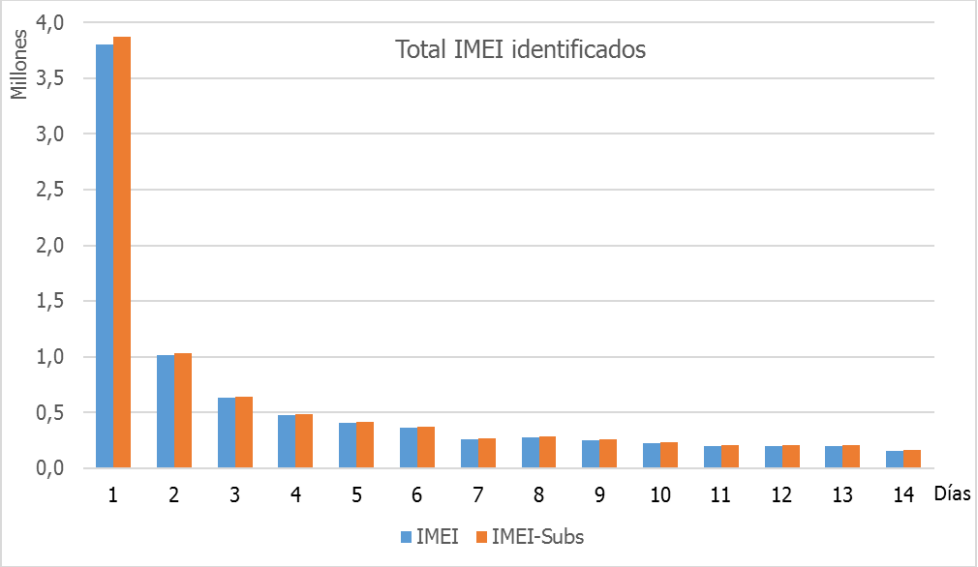


Fuente: Elaboración CRC

Finalmente, se debe tener en cuenta que este ciclo debe repetirse a partir de la actividad diaria de equipos en la red. Sin embargo, los IMEI que sean detectados en un día en las categorías de sin formato, inválidos, no homologados, duplicados y no registrados en la BDA positiva, no deben ser clasificados en días posteriores, pues ya estarán sometidos a los respectivos controles. Sin embargo, los IMEI a los que no se les aplica ningún tipo de control, deberán reingresar al proceso de detección de duplicados en días posteriores, siempre que presenten actividad en las redes en esos días.

Con base en este flujo de priorización, se procedió a realizar una simulación del mismo, utilizando para ello los CDR de voz de reportados por los PRSTM para 14 días consecutivos del mes de febrero de 2016. Los resultados se pueden observar a continuación.

Gráfico 7. Escenario de simulación para el mecanismo de priorización de las medidas de la etapa de control



Fuente: Elaboración CRC con base en información de los PRSTM

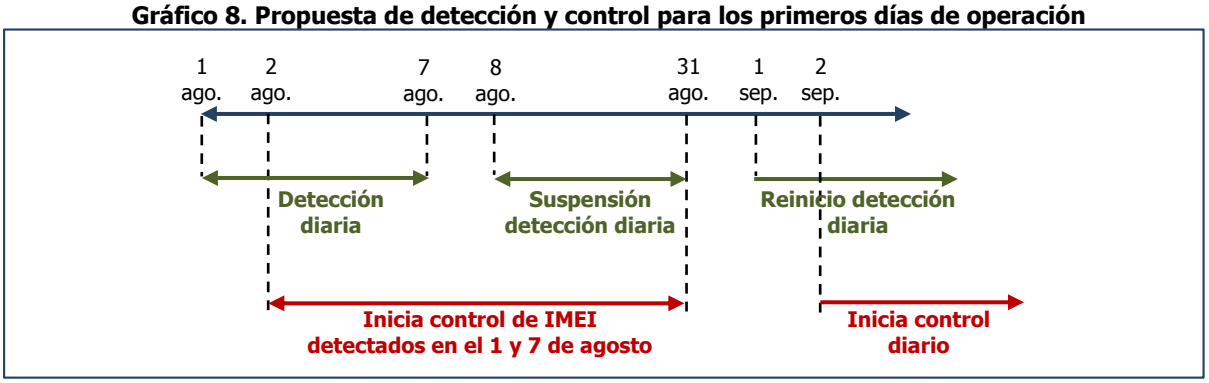
Con base en la anterior simulación, en el día 1 se identificaron 3,87 millones de parejas IMEI-IMSI con IMEI sin formato, inválido, no homologado, duplicado y no registrado en la BDA positiva, a las cuales se les deberían aplicar las medidas de control. Esta cifra hace inviable iniciar con la ejecución de las medidas en control en el día 2, por la cantidad de usuarios que deberían ser contactados. A partir de lo anterior, se propone modificar los primeros días de detección y control de ETM, así:

- Identificación de IMEI
  - Detección diaria de IMEI entre el 1 y 7 de agosto de 2016.
  - Suspensión de la detección diaria de IMEI entre el 8 y el 31 de agosto de 2016.
  - Reinicio de la detección diaria de ETM, a partir del 1 de septiembre de 2016.

- Control de IMEI
  - Control de IMEI detectados entre el 2 y 31 de agosto de 2016, para los IMEI identificados entre el 1 y 7 de agosto de 2016.
  - Control diario de IMEI, a partir del 2 de septiembre de 2016 con los IMEI identificados el día anterior.

Lo anterior, puede observarse de manera ilustrativa en el Gráfico 8.

Gráfico 8. Propuesta de detección y control para los primeros días de operación



Fuente: Elaboración CRC

3.2 Acciones a desarrollar para cada tipología de IMEI

A continuación, se describen las diferentes medidas de control propuestas para cada tipo de IMEI, identificando las opciones que están disponibles a nivel técnico y operativo.

3.2.1 IMEI sin formato

En la especificación técnica 3GPP TS 23.003 se definen dos versiones de IMEI. En la primera de ellas se describe un IMEI conformado por 14 dígitos más un digito adicional de verificación o Check Digit (CD) y en la segunda conocida como IMEISV se describe el IMEI en términos de los mismos 14 dígitos más 2 dígitos adicionales correspondientes al Software Version Number (SVN).

Los 14 dígitos que conforman la estructura raíz del IMEI (comunes en ambas versiones) corresponden a la identificación física del equipo y constan de 8 dígitos relacionados con la marca, el modelo y lote del equipo, descritos mediante el Type Allocation Code (TAC) y los 6 dígitos restantes están relacionados con el número serial del equipo (Serial Number o SN) en el marco del TAC asignado.

Por otra parte se resalta que la especificación técnica que define el formato base del IMEI desde su versión inicial hasta la última versión vigente a la fecha de realizar el presente documento (3GPP TS 23.003 V13.5.0 (2016-03)), ha indicado que los dígitos que componen el IMEI son "dígitos decimales", es decir que sólo pueden tomar valores entre 0 y 9 y adicionalmente se indica que para efectos de validación por parte de la red sólo son transmitidos 14 dígitos (que naturalmente corresponden al TAC y SNR).

En relación con los dígitos decimales que componen el IMEI y dado que la implementación en hardware de estos se codifica mediante BCD (Binary Coded Decimal), el cual es un código de 4 bits, es posible que fabricantes que no cumplan con la especificación técnica o fruto de procesos de adulteración del IMEI, permitan o se presenten casos en los cuales se programen otros dígitos por fuera de las 10 combinaciones que usa el código BCD para dígitos decimales (combinaciones desde 0000 para el digito

"0" hasta 1001 para el digito "9") de manera tal que se presenten combinaciones adicionales, no decimales, soportadas por los 4 bits con los cuales se codifican los dígitos (combinaciones desde 1010 para el dígito hexadecimal "A" hasta 1111 para el dígito hexadecimal "F").

De acuerdo con lo anteriormente expresado, eventuales IMEI que sean enviados por ETM en el proceso de registro en la red y que cuenten con una cantidad de dígitos diferente a 14 o utilicen dígitos no decimales (de la "A" a la "F") representan una clara violación a la especificación técnica y son de facto equipos que por una parte no cumplirían ningún proceso de homologación riguroso (por no cumplimiento de la especificación técnica 3GPP TS 23.003) y por otra parte son claramente equipos que pueden haber llegado a esa condición por la ejecución de procesos de adulteración del IMEI.

En este sentido, y no sólo en el marco de la estrategia contra el hurto de celulares, sino también en el marco mismo del cumplimiento de las condiciones técnicas para acceder al servicio, a tales equipos no se les debe permitir el registro en la red, considerando que detrás de la violación de la respectiva especificación técnica para programar el IMEI, no solo puede estar detrás la presunta comisión del delito de adulteración de IMEI, sino que también puede estar presente violación de otras especificaciones técnicas más complejas como como por ejemplo las relativas al establecimiento de llamadas o al control de potencia.

Con base en la información de CDR enviada por los PRSTM durante la etapa de validación y diagnóstico preliminar definida en la Resolución CRC 4813 de 2015, los análisis realizados por la CRC en cuanto a los IMEI sin formato evidenciaron que fueron vistos con actividad en las redes de los PRSTM 3.733 IMEI con al menos un carácter alfabético y 258 con menos de 14 dígitos, cifras que muestran un comportamiento similar para los meses analizados[15].

El control de tales equipos denominados como "IMEI sin formato" se debe realizar preferencialmente en un esquema "ex ante" es decir en el momento mismo del intento de registro en la red o en su defecto y de manera alterna, en un esquema "ex post", es decir mediante el bloqueo IMEI por IMEI una vez se tiene registro de que los equipos con "IMEI sin formato" han utilizado la red, como se ha evidenciado en la información remitida por los PRSTM en la etapa de validación inicial.

De acuerdo con las consultas realizadas por la CRC, las versiones de software de los EIR actualmente en servicio no implementan reglas de validación de formato y por otra parte sólo soportan la programación de 14 dígitos y "no todos" soportan a hoy la programación de dígitos no decimales, por lo que es pertinente dar un plazo a los PRSTM para que implementen un mecanismo para evitar el registro en la red equipos con "IMEI sin formato" o en su defecto su bloqueo.

De acuerdo con lo anterior se presentan 2 opciones de las cuales cada PRSTM podrá optar por una a más tardar el 1º de febrero de 2017:

[15] Noviembre de 2015 a febrero de 2016

- Mecanismo preferente (ex-ante): Se debe evitar el registro en la red para equipos con "IMEI sin formato". Este mecanismo considera que un equipo sin formato entre otros aspectos no cumple con las especificaciones técnicas del 3GPP y por lo tanto no se le debe permitir su registro en la red. Debido a que este mecanismo no permite que los equipos se registren y por lo tanto no existirá tráfico generado por parte de estos, no es obligatorio contar con estadísticas ni reportes asociados con la ejecución de este proceso.

  A nivel técnico la implementación de este mecanismo debe realizarse mediante facilidades que verifiquen dentro de la señalización, que el IMEI transmitido por los equipos sea de 14 dígitos decimales en cumplimiento del estándar técnico 3GPP TS 23.003. Esta implementación podrá hacerse en cualquier punto de la red, como lo pueden ser EIR, STP/SCP (puntos de transferencia y control de señalización), centrales de conmutación móvil/MSC Servers o red de acceso.

- Mecanismo alterno (ex-post): Se debe proceder a bloquear los equipos que tuvieron acceso a la red con "IMEI sin formato" una vez se detecte que han generado tráfico. Al tratarse de equipos con "IMEI sin formato" y no cumplir con las especificaciones técnicas que definen la estructura de éste parámetro, no es aplicable la programación de los mismos en la BDA, pero si el reporte de la cantidad de "IMEI sin formato" bloqueados a la CRC.

  A nivel técnico la implementación de este mecanismo implica la detección periódica de los "IMEI sin formato" mediante análisis de CDRs con el fin de notificar a los usuarios que su equipo será bloqueado y proceder a hacer su programación en los EIR para lo cual estos equipos deberán soportar esta facilidad.

Teniendo en cuenta lo anterior, se propone aplicar el mecanismo preferente para el control de IMEI sin formato, para lo cual se define que el 1° de febrero de 2017 como la fecha a partir de la cual no se debe permitir el registro de este tipo de IMEI en las redes de los PRSTM.

Así las cosas, a partir del 1° de agosto de 2016 y hasta el 31 de enero de 2017, cada vez que sea detectado un IMEI sin formato, que no haya sido detectado en días anteriores, se le deberá informar al usuario mediante mensajes SMS que, a partir del 1 de febrero de 2017, su equipo no podrá operar en las redes móviles de Colombia

3.2.2 IMEI inválidos

De acuerdo con la especificación técnica 3GPP TS 22.016[16], el IMEI se define como un número único que debe ser asignado a cada equipo terminal móvil de manera individual, y es utilizado para que la red pueda tomar medidas contra el uso de equipos robados o contra equipos de los cuales su uso en la red no pueda ser tolerado por razones técnicas.

[16] 3rd Generation Partnership Project - 3GPP 8 . Technical Specification Group Services and Systems Aspects. International Mobile station Equipment Identities (IMEI). Define el propósito principal y uso del IMEI.

El IMEI está incorporado en un módulo que esta contenido dentro del equipo del usuario, y entre sus características está que debe ser único y no debe ser cambiado después del proceso de producción final del equipo móvil. Por otra parte, la especificación técnica ETSI TS 123 003[17], además anota que estas condiciones del IMEI son requeridas para los equipos móviles GSM aprobados desde del 1 de junio de 2002, y deben ser aplicables a todos los equipos de usuario compatibles con el sistema 3GPP desde el inicio de su producción.

Así mismo, la especificación técnica es clara en definir que el fabricante que implemente el modulo del IMEI en el equipo móvil es responsable de asegurar que **cada IMEI dentro de los rangos asignados es único del equipo en el cual reside, y también es responsable de conservar registros detallados de los equipos móviles producidos y entregados**, lo cual evidencia la importancia que la asignación del IMEI se realice de manera tal que dichos mecanismos de identificación del equipo sean entregados de manera organizada, de forma que se pueda asegurar la asignación única de IMEI a cada equipo fabricado.

Bajo este contexto, la Resolución CRC 3128 de 2011, define un IMEI inválido como aquel cuyo TAC[18] no se encuentra en la lista de TAC asignados por la GSMA, ni en la lista de TAC de los equipos homologados ante CRC.

Con base en la anterior definición, y teniendo en cuenta que en la documentación específica requerida en el proceso de homologación de equipos terminales contenido en el Capítulo I del Título XIII de la Resolución CRT 087 de 1997, es necesario que se presente la carta mediante la cual la GSMA informa al fabricante el TAC asignado y en la cual además se encuentra consignado el nombre de la marca y del modelo del equipo terminal móvil, los IMEI inválidos no pueden modificar su situación de invalidez, pues no es posible homologarlos.

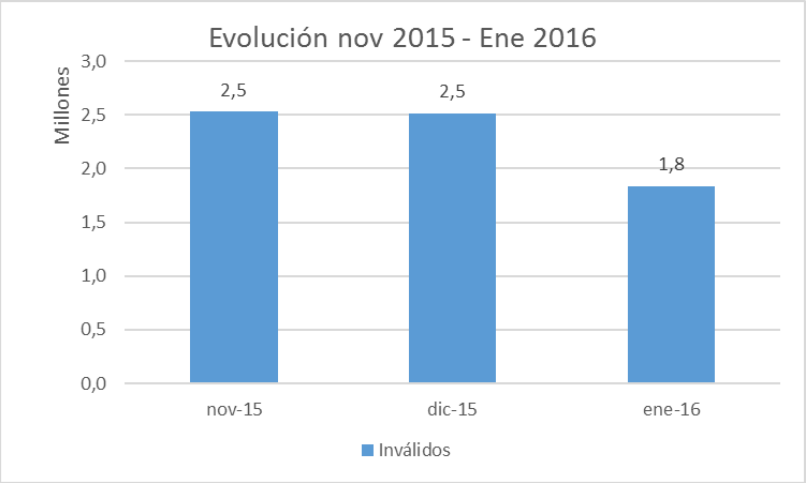
A nivel internacional, algunos países han implementado medidas para el control de equipos terminales móviles con IMEI inválido (ver numeral 6.1 del ANEXO), las cuales abarcan desde condiciones de bloqueo inmediatas hasta campañas de sensibilización con los usuarios para que éstos conozcan los efectos nocivos que pueden causar los equipos que no han sido sometidos a evaluaciones y pruebas de cumplimiento de normativas de seguridad y de uso de materiales peligrosos.

Con base en la información de CDR enviada por los PRSTM durante la etapa de validación y diagnóstico preliminar definida en la Resolución CRC 4813 de 2015, los análisis realizados por la CRC evidenciaron

[17] Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Numbering, addressing and identification (3GPP TS 23.003). Define el propósito principal y uso del IMEI dentro del sistema digital de telecomunicaciones celulares y el sistema 3GPP, describiendo a detalle, entre otros aspectos, el plan de identificación de suscriptores en el sistema GSM, plan de identificación para elementos de red, áreas, enrutamientos, y estaciones bases del sistema GSM y principios de asignación de identificadores internacionales de equipos móviles y su estructura.
[18] Type Allocation Code o código de asignación del tipo., que corresponde a los 8 primeros dígitos del IMEI.

que fueron vistos con actividad en las redes de los PRSTM en enero de 2016, 1,8 millones de IMEI inválidos, cifra que cayó un 27% con respecto a lo observado para meses anteriores[19].

Gráfico 9. Análisis etapa diagnóstico preliminar - IMEI inválidos



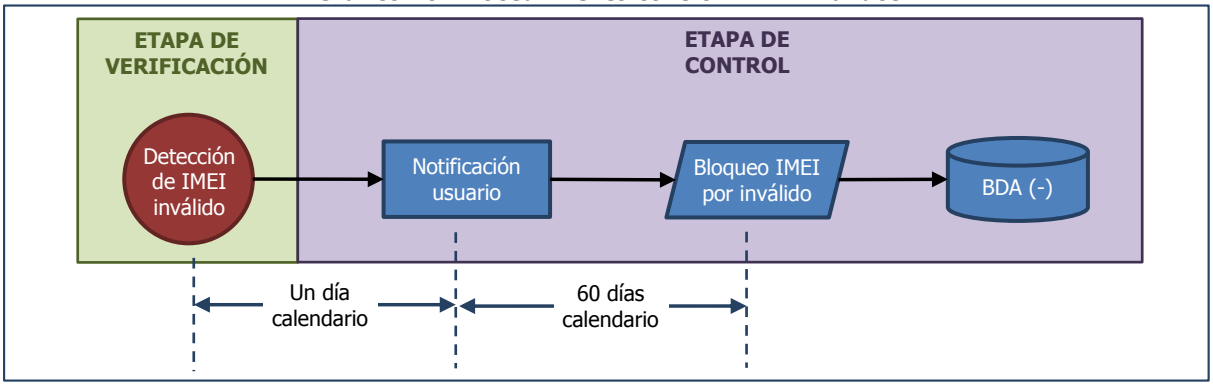
Fuente: Elaboración CRC con base en información de los PRSTM y la GSMA

Así mismo, de acuerdo con lo establecido en la Resolución CRC 4868 de 2016, los PRSTM debían identificar en el mes de febrero los IMEI inválidos que no estaban registrados en la BDA positiva, para posteriormente solicitar el registro a los usuarios y bloquearlos en caso que no lo realizaran. De acuerdo con las cifras reportadas por los PRSTM, se identificaron 940 mil IMEI inválidos, cuyos usuarios serán contactados en un lapso de 4 meses. Es de anotar que en dicho intervalo de tiempo, hay equipos que posiblemente ya no estarán en funcionamiento, razón por la cual puede disminuir el número de usuarios que son contactados. En el primer mes se bloquearon 62 mil IMEI en abril de 2016. La labor de notificación a los usuarios y bloqueos por no registro deberá continuar hasta el mes de julio.

Así las cosas, se proponen la realización de las actividades mostradas en el Gráfico 10, en el que se le informa al usuario la fecha a partir de la cual su equipo no podrá operar en las redes móviles de Colombia. Luego de 60 días calendario a partir de la notificación al usuario, el PRSTM deberá proceder al registro del IMEI en la BDA negativa con tipo "Inválido". Se deberá tener en cuenta que no sería posible desbloquear un IMEI que ha sido bloqueado por inválido. Así mismo, se propone enviar una nueva notificación al usuario un día antes de realizar el respectivo bloqueo.

[19] Noviembre y diciembre de 2015.

Gráfico 10. Procedimiento control IMEI inválidos



Fuente: Elaboración CRC

3.2.3 IMEI no homologados

En términos generales, el objetivo de la homologación de equipos y aparatos de telecomunicaciones, es asegurar el adecuado cumplimiento de las especificaciones técnicas a que éstos deben sujetarse para prevenir daños a las redes a que se conectan, evitar interferencias en otros servicios de telecomunicaciones, y garantizar la integridad y calidad de las redes de telecomunicaciones, del espectro radioeléctrico y la seguridad de los usuarios, proveedores y terceros.

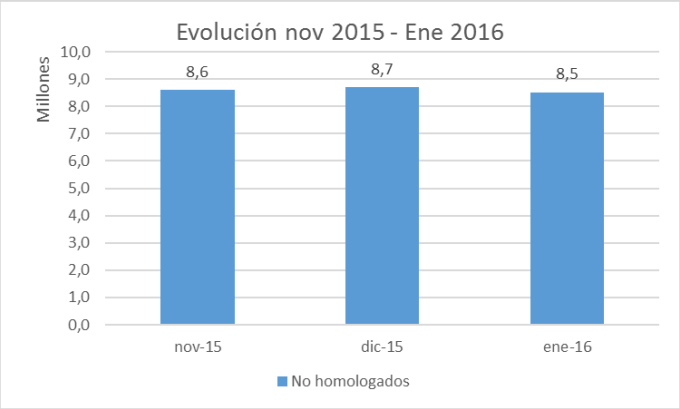
De acuerdo con lo establecido en la Resolución CRC 3066 de 2011, es obligación de los usuarios utilizar equipos homologados, cuando dicha homologación sea obligatoria, que es el caso de los equipos terminales móviles.

En Colombia, el procedimiento y los requisitos para la homologación de equipos terminales está contenido en el Capítulo I del Título XIII de la Resolución CRT 087 de 1997. En dicha norma se establece que los proveedores de redes y servicios de comunicaciones, en concordancia con lo establecido en el artículo 105 de la Resolución CRC 3066 de 2011, sólo podrán exigir como condición para la activación de los equipos terminales en sus redes que dichos equipos se encuentren homologados, cuando la homologación sea obligatoria.

Con base en la información de CDR enviada por los PRSTM durante la etapa de validación y diagnóstico preliminar definida en la Resolución CRC 4813 de 2015, los análisis realizados por la CRC evidenciaron que fueron vistos con actividad en las redes de los PRSTM 8,5 millones de IMEI cuyo TAC corresponde a un ETM que no ha sido homologado por la CRC, cifra que muestra un comportamiento similar para los meses analizados[20].

[20] Noviembre de 2015 a enero de 2016

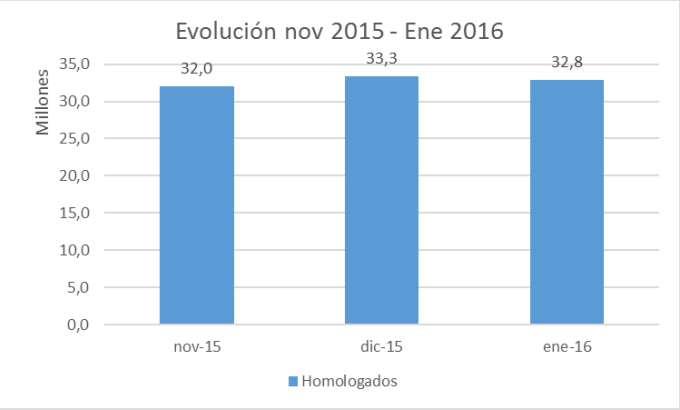
Gráfico 11. Análisis etapa diagnóstico preliminar - IMEI no homologados



Fuente: Elaboración CRC con base en información de los PRSTM

Así mismo, es importante destacar que fueron observados 32,8 millones de IMEI cuyo TAC pertenece a un ETM homologado por la CRC, cifra que se mantiene relativamente constante para los meses analizados.

Gráfico 12. Análisis etapa diagnóstico preliminar - IMEI homologados



Fuente: Elaboración CRC con base en información de los PRSTM

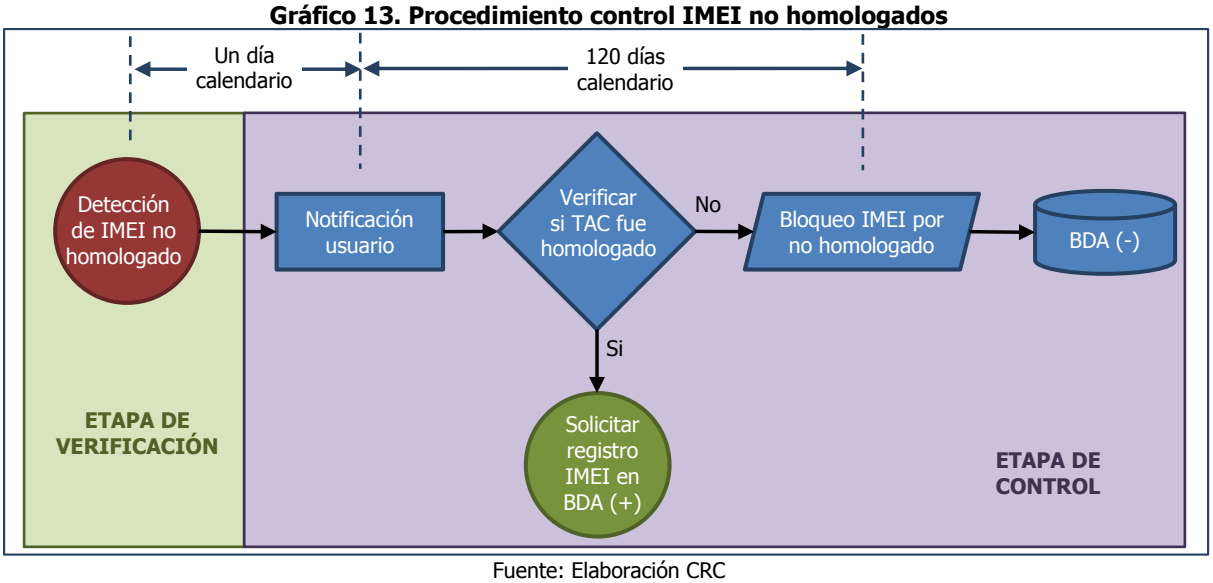
En este sentido, resulta evidente que los equipos que operan en las redes de los PRSTM deben estar homologados. Es importante tener en cuenta que si no se controlan este tipo de equipos, es decir equipos con TAC válido pero no homologados, ello representa una brecha de control de equipos que puede llegar a ser utilizada por las bandas dedicadas a la alteración de los IMEI, pues estas podrían optar por incluir IMEI no homologados en los equipos que modifiquen.

Por lo anterior, resulta necesario realizar el control de los IMEI cuyo TAC no se encuentra en lista de homologados ante la CRC. Así las cosas, se proponen la realización de las actividades mostradas en el

Gráfico 13, en el que se le informa al usuario que en 120 días calendario será bloqueado su IMEI si la marca y modelo de su equipo no es homologado ante la CRC. Esta medida, fortalece el mercado legal de equipos, pues conlleva a que el usuario adquiera equipos homologados para su uso en las redes móviles del país. Luego de 120 días calendarios a partir de la notificación al usuario, y en caso que se haya verificado que el equipo no fue homologado, el PRSTM deberá proceder al registro del IMEI en la BDA negativa con tipo "No homologado". Se deberá tener en cuenta que es posible desbloquear un IMEI que ha sido bloqueado por no homologado, cuando se verifique que el modelo del equipo ha surtido el proceso de homologación ante la CRC. Así mismo, se propone enviar una nueva notificación al usuario un día antes de realizar el respectivo bloqueo.

Por otra parte, teniendo en cuenta que la lista de TAC de los equipos homologados ante CRC es dinámica, se propone incluir una obligación a los PRSTM de informar su actualización a los usuarios, con base en la información suministrada por la CRC.

Gráfico 13. Procedimiento control IMEI no homologados



Fuente: Elaboración CRC

3.2.4 IMEI duplicados

Se entiende por IMEI duplicado aquel que está programado simultáneamente en dos o más ETM, lo cual evidencia la existencia de por lo menos un proceso de adulteración de equipos y de incumplimiento de estándares técnicos. Su detección se realiza mediante la aplicación de algoritmos de "simultaneidad de llamadas en el tiempo" y de "conflicto tiempo distancia", los cuales basados en los registros que

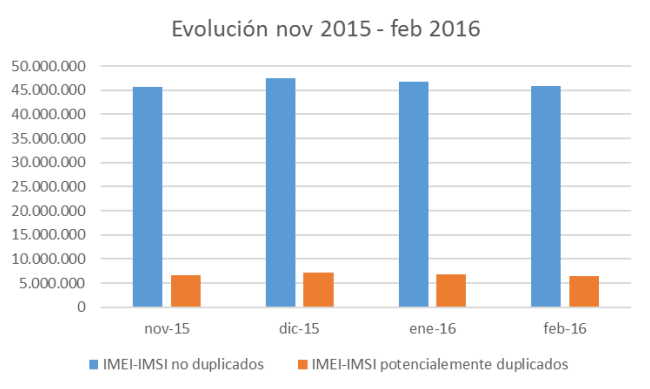
evidencian la actividad[21] de los equipos (identificados por su IMEI) y la IMSI que fue identificada, determinen la existencia de equipos duplicados en razón a que en algún momento del tiempo se detecta que con el mismo IMEI diferentes IMSI están simultáneamente generando actividad en la red, o que al aplicar reglas de tiempo y distancia se evidencie que con el mismo IMEI diferentes IMSI han generado actividad en la red en diferentes momentos y lugares, de tal manera que no es factible que tal actividad obedezca a un cambio de SIM sobre el mismo equipo.

Con base en la información de CDR enviada por los PRSTM durante la etapa de validación y diagnóstico preliminar definida en la Resolución CRC 4813 de 2015, se realizó una aproximación al uso de varias SIM con un mismo IMEI, sin que este hecho implique en sí mismo que dicho IMEI está duplicado. Es de tener en cuenta que en la realidad del mercado colombiano, existen usuarios que cambian de SIM para aprovechar las ofertas comerciales de diferentes PRSTM, o existen comercializadores informales de minutos en las calles, que pueden cambiar de SIM en el mismo equipo cuando han agotado los recursos iniciales.

Es así como se identificaron en el mes de febrero 2016, 42,4 millones de IMEI que presentaron actividad en las redes de los PRSTM, cifra similar a los meses previos analizados. Sin embargo, es importante tener en cuenta que un mismo IMEI pudo ser utilizado con más de una IMSI, lo cual da como resultada que para el mes de febrero, 52,4 millones de parejas IMEI-IMSI registraron actividad. Este último dato es el más cercano conteo al número de equipos presentes en las redes móviles del país.

Bajo este escenario, los análisis realizados por la CRC evidenciaron que del total de parejas IMEI-IMSI observadas en febrero de 2016, el 87,6% son únicas, y el 12,4% (alrededor de 6,5 millones) fueron vistas con 3 o más IMSI, que fue el umbral de potencial duplicidad utilizado en los análisis.

Gráfico 14. Análisis etapa diagnostico preliminar - Parejas IMEI-IMSI



Fuente: Elaboración CRC con base en información de los PRSTM

[21] A hoy solo se ha considerado el uso de CDRs de tráfico de voz y posteriormente los de tráfico de datos. A futuro podrán considerarse otro tipo de CDRs o registros en HLR, VLR, SLR siempre y cuando se desarrollen las aplicaciones que permitan su uso y tales registros permitan hacer una detección de equipos duplicados estandarizada y más versátil.

Sólo los análisis posteriores que realizarán los PRSTM incluyendo los criterios y simultaneidad y conflicto tiempo distancia permitirán llegar a la cifra real de equipos duplicados. Ejercicios preliminares realizados al interior de algunas redes, ubican la cifra en el orden de cientos de miles de equipos.

FUNCION DE LAS REDES MÓVILES PARA LA VALIDACION DEL EQUIPO TERMINAL MOVIL.

Cuando un ETM interactúa con una red móvil, esta última realiza una serie de validaciones a nivel de señalización MAP[22] con el fin de autorizar el acceso a la misma. Dentro de estas validaciones se realiza la conocida como el CHECK_IMEI[23] mediante la cual el equipo es requerido para enviar la información del IMEI, la cual es contrastada contra las listas del EIR[24] y en caso de encontrarse allí el IMEI, se niega el acceso a la red móvil. Así, a partir de los reportes de hurto y extravío que recibe el operador móvil, el IMEI del equipo reportado es incluido en dicha lista.

Sin embargo, en los casos en que un mismo IMEI está programado en varios equipos terminales móviles, este bloqueo afecta a todos los usuarios que usan dichos equipos, impidiendo al usuario del equipo genuino que haga uso del servicio, a raíz de un reporte de hurto o extravío que él no realizó.

Ahora bien, cuando se identifica un conjunto de equipos que tengan el mismo IMEI y se logre determinar cuál de éstos es el equipo genuino (ver numeral 4.2.4.2.), se podrá individualizar cual IMSI corresponde al usuario o propietario de dicho equipo y, por lo tanto, solamente éste debería tener servicio mientras que los otros equipos deberían ser bloqueados. Para lograr esto, la validación inicial que realiza la red móvil debería hacerse sobre el IMEI y también sobre el IMSI, a fin de poder distinguir y decidir a cuál de todas las IMSI que puedan intentar usar dicho IMEI, se le autoriza el acceso a la red móvil.

ALTERNATIVAS DE CONTROL PARA IMEI DUPLICADOS.

Respecto de las alternativas disponibles en el mercado, se ha evidenciado la disponibilidad de la funcionalidad de validación de IMEI-IMSI soportada por los EIR que actualmente operan en el país[25], la cual funciona de manera complementaria a la validación actual basada en el chequeo del IMEI que es ejecutado entre los elementos de red MSC/SGSN[26] y el EIR cada vez que un equipo terminal móvil se registra o en otros eventos de red que se puedan configurar.

La validación de IMEI-IMSI permite que en los casos en que se identifica la pareja correspondiente al equipo genuino, la misma se pueda introducir en la base de datos del EIR de manera tal que cuando se

[22] Mobile Application Part
[23] Término proveniente del nombre asociado al mensaje de señalización dentro del protocolo de validación.
[24] Equipment Identity Register por sus siglas en inglés. Registro de identificadores de los equipos terminales móviles. Tiene la capacidad de prevenir que se realice una llamada cuando se detecte que el equipo terminal móvil tiene un reporte de hurto o extravío o sufre de algún fallo susceptible de afectar negativamente a la red. El tipo de respuesta hacia la red móvil se basa en el manejo de listas de colores "blanca", "gris" y "negra", siendo esta última la utilizada para negar el servicio.
[25] Con base en consultas realizadas en las páginas web de los fabricantes y en una respuesta de los PRSTM al requerimiento de información formulado por la CRC (Rad. 201651840).
[26] MSC: Mobile Switching Center; SGSN: Serving GPRS Suport Node.

realiza la validación del equipo para autorizar o negar su acceso a la red móvil, éste envía la información de IMEI e IMSI, y si la pareja coincide con la incluida en EIR se autoriza el acceso, en caso contrario se niega. Esto trae como efecto que de diferentes equipos terminales móviles que hagan uso de un mismo IMEI, y por lo tanto utilizado con diferentes tarjetas SIM, solamente funcione en las redes aquel que el operador móvil configure con la SIM del usuario del equipo genuino.

Por información de la industria, una funcionalidad de este tipo puede alcanzar un valor de aproximadamente USD$ 200.000 y un tiempo de implementación en elementos de red de hasta 3 meses.

A manera de referencia, a continuación se explica el funcionamiento de esta capacidad en uno de los EIR disponibles actualmente en el mercado.

Cuando el mensaje CHECK_IMEI es recibido por protocolo, la información de IMSI (si esta activa) y de SVN (Software Versión Number, por sus siglas en inglés) son extraídos de la unidad de mensajería de señalización (MSU, por sus siglas en inglés) e interpretados. Debido a que diferentes vendedores colocan la información de IMSI en diferentes ubicaciones dentro del mensaje, el decodificador busca el IMSI en múltiples sitios del mensaje y una vez el dato es interpretado, se realiza la búsqueda en la base de datos de tiempo real del EIR para determinar el tipo de respuesta para la combinación IMEI/IMSI, con lo cual el mensaje de respuesta apropiado es enviado al MSC.

En el Gráfico 15 se aprecia el flujo de llamada hacia el EIR de uno de los fabricantes, en cuyo caso se cumple el siguiente proceso.

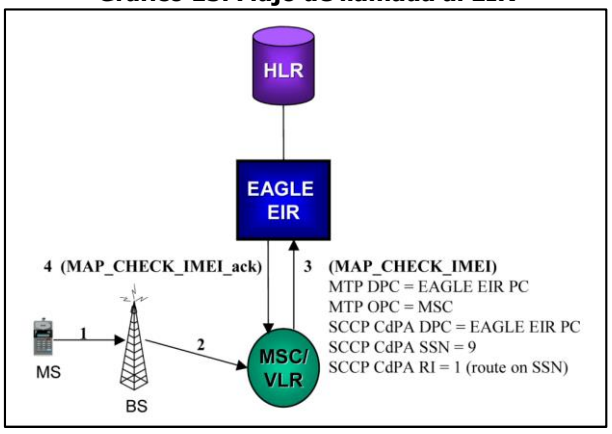
La base de datos en tiempo real del EIR contiene la lista de IMEIs, y una indicación de la lista en la cual están incluidos.

El flujo de eventos es:

1. *Un mensaje CHECK_IMEI es recibido con IMEI e IMSI*
2. *El IMEI es encontrado en la "lista negra"*
3. *La respuesta del EIR es puesta en la condición "lista negra"*
4. *Sin embargo, debido a que un IMSI está presente en la mensajería y el IMEI está en lista negra, el IMSI es comparado con el registro almacenado en la base de datos en tiempo real.*
5. *Si el IMSI en la base de datos coincide con el enviado en el mensaje de señalización, la condición de respuesta "lista negra" es cancelada.*
6. *El EIR formula la respuesta al mensaje CHECK_IMEI con "Equipment Status = 0 whitelisted"*

Si en el paso 5 el IMSI no coincide con el registrado en la base de datos en tiempo real, la condición de "lista negra" se mantiene y la respuesta del EIR al CHECK_IMEI se formula con "Equipment Status = 1 BlackListed".

Gráfico 15. Flujo de llamada al EIR



Fuente: Oracle Communications. EAGLE EIR User´s Guide

OTRAS ALTERNATIVAS

De acuerdo a un estudio que desarrolla la Agencia Nacional de Telecomunicaciones de Brasil, ANATEL[27], autoridad reguladora de dicho país, mediante el cual consultó a la industria sobre las posibilidades tecnológicas para la prevención y control de equipos terminales móviles clonados, a continuación se presentan son algunas de las conclusiones preliminares, dado que el estudio aún está en fase de ampliar algunos detalles.

El estudio evaluó alternativas de desarrollos del Sistema Integrado de Gestión de Dispositivos[28] (SIGA, por sus siglas en portugués) con el fin de dar tratamiento a los equipos con IMEI clonados, y el bloqueo automático en las redes de equipos no homologados de acuerdo a los estándares de ANATEL. El grupo de estudio conformado por diferentes actores de la industria presentó una visión comparativa a nivel internacional de las principales acciones realizadas en decenas de países que, como Brasil, enfrentan dificultades relacionadas con delitos que involucran dispositivos móviles (robo, hurto, contrabando, piratería) países en los cuales coordinan acciones contra el crimen, así como acciones tecnológicas para restringir el uso de equipos irregulares.

Del estudio se observó que las soluciones tecnológicas están basadas principalmente en el tratamiento del IMEI, a partir del cruce de una base de datos de referencia de IMEIs con los CDR´S de las prestadoras del servicio. En algunos casos, el SIGA se encuentra a la delantera en estas soluciones una vez que viró hacia el tratamiento de la tripleta (MSISDN+IMSI+IMEI), por medio del manejo integrado y centralizado de información de todas las prestadoras de servicios de Brasil, destacándose por el volumen de información dirigida y la posibilidad de cruce de datos entre prestadoras.

[27] "*SIGA-Estudo Novas Tecnologias*", ANATEL, Brasilia 17 de febrero de 2016.
[28] "*Informe Técnico UIT-T de Equipos TIC falsificados"*, página 55. noviembre de 2014, http://www.itu.int/pub/T-TUT-CCICT-2014

El estudio evidenció igualmente que la actual solución del SIGA está en línea con otras soluciones respecto de la identificación de los casos y de las acciones de bloqueo o restricción, las cuales se dan después de la detección de las alarmas generadas por la solución y de la comunicación a los usuarios que poseen equipos no conformes. No se identificaron, a nivel mundial, soluciones con un nivel de madurez suficiente, tal que permitan bloqueos automáticos. Este aspecto fue una lección aprendida en el proyecto ejecutado en Egipto, donde el bloqueo automático fue aplicado y en virtud del alto impacto fue necesaria la realización de un *rollback* o reversión del proceso. Se concluyó con el estudio que aún no es aconsejable el proceso de bloqueo automático en la red, hasta que haya soluciones maduras o suficientes que permitan un índice de error marginal.

Específicamente en relación al análisis de nuevas tecnologías para el direccionamiento de la identificación automática del aparato original en caso de clonación, el proyecto indica que no hay, en este momento, un producto disponible en el mercado que direccione plenamente este escenario. Tanto las propuestas de solución basadas en aplicativo, la formación de una identidad del aparato (*fingerprint*), así como la alteración en el proceso de registro/señalización del aparato (para el caso del certificado digital en zonas seguras), necesitan aún evolucionar en términos de investigación y desarrollo por los propios proveedores, prestadores y fabricantes para que haya un grado adecuado de confiabilidad, eficiencia, esfuerzo y plazo de implementación de la solución.

Además de las cuestiones técnicas mencionadas, existe la necesidad de ampliación del debate en relación a la reglamentación y de los estándares mundiales actualmente seguidos por la industria de las telecomunicaciones. Como ejemplo de esta necesidad, está la solución estudiada por el Grupo de Trabajo con mayor probabilidad de eficiencia, que es la de certificado digital en zonas seguras que impacte directamente el actual modelo de autenticación y fabricación de aparatos establecidos por el 3GPP y GSMA.

Frente a este escenario, considerando la alineación del modelo brasileño en relación a las mejores prácticas adoptadas en el mundo, reforzado por las cifras ya presentados por el sistema SIGA, El Grupo de Trabajo sugirió que en este momento se centralicen los esfuerzos en iniciar el tratamiento de los casos generados y ya identificados por el SIGA, o sea, aproximadamente 95% de no conformidades y 5% de clonación. Al mismo tiempo, se recomienda a los equipos técnicos mantener un plan de trabajo que incluye monitoreo de resultados, evolución de indicadores, análisis de impactos y afinación de procedimientos para el tratamiento de los casos de no conformidad y clonación.

Vistas las conclusiones del estudio realizado por Brasil y la disponibilidad en nuestro mercado de la capacidad de validación en el EIR de la pareja IMEI-IMSI, la alternativa de control selectivo a través de dicha funcionalidad es la única alternativa viable para permitir que solo tenga servicio el usuario del equipo genuino a fin de respetar sus derechos y bien adquirido, sin que los demás equipos en los cuales el IMEI fue clonado puedan funcionar. De no implementarse, implica tener que tomar decisiones sobre desbloquear el IMEI del usuario del equipo genuino en aras de proteger sus derechos, permitiendo así que los clones funcionen y abriendo la brecha para que se aumenten los casos de IMEI duplicado recurriendo a copiar identificadores de equipos genuinos funcionando en el país.

3.2.4.1 Tipos de IMEI duplicados (clonados) a detectar.

Cuando se detecten IMEIs duplicados con la aplicación de los algoritmos de "simultaneidad de llamadas en el tiempo" y de "conflicto tiempo distancia", los PRSTM deberán ejecutar una serie de acciones respecto de los equipos implicados, dirigidas a determinar la existencia del equipo genuino[29] con el fin de proteger los derechos de los usuarios de tales equipos, haciendo uso de los mecanismos de validación en el EIR para dar servicio solamente a la combinación de IMEI-IMSI que corresponde.

Identificados los IMEI duplicados, el desarrollo de las acciones se realizará de acuerdo con las condiciones de mayor prioridad indicadas en los numerales anteriores de este documento. Así, se presentan los siguientes escenarios que deben tenerse en cuenta para lo toma de medidas respecto de estos casos:

Tabla 4. Tipos de IMEI duplicados

Duplicado	Homologado	IMEI en BD+	TAC en GSMA	Caso Resultante	Número de Caso
Si	No	Si	No	Duplicado inválido (registrado)	1
Si	No	Si	Si	Duplicado no homologado (registrado)	2
Si	Si	N/A	N/A	Duplicado homologado	3

Fuente: Elaboración CRC

Casos Resultantes:

1. **Duplicado con IMEI inválido (registrado en la BDA positiva antes del 1 de agosto de 2016):** Este caso corresponde a equipos con IMEI duplicado y que hayan sido registrados en la base de datos positiva antes del 1° de agosto de 2016, pero cuyo TAC no es válido en GSMA (no existe en la base de datos de TACs asignados a fabricantes) y no corresponde a ningún TAC de la lista de marcas y modelos de equipos homologados por la CRC.

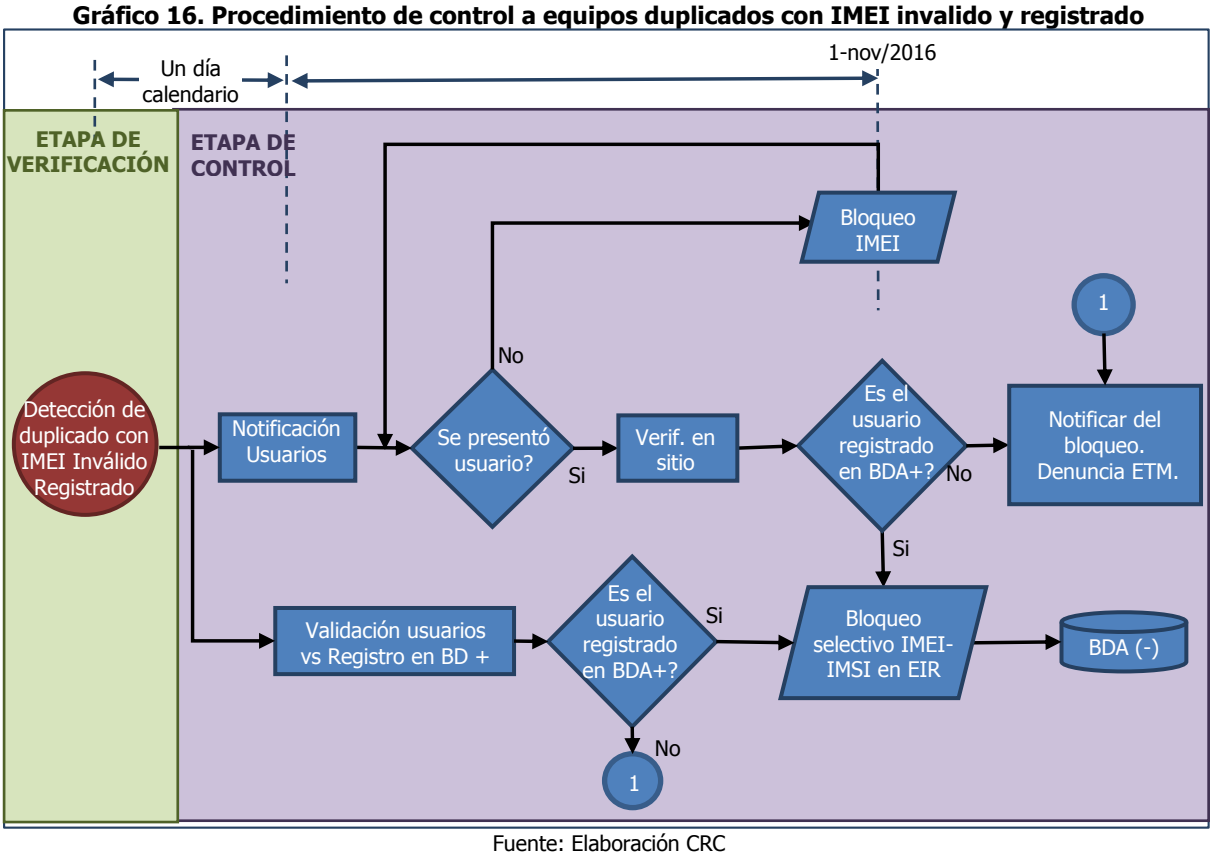
   Dado lo anterior, no se cuenta con registros que permitan verificar la correspondencia de información y características de un equipo a partir de su IMEI (Porción del TAC) con una determinada marca, modelo y referencia comercial, y de esta manera el único parámetro disponible para analizar y definir las medidas a tomar en estos casos es el registro que se haya realizado en la base de datos positiva, a fin de determinar aquel equipo que fue debidamente registrado de acuerdo a las normas, así como los soportes presentados por el usuario para asociar la propiedad del equipo con el número de identificación registrado en la base de datos positiva.

   Para este caso, las acciones propuestas son:

[29] Según la real academia española de la lengua, la definición de "genuino" corresponde a "auténtico", "legitimo". Por lo tanto, se utilizará este término para referirnos al equipo terminal móvil que fue producido por el fabricante al cual se le asignó el TAC y el IMEI de conformidad con el procedimiento GSMA TS.06 IMEI ALLOCATION AND APPROVAL PROCESS.

i) validación de la existencia de una asociación entre el documento de identidad del usuario que registró el equipo en la base de datos positiva y los usuarios titulares de las líneas (IMSI) identificadas usando equipos con dicho IMEI,
ii) notificación a los usuarios vía SMS (incluido SMS flash), o preferiblemente por otros medios de contacto, y
iii) verificación (en puntos de atención del PRSTM, ver sección 4.2.4.2.) para identificar el usuario y el equipo que fue objeto de registro, a fin de proceder a su protección con un mecanismo de bloqueo selectivo por medio de la validación en el EIR de la pareja IMEI-IMSI correspondiente al usuario registrado en la base de datos positiva antes del 1 de agosto de 2016.

Gráfico 16. Procedimiento de control a equipos duplicados con IMEI invalido y registrado



Fuente: Elaboración CRC

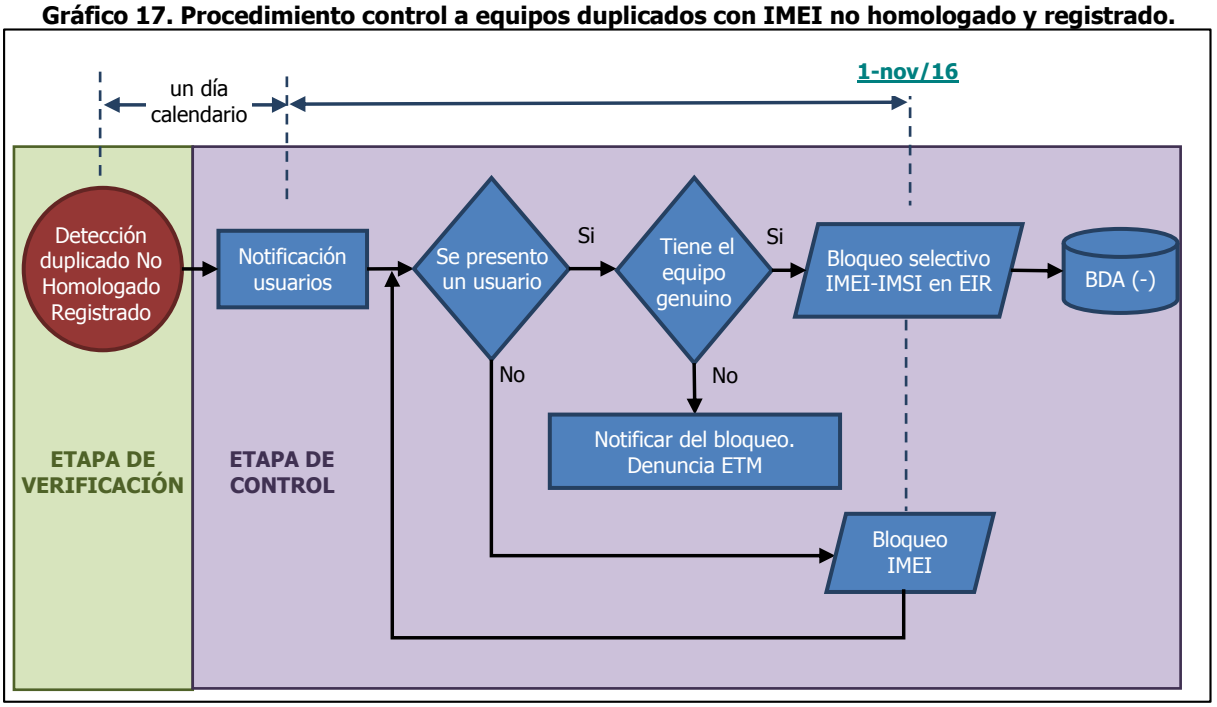
2. **Duplicado con IMEI no homologado (registrado en la BDA positiva antes del 1 de agosto de 2016):** Este caso corresponde a equipos con IMEI duplicado, en el cual el IMEI fue registrado en la base de datos positiva antes del 1° de agosto de 2016, cuyo TAC existe en la

base de datos de GSMA (asignado a un fabricante) y el cual no corresponde a ningún TAC de la lista de marcas y modelos de equipos homologados en la CRC.

Para este caso, se cuenta con parámetros de verificación del TAC registrado en la GSMA, por lo cual las acciones propuestas son:

i) notificación a los usuarios de esos equipos por los diferentes medios de atención al cliente y
ii) verificación (en puntos de atención del proveedor, ver sección 4.2.4.2.) con el fin de determinar cuál es el usuario con el equipo genuino para proceder a su protección con un mecanismo de bloqueo selectivo por medio de la validación en el EIR de la pareja IMEI-IMSI, correspondiente al equipo genuino.

Gráfico 17. Procedimiento control a equipos duplicados con IMEI no homologado y registrado.



Fuente: Elaboración CRC

3. **Duplicado con IMEI homologado:** Este caso corresponde a equipos con IMEI duplicado, el cual puede tener o no registro en la base de datos positiva. En caso que haya registro en la BD positiva, el mismo puede haberse realizado antes o después del 1 de agosto de 2016. También cuentan con un TAC que corresponde a una marca y modelo de la lista de equipos homologado por la CRC. En algunos casos, el TAC de la lista de equipos homologados en la CRC puede no existir en la lista de TAC asignados por la GSMA.

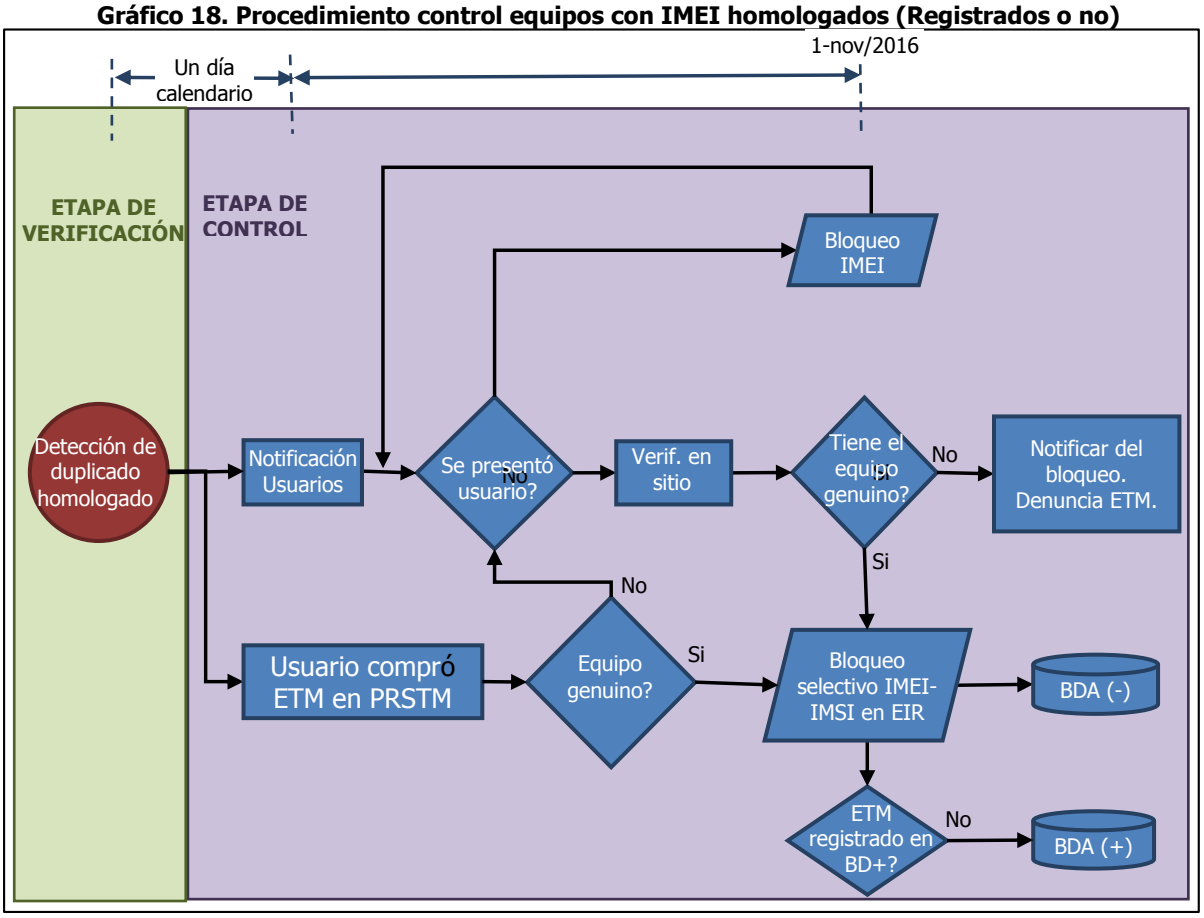
   Para este caso, las acciones a propuestas son:

i) Determinar la existencia de registros que evidencien la compra legal del equipo por parte de un usuario en tiendas del proveedor de servicios y así mismo si el IMSI corresponde al mismo usuario que realizó la compra del equipo, en cuyo caso sería la pareja IMEI-IMSI valida,

ii) En caso de no encontrarse dicha asociación, proceder a la notificación a los usuarios de esos equipos por los diferentes medios de atención al cliente, y

iii) verificación (en puntos de atención del proveedor, ver sección 4.2.4.2.) con el fin de determinar cuál es el usuario con el equipo genuino para proceder a su protección con un mecanismo de bloqueo selectivo mediante la validación en el EIR de la pareja IMEI-IMSI correspondiente al equipo genuino.

Gráfico 18. Procedimiento control equipos con IMEI homologados (Registrados o no)



Fuente: Elaboración CRC

3.2.4.2 Identificación del Equipo genuino.

Con el fin de determinar la existencia de un equipo genuino entre los diferentes equipos que tengan programado un mismo IMEI, de acuerdo con los casos explicados anteriormente, se deben ejecutar por parte de los PRSTM procedimientos de notificación a los usuarios de dichos equipos y de verificación de los mismos, lo cual conllevaría en caso de presentarse, a la identificación de la pareja IMEI-IMSI válida, para proceder a su protección con un mecanismo de bloqueo selectivo mediante la validación en el EIR de la pareja IMEI-IMSI correspondiente al equipo genuino.

Con base en lo anterior, se tienen dos posibles escenarios para buscar identificar el equipo genuino:

i) verificación de información disponible respecto del IMEI en la red móvil y en las bases de datos que incluyen el ciclo de vida de un equipo (asignación del TAC e IMEI, fabricación, homologación, importación, venta, activación o uso, bases de datos positivas y bases de datos negativas) y
ii) verificación física del equipo (marca, modelo, soportes de adquisición, caja, características del hardware y del software).

La verificación inicial de información del IMEI no siempre será posible (es el caso de los IMEI inválidos de los cuales no se tiene información de referencia en las bases de datos de GSMA ni en la de equipos homologados en la CRC), o no estará disponible en su totalidad, con lo cual disminuye la probabilidad de identificar el equipo genuino. No obstante, la verificación física de los terminales que contienen un mismo IMEI aumenta dicha probabilidad, ya que ofrece la posibilidad de contrastar la información que esté disponible en las diferentes bases de datos contra las características de los diferentes equipos que los usuarios decidan someter a revisión (marca, modelo, referencia comercial). Adicionalmente, permite analizar otros elementos necesarios (soportes de adquisición, correspondencia de información entre el usuario y los datos del titular o usuario de la línea en el PRSTM y respecto del registro del IMEI en la base de datos positiva). También trae como consecuencia disuadir a quienes hacen uso de equipos con IMEI alterado, de manera consciente, y no se presentan con el equipo, generando reducción de carga operativa en el PRSTM en cuanto a los análisis preliminares y la atención personalizada.

Por las razones anteriores, se propone establecer el procedimiento con los pasos de: detección – notificación – verificación en sitio, dejando de manera opcional la verificación inicial y análisis de información en red móvil o bases de datos.

1. Verificación inicial

   El objetivo de esta verificación es la realización de un chequeo inicial a partir de cruces de información proveniente de los CDR (u otros insumos o elementos de la red) contra la información de los TAC según GSMA, y con otros registros administrativos con los que cuente en proveedor con el fin de determinar proactivamente si es posible identificar la pareja IMEI-IMSI del equipo genuino. Para realizar esta verificación se deben ejecutar como mínimo las siguientes acciones:

Para usuarios con IMEI duplicado inválido (registrado).

a. Verificación de la asociación entre el documento de identidad del usuario que registró el equipo en la base de datos positiva y los datos de los usuarios titulares de las líneas (cuyas IMSI tienen actividad con el mismo IMEI).

   En caso que se encuentre una pareja IMEI-IMSI que cumpla esta asociación se debe proceder a incluirla en el EIR a fin de autorizar el servicio solamente a esta combinación.

Para usuarios con IMEI duplicado no homologado (registrado) y homologados:

a. Verificación de la existencia de registros que evidencien la compra legal del equipo por parte de un usuario en puntos de venta autorizados, en caso de registro en BD positiva o de venta directa por el PRSTM, y si el IMSI corresponde al mismo usuario.

   En caso que se encuentre una pareja IMEI-IMSI que cumpla esta asociación se debe proceder a incluirla en el EIR a fin de autorizar el servicio solamente a esta combinación.

b. Verificación de información proveniente de los CDRs para cada pareja IMEI-IMSI con el fin de contrastar las características del equipo utilizado en las comunicaciones, contra la información asociada al TAC, dentro de las cuales se incluyen, pero no se limitan a:
   i. Constatar si según el TAC las bandas soportadas por los equipos permiten su uso en la red en la cual cursó tráfico en razón a que tales bandas han sido asignadas al operador que presta el servicio. De acuerdo con esta verificación, se tiene por ejemplo que equipos que solo soportan la banda de 850 no deberían cursar tráfico en banda de 1900.
   ii. Constatar si según el TAC las tecnologías de acceso a la red empleadas corresponden con las tecnologías de redes de acceso soportadas. De acuerdo con esta verificación, se tiene por ejemplo que equipos que según su TAC solo soportan acceso a redes 2G no deberían cursar tráfico en redes de 3G o posteriores.
   iii. Constatar si la fecha de expedición del TAC es anterior a las fechas de fabricación, importación, venta o inicio de actividad en la red.
   iv. Otras verificaciones propuestas por el PRST basadas en el cruce de información proveniente de los diferentes campos de los CDRs o de otros registros y la información del TAC, tales como la correspondencia entre marca y modelo con la actividad en la red.

   En caso que se logre determinar todas las parejas IMEI-IMSI no válidas y sólo quede una que cumpla una correcta asociación, se debe garantizar que esta pueda cursar tráfico en la red mediante la validación en EIR de la pareja IMEI-IMSI y de esta manera bloquear el tráfico en la red al resto de parejas.

2. Verificación en punto de atención del proveedor

Esta verificación tiene por objeto realizar un chequeo físico del equipo para contrastar la información física, de software y de parámetros lógicos del equipo, así como los soportes que allegue el usuario con el fin de verificar la propiedad del mismo y/o contrastar tal información con bases de datos como las de la GSMA y con otros registros administrativos con los que cuente el proveedor con el fin de determinar la legalidad de la pareja IMEI-IMSI verificada. Para realizar esta actividad se deben ejecutar como mínimo las siguientes acciones:

a. Revisión física del equipo terminal móvil para determinar la concordancia de la etiqueta en la cual se plasma el IMEI y la correspondencia con el IMEI programado[30] en el equipo.

b. Revisión física para verificar correspondencia de marca, modelo y referencia comercial del equipo de acuerdo con la información de fabricación en la GSMA para el TAC del IMEI, así como logos, caja original si se tiene, apariencia del equipo (genuino o falsificado según el tipo de materiales, letras, carcasa, etc.). En caso de no existir consistencia entre la marca, modelo y referencia comercial respecto del TAC, o en cuanto a la caja, materiales, logos, etc. no se considerará como equipo genuino.

c. Revisión física del equipo para verificar aspectos como el sistema operativo y/o número de IMEISV versus información de fabricación en la GSMA para el TAC del IMEI.

d. Revisión de la factura de compra del equipo si se tiene. En esta revisión se debe determinar lo siguiente:

   i. Concordancia de la factura respecto del equipo que se pretende soportar en cuanto a la relación de ésta con el IMEI del equipo analizado, u otros parámetros que lo relacionen (marca, modelo, referencia, color, etc.).
   ii. Concordancia de la factura respecto de la persona que se presenta a soportar la propiedad y legalidad del equipo y/o soportes que de manera adicional a la factura soporten la tenencia o transferencia del equipo.

En caso que se encuentre una pareja IMEI-IMSI que cumpla esta asociación se debe garantizar que esta asociación pueda cursar tráfico en la red mediante la validación en el EIR de la pareja IMEI-IMSI y así bloquear el tráfico en la red al resto.

Si en el marco de estas verificaciones no es posible establecer la existencia de la pareja IMEI-IMSI válida, se debe proceder a realizar bloqueo del IMEI en la BDA negativa.

[30] Verificación realizada mediante el marcado del código *#06#

3.2.4.3 Condiciones operativas para las acciones de control sobre equipos con IMEI duplicado

Notificación a los usuarios

Independientemente que en el marco de las verificaciones iniciales sea posible o no establecer la pareja IMEI-IMSI válida, se requiere notificar a los usuarios (de la línea o IMSI) involucrados en el uso de un equipo cuyo IMEI se ha detectado duplicado.

Los mensajes de notificación se deberán enviar mediante un SMS normal y otro SMS flash, el primero con el objetivo de asegurar el almacenamiento del mensaje de notificación en el equipo para su lectura cuando lo considere el usuario y el segundo para asegurar la lectura por parte de los usuarios al llegar el mensaje abierto al equipo.

Preferiblemente deben usarse también otros medios disponibles de notificar a los usuarios (dirección y teléfonos de contacto, correo electrónico, call center in bound y out bound, pagina web, redes sociales), con el objetivo que el o los usuarios que consideren que cuentan con los soportes para comprobar la legalidad de sus equipos asistan a un punto de atención.

El mensaje de texto deberá incluir el siguiente texto: *"El IMEI de su equipo esta duplicado y podría ser bloqueado. Presente ante su operador el equipo y sus soportes de compra o adquisición"*

En caso en que el PRSTM haya notificado a un usuario respecto de un IMEI duplicado y reciba la información proveniente del proceso de detección inter redes, de haber sido detectado duplicado en relación con otras redes, se debe revisar si es necesario o no enviar una nueva notificación y en cualquier caso evitar enviar más de un mensaje o notificación con diferentes instrucciones (en cuanto a plazos diferentes, o condiciones de detección diferentes, como por ejemplo IMEI no registrado, IMEI inválido o IMEI duplicado).

En caso en que el PRSTM haya identificado un equipo genuino en la etapa de verificación inicial (antes de vencer el plazo para que se presenten los usuarios involucrados), deberá notificar al usuario del equipo legitimo del control por validación IMEI-IMSI y a los usuarios del resto de equipos que usan el mismo IMEI, que su equipo será bloqueado con por lo menos 30 días a aplicar el bloqueo selectivo sobre el IMEI en cuestión.

Verificación en sitio

Es requisito indispensable que se presente el titular de la línea que hace uso del equipo con IMEI duplicado, con su documento de identificación, o en su defecto podrá presentarse un tercero con el debido poder autenticado por un notario público. Asimismo, deberá presentarse el equipo terminal móvil en cuestión.

Dado que no hay otra manera más efectiva y segura de descartar los equipos involucrados que la revisión física del mismo, resulta indispensable que todos los PRSTM atiendan la diligencia de manera presencial y así destinen sus centros de atención al cliente u oficinas o sedes administrativas.

Bloqueo selectivo usando pareja IMEI-IMSI del equipo genuino

Como se observa en los gráficos para los escenarios de control a los casos detectados de la sección número 4.2.4.1., el bloqueo selectivo basado en la inclusión de la pareja IMEI-IMSI en el EIR, se podrá realizar solo hasta que todas las redes de los PRSTM hayan implementado tal funcionalidad. Para ello, la CRC considera que el plazo prudencial es hasta el 1 de noviembre de 2016, atendiendo las consultas realizadas a la industria en las cuales se ha manifestado las condiciones y cambios que ello implica, junto con el inicio y adecuación de otros procesos relacionados con la detección y control a los IMEIs sin formato, los inválidos, los duplicados, los no homologados y los no registrados en base de datos positiva, y el periodo de cuarentena a que convencionalmente se someten los cambios en la red móvil durante diciembre dadas las condiciones de tráfico en dicho periodo.

La configuración y operatividad asociada a la nueva funcionalidad de los EIR relacionada con la validación de IMEI-IMSI será revisada y definida en el Comité Técnico de Seguimiento -CTS-, instancia creada por norma para el seguimiento a la implementación y operación de las bases de datos negativas y positivas contra el hurto de equipos terminales móviles. Deberán considerarse las opciones de utilizar la lista blanca o la lista negra y la lógica de respuesta del EIR según la lista utilizada, la cantidad máxima de IMSI que se podrán configurar a cada IMEI, los procesos en casos de portación y otros aspectos que sean necesarios revisar.

Por esta razón, los casos detectados antes de dicha fecha deben ser notificados en el tiempo propuesto (al día siguiente a su detección). Sin embargo, las acciones de bloqueo solo pueden aplicarse a partir de noviembre 1 de 2016, fecha en la que vence el plazo para tener operativa la funcionalidad en el EIR y red móvil de la validación IMEI-IMSI. Durante dicho periodo, puede invitarse a los usuarios con equipos cuyo IMEI se identifica como duplicado a realizar el cambio de su terminal a efecto de evitar el bloqueo y consiguiente afectación al uso del servicio.

Ahora bien, en caso que sea posible determinar que ninguno de los equipos que hacen uso de un mismo IMEI sea el genuino, y se cuente con los respectivos soportes de tal decisión (por ejemplo, se tiene el equipo genuino en el inventario de un proveedor o punto de venta autorizado), se podrá bloquear el IMEI en el EIR previa notificación a los usuarios que hacen uso de los equipos cuyo IMEI está duplicado, de acuerdo a las condiciones descritas en la siguiente sección.

Posterior al 1 de noviembre de 2016, el plazo para la presentación en los centros de atención a clientes u oficinas de los OMV de los usuarios con su respectivo equipo será de 30 días calendario contados a partir de la notificación al usuario.

Bloqueo del IMEI

Esta acción aplica cuando sobre un IMEI detectado como duplicado en varios equipos terminales móviles, se determina que ninguno de ellos corresponde al equipo genuino o en los casos en que habiendo sido notificados los usuarios que hacen uso de equipos con IMEI duplicado, ninguno se presenta al proveedor de servicios.

Bajo este escenario se debe bloquear en el EIR el IMEI, aplicando el siguiente procedimiento:

a) En caso de aplicar el bloqueo antes de vencerse el plazo de implementación de la validación en el EIR de la pareja IMEI-IMSI, enviar un mensaje de notificación con 30 días calendario de anticipación a la fecha de bloqueo para informar a todos los usuarios que usan un equipo con IMEI duplicado que su equipo será bloqueado por poseer un número de identificación duplicado en la red.
b) Los mensajes de notificación se deberán enviar mediante un SMS normal y otro SMS flash, el primero con el objetivo de asegurar el almacenamiento de la notificación mensaje en el equipo para su lectura cuando lo considere el usuario y el segundo para asegurar la lectura por parte de los usuarios al llegar el mensaje abierto al equipo.
c) Al realizarse el bloqueo, se deberá reportar esta novedad al BDA para su programación en la Base de Datos negativa con tipo de bloqueo "duplicado".
d) En la misma condición debe marcarse un IMEI cuando es compartido en la base de datos de la GSMA.

Confirmación a los usuarios

Una vez sea posible determinar el equipo genuino y/o los equipos que tienen el IMEI modificado, el PRSTM deberá notificar a los usuarios de unos y otros, el bloqueo de su equipo o la manera en que podrá utilizarlo (en caso del equipo genuino), indicando en este último caso los procedimientos para inscribir la tarjeta o tarjetas SIM que podrán ser usadas con el equipo, la cantidad máxima de líneas a usar en tal equipo, los tiempos de atención y respuesta para tales configuraciones, así como de los cambios en las mismas, y las indicaciones en caso en que el usuario use el servicio con otro proveedor de servicio o decida portarse.

Cuando se haya determinado en el proceso de verificación inicial o en el punto de atención la existencia de un usuario con equipo genuino, se puede tener una o varias parejas IMEI-IMSI válidas asociadas a un determinado equipo (un mismo usuario que tiene varias líneas, o un equipo que utilizan diferentes usuarios), así que las restantes parejas IMEI-IMSI no son válidas.

Bajo este escenario para el usuario o usuarios válidos se debe programar en el EIR una validación para las parejas de IMEI-IMSI válidas de tal manera que cualquier otra combinación no pueda cursar el servicio, para lo cual se debe:

a) Notificar al usuario o los usuarios con asociación IMEI-IMSI validos que debido a la duplicación del número de IMEI de sus equipos por parte de otros usuarios, se hará seguimiento a su equipo de

tal manera que los cambios de SIM deben ser registrados ante su operador con el fin de evitar el eventual bloqueo de su equipo.

b) Por otra parte, para los usuarios con asociaciones IMEI-IMSI no válidas se debe enviar un mensaje de notificación con 30 días calendario de anticipación a la fecha de bloqueo del IMEI con el fin de informar que al tener un equipo con un número de identificación que suplanta a un equipo válido, no podrá hacer uso del servicio mientras que use dicho equipo con la SIM actual o con otra.
c) Los mensajes de notificación se deberán enviar mediante un SMS normal y otro SMS flash, el primero con el objetivo de asegurar el almacenamiento de la notificación mensaje en el equipo para su lectura cuando lo considere el usuario y el segundo para asegurar la lectura por parte de los usuarios al llegar el mensaje abierto al equipo.

Denuncia de los equipos detectados con IMEI alterado

La Ley 1453 de 2011 en su artículo 105 tipificó como delito la reprogramación, remarcación o modificación de los equipos terminales móviles en cualquiera de sus componentes con el fin de alterar las bases de datos positivas y negativas creadas para control del hurto de celulares, e indica que los terminales que hayan sido alterados serán decomisados por las autoridades de policía y cuando la detección la haga el proveedor de servicios, procederá a efectuar la respectiva denuncia ante las autoridades competentes.

Procesos relacionados con las bases de datos positiva y negativa

Finalmente, respecto del envío a la BDA negativa de los IMEI incluidos en el EIR con el IMSI correspondiente al equipo genuino, debe tenerse en cuenta que la combinación IMEI-IMSI funciona únicamente para la red a la cual pertenece dicho IMSI, por lo cual es necesario que el IMEI sea bloqueado en las otras redes móviles. Esto se realiza a través de la BDA, que recibe el mensaje de inclusión en base de datos negativa y lo replica al resto de operadores móviles en donde debe ingresarse el IMEI a sus respectivos EIR.

Así, el usuario del equipo genuino que intente usarlo con una IMSI de otro operador no obtendrá servicio dado el bloqueo aplicado al IMEI. Por esta razón se requiere que en las bases de datos negativas (BDA y BDOs) se adecúe una marcación específica para estos casos, tal que los PRSTM estén en la capacidad de identificar los IMEI sometidos a validación IMEI-IMSI y procedan a configurar la respectiva pareja IMEI-IMSI en cada uno de sus EIR, previa solicitud del usuario, la cual será debidamente verificada, incluyendo la validación física del equipo terminal móvil por parte del PRSTM que recibe la solicitud.

Tal funcionalidad deberá también incluir la posibilidad de que el IMEI de los equipos sometidos a validación IMEI-IMSI puedan ser registrados en la base de datos positiva de acuerdo a las normas y condiciones operativas que apliquen.

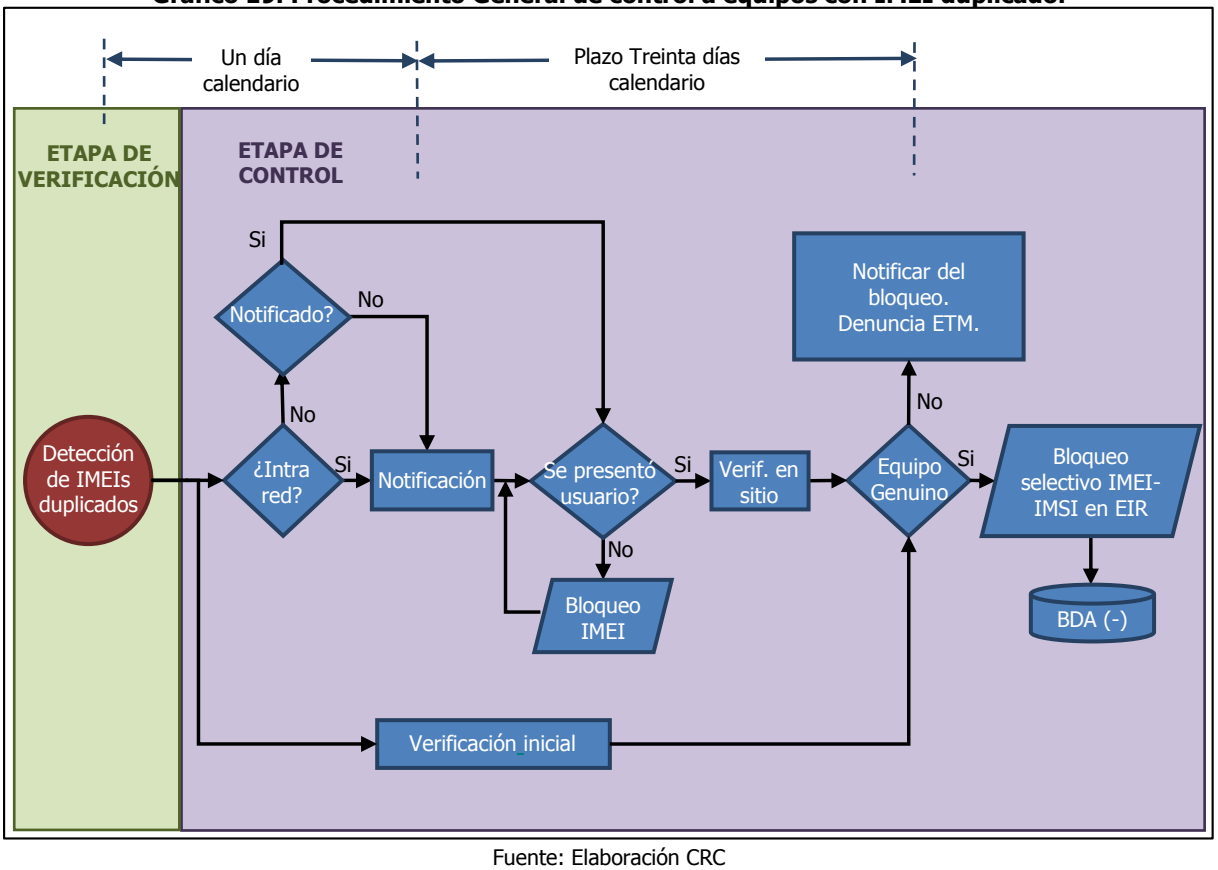
Los PRSTM y el ABD deberán definir los mecanismos y operatividad de esta adecuación y presentarla al CTS un mes antes de la entrada en operación.

Desbloqueo de IMEI duplicado

Cuando se haya efectuado un bloqueo de IMEI y con posterioridad a la medida se presente en un punto de atención del proveedor un usuario con los soportes válidos que permitan demostrar la validez de su equipo, el PRSTM deberá efectuar un proceso de desbloqueo en EIR del IMEI del equipo y su posterior baja de la BDA negativa, y activar el proceso de validación en EIR de la pareja IMEI-IMSI para que sólo la IMSI asociada al usuario pueda acceder al servicio.

Con base en las anteriores consideraciones operativas, se representa en el Gráfico 19 el procedimiento para los casos de IMEI detectados como duplicados considerando los plazos que aplicarían a partir de noviembre 1 de 2016:

Gráfico 19. Procedimiento General de control a equipos con IMEI duplicado.



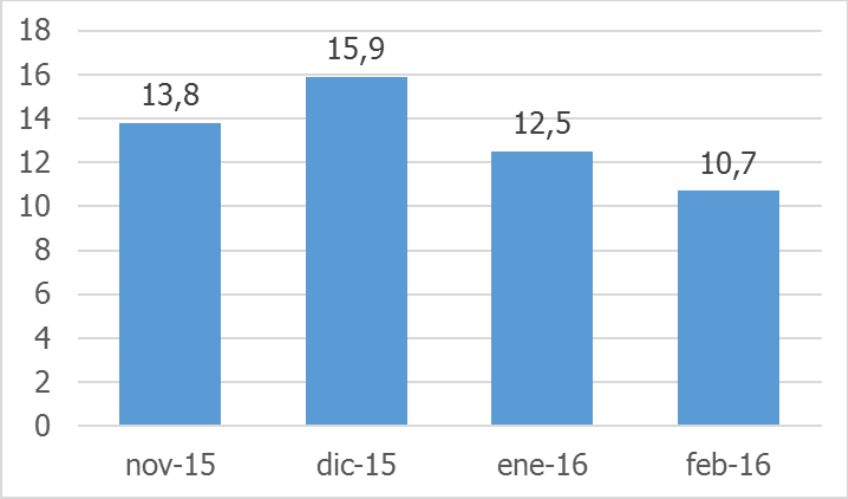
Fuente: Elaboración CRC

3.2.5 IMEI no registrados en la BDA positiva

Actualmente, los PRSTM tienen implementada y en operación una funcionalidad que permite detectar los cambios de equipo terminal móvil respecto a la SIM, sobre la cual se identifican los equipos no registrados, se procede a contactar al usuario y luego al bloqueo de los equipos que no hayan sido registrados en la BDA Positiva. Dicho bloqueo solamente es realizado cuando se modifica al mismo tiempo el IMSI y el MSISDN.

Con base en la información de CDR enviada por los PRSTM durante la etapa de validación y diagnóstico preliminar definida en la Resolución CRC 4813 de 2015, los análisis realizados por la CRC evidenciaron que fueron vistos con actividad en las redes de los PRSTM en febrero de 2016, 10,7 millones de IMEI no registrados en la BDA positiva, cifra que cayó un 14% con respecto a lo observado para el mes de enero de 2016[31].

Gráfico 20. Análisis etapa diagnostico preliminar - IMEI no registrados en la BDA positiva

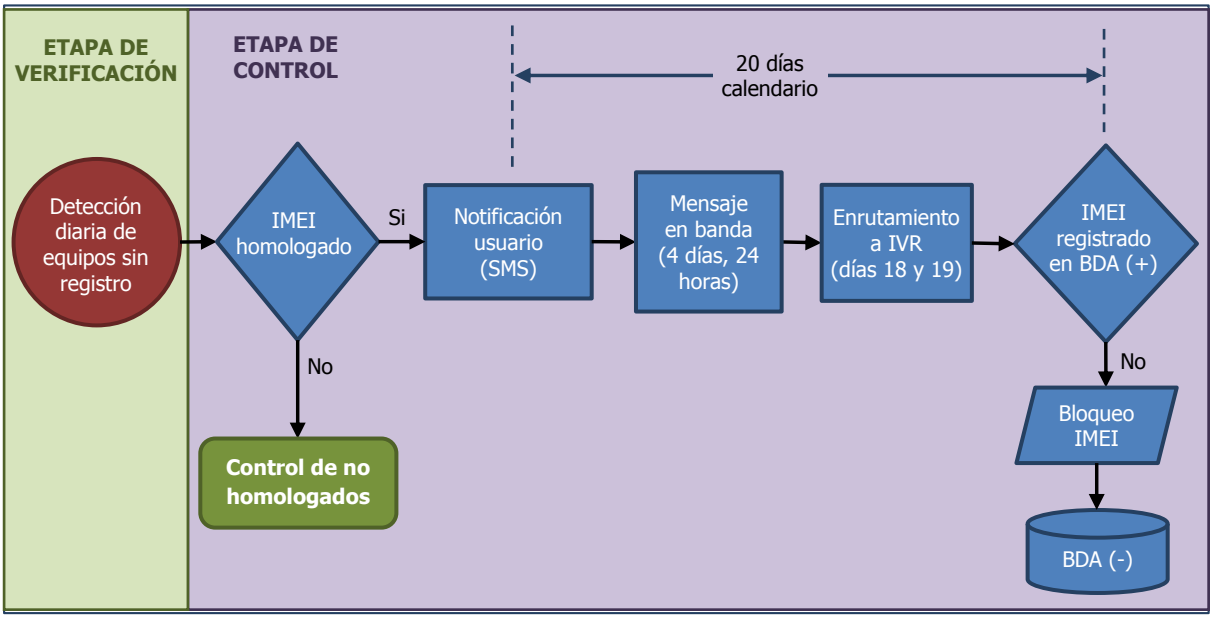


Fuente: Elaboración CRC con base en información de los PRSTM

Sin embargo, a partir de la entrada en operación de las etapas de verificación y control de equipos terminales móviles, se propone ejecutar este control a todos los equipos pero sólo se permitirá el registro a aquellos equipos que se encuentren homologados ante la CRC para su operación en Colombia. Lo anterior, teniendo en cuenta que a partir del 1° de agosto de 2016, los IMEI inválidos y los no homologados serán identificados de manera diaria.

Gráfico 21. Procedimiento control IMEI no registrados en la BDA positiva

[31] Noviembre y diciembre de 2015.



Fuente: Elaboración CRC

En este sentido, se propone adicionar el parágrafo 3 al artículo 7a de la Resolución CRC 3128 de 2011 que se refiere al procedimiento de registro de IMEI, en el que se indique que a partir del 1° de agosto de 2016, solo se permitirá el registro en la BDA positiva de IMEI homologados.

Por cifras históricas respecto de los resultados mensuales del referido proceso, los cuales son reportados a la CRC[32], se ha identificado que en promedio, el nivel de respuesta de los usuarios que reciben el mensaje de texto y se registran dentro de los 15 días de plazo es del 30%. De acuerdo con el numeral 3.8 de la Resolución CRC 3128 de 2011, la obligación de notificación al usuario consiste en el envío de un mensaje de texto y el enrutamiento de los intentos de llamada, como mínimo durante 24 horas, el día previo al vencimiento del plazo a fin que el usuario se entere de la medida y evite ser bloqueado.

Por la anterior razón, se requiere mejorar y reforzar el procedimiento de notificación al usuario para reducir al máximo el impacto del bloqueo, la carga operativa que ello implica al operador y aumentar el nivel de registro en la base de datos positiva. En este sentido la propuesta para la notificación de este grupo de usuarios es la siguiente:

a. Envío del SMS (normal y flash) al día calendario siguiente a la detección del IMEI no registrado en BD positiva.

[32] De conformidad con la Resolución CRC 3496 de 2011, formato 42.

b. Desplegar un mensaje en banda[33] en los intentos de llamada originada por el usuario, como mínimo en 4 de los 20 días del plazo anunciado al usuario para registrar su equipo. El mensaje en banda debe realizarse durante las 24 horas de los días que el operador defina.
c. Enrutar a un IVR los intentos de llamada del usuario que hace uso del ETM, al menos 24 horas antes del plazo establecido, indicando que debe proceder al registro para evitar ser bloqueado.

3.3 Retiro de IMEI de la BDA Negativa

Teniendo en cuenta que van a ser ingresados nuevos tipos de bloqueo en la BDA Negativa, resulta necesario establecer cuando procede su retiro, teniendo en cuenta tanto el tipo de bloqueo que fue realizado como el IMEI sobre el cual se solicita.

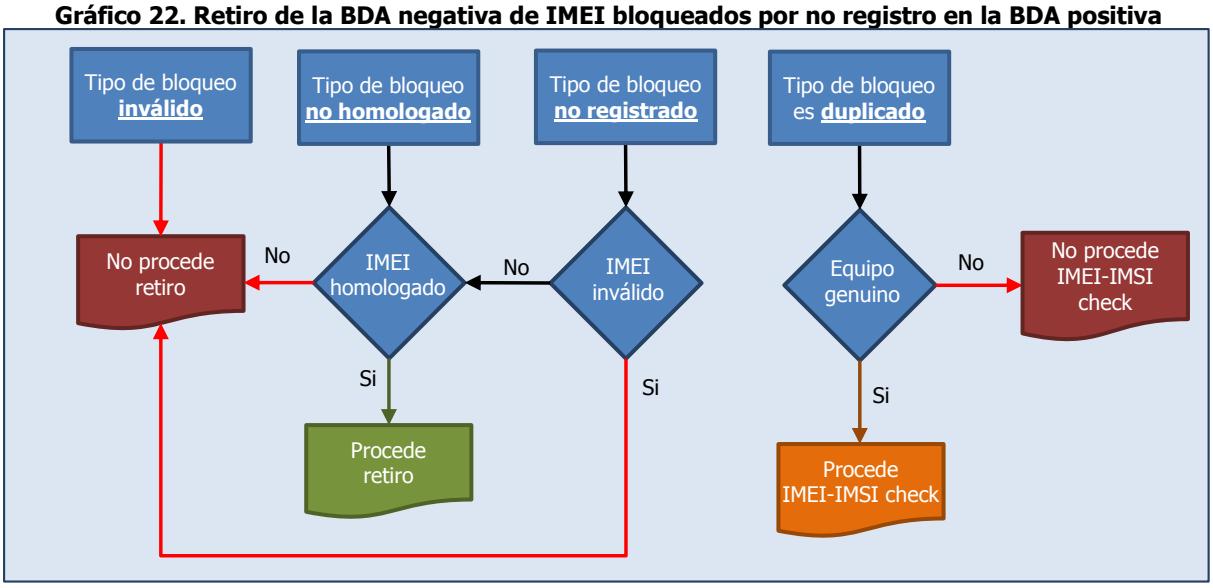
En este sentido, de acuerdo con lo desarrollado en los numerales anteriores, para el retiro de la BDA Negativa para los IMEI inválidos, los no homologados, los no registrados y los duplicados, se tiene en cuenta lo siguiente:

- Bloqueo por inválido: No procede el desbloqueo.
- Bloqueo por no homologado: Solo procede si el TAC del IMEI se encuentra en la lista de TAC de equipos homologados ante la CRC.
- Bloqueo por no registrado: Solo procede si el IMEI es válido y pertenece a un ETM que esté homologado, caso en el cual el usuario presenta ante su proveedor la declaración en la cual manifieste expresamente la adquisición legal de su ETM, mediante factura o a través del Anexo definido para tal fin.
- Bloqueo por duplicado: No procede el retiro del IMEI de la BDA Negativa. Sin embargo, se debe realizar la asociación de la pareja IMEI-IMSI válida a través de la funcionalidad descrita en el numeral 3.2.4 del presente documento para el caso de identificación de un equipo genuino.

Lo anterior puede observarse a continuación.

[33] Anuncio de voz que se realiza a la línea que origina una llamada antes de que la misma sea completada.

Gráfico 22. Retiro de la BDA negativa de IMEI bloqueados por no registro en la BDA positiva



Fuente: Elaboración CRC

4 PROPUESTAS ADICIONALES

4.1 Modificación del Parágrafo 1 del artículo 7a de la Resolución CRC 3128 de 2011

Atendiendo a las obligaciones de validación, verificación y control de equipos terminales dispuestas en el artículo 4 de la Resolución CRC 4813 de 2015, por la cual se establecen medidas de identificación de equipos terminales móviles dentro de la estrategia nacional contra el hurto de equipos terminales móviles; en la tercera etapa que se debe adelantar a efectos de garantizar que en las redes móviles operen equipos terminales que se ajusten a las condiciones técnicas de las mismas, hayan sido debidamente homologados, no hayan sido alterados y se encuentren registrados en la BDA (Base de Datos Administrativa administrada por el Administrador de la Base de Datos) positiva, esto es la Etapa de Control, los PRSTM deben desarrollar actividades a efectos de realizar la depuración de dichos terminales.

Ahora bien, tal y como dispone el numeral 4.3 del artículo en mención esta Entidad, debe definir las acciones relativas al condicionamiento o restricción de uso del terminal, las cuales al corresponder a la Etapa de Control deben ser aplicadas a partir del 1º de agosto de 2016.

En línea con lo anterior, el parágrafo 1 del artículo 11[34] de la Resolución CRC 4813 de 2015, dispuso que *"(…) A partir del 1° de agosto de 2016, solo se permitirá la prestación de servicios a los IMEI que hayan sido registrados antes de dicha fecha en la BDA Positiva, o que sean cargados como resultado del proceso de importación legal al país según lo estipulado en el Decreto 2025 de 2015 o el que lo sustituya, adicione o modifique. (…)"*

Respecto del Parágrafo en mención, fue formulada una propuesta por parte de la industria en el Comité Técnico de Seguimiento celebrado el 18 de marzo de 2016, según consta en su Acta 17, según el cual la CRC debe revisar el inciso segundo de dicho parágrafo atendiendo a que su interpretación puede ser de alto impacto para los usuarios y para los proveedores. En este mismo sentido Asomóvil mediante comunicación del 30 de marzo de 2016 solicitó a esta Entidad aclarar el alcance de dicho inciso, señalando que tal y como se encuentra redactado permite entender que, a partir del 1 de agosto de 2016, se tendrían que bloquear aproximadamente 12 millones de equipos.

De acuerdo con lo anterior, se reitera que, a partir del 1 de agosto de 2016, fecha en la cual tendrá lugar el inicio de la Etapa de Control descrita en el artículo 4 de la Resolución CRC 4813 de 2015, los PRSTM deben desarrollar actividades a efectos de realizar la depuración de los equipos terminales móviles detectados con IMEI inválidos, duplicados, no homologados y no registrados. Dichas actividades para condicionar o restringir el uso de dichos equipos, corresponden a las descritas en el acto administrativo que se soporta en el presente documento. Es así como es erróneo interpretar que a partir de dicha fecha los PRSTM tienen que bloquear de manera masiva equipos terminales.

Ahora bien, atendiendo a las inquietudes en cuestión, se procede a modificar el mismo, el Parágrafo 1 del artículo 7a de la Resolución CRC 3128 de 2011el cual quedará de la siguiente manera:

> *PARÁGRAFO 1. De no encontrarse dicho IMEI en la BDA positiva, para el proceso de registro el PRSTM deberá solicitar la prueba de adquisición del Equipo Terminal Móvil de acuerdo con lo establecido en la Resolución CRC 4584 de 2014, o una declaración del usuario titular de la línea en la cual manifieste expresamente la adquisición legal de su ETM, para cuyo efecto el formato utilizado será el establecido por la regulación vigente, el cual podrá validarse en medio físico o electrónico. Una vez almacenado dicho soporte, se podrá continuar con el proceso de asociación de datos.*
>
> *Para el caso de equipos ingresados al país en la modalidad de viajeros, de que trata el artículo 205 del Decreto 2685 de 1999, y los cuales no estén haciendo uso del Roaming Internacional, el usuario deberá presentar para el registro del IMEI en la BDA Positiva la factura de compra en el exterior ante el PRSTM con quien tiene contratados los servicios de telecomunicaciones.*

[34] Por medio del cual fue modificado el artículo 7ª de la Resolución CRC 3128 de 2011

4.2 Registro de IMEI para equipos terminales móviles importados

Atendiendo a la necesidad de reforzar e integrar los controles para disminuir el hurto de equipos terminales móviles en Colombia, fue expedido el Decreto 2025 de 2015, mediante el cual se establecieron medidas respecto del régimen de importación y exportación de dichos equipos. Es así como en su artículo 4 estableció el procedimiento que deben adelantar las personas naturales o jurídicas que importen terminales móviles, el cual incluye un registro policial de conformidad con el artículo 8 de la norma en mención y posteriormente, la consulta al Ministerio de Tecnologías de la Información y las Comunicaciones, quien adelantará una verificación de los IMEI de los respectivos terminales, lo cual permitirá posterior declaración ante la Autoridad Aduanera, que éstos sean incluidos en la Base de Datos Administrativa positiva.

De acuerdo con lo anterior, se evidencia como con el nuevo procedimiento establecido por el Decreto 2025 de 2015, los equipos terminales importados legalmente al país pueden ser incorporados a la Base de Datos Administrativa positiva, de una forma distinta a la consagrada en el artículo 7a de la Resolución CRC 3128 de 2011. Ahora bien, es necesario aclarar entonces, que el cumplimiento del procedimiento dispuesto en el Decreto en mención para la importación de equipos, no constituye el Registro de IMEI de que trata la referida Resolución, sino uno proceso de cargue de información en la Base de Datos.

Es así como resulta pertinente en aras de generar claridad respecto de estos dos trámites, establecer un nuevo campo en la Base de Datos positiva, en el cual se incorpore la identificación de la persona natural o jurídica que realizó la importación; lo cual permitirá diferenciar ésta de la identificación del propietario del equipo terminal, siendo esta última suministrada en el momento del Registro del IMEI, de acuerdo con el procedimiento dispuesto en el referido artículo 7a.

En línea con los argumentos previamente expuestos, se procederá a modificar el artículo 4 de la Resolución CRC 3128 de 2014, el cual contiene las obligaciones del Administrador de la BDA, adicionando un numeral al mismo, que disponga:

> "*Garantizar que en la BDA Positiva pueda diferenciarse la identificación de la persona natural o jurídica que realice la importación del equipo terminal móvil, de la identificación del propietario del mismo"*

Adicionalmente en aras de generar claridad y evitar que se confunda el procedimiento de cargue de información en la BDA Positiva de que trata el Decreto 2025, del Registro del IMEI dispuesto en el artículo 7a de la Resolución CRC 3128 de 2014, se modificará el inciso primero del artículo 8 de dicha Resolución, el cual quedará así:

> "***ARTÍCULO 8. REGISTRO DE IMEI EN LA BDA PARA EQUIPOS TERMINALES MÓVILES IMPORTADOS.*** *Los procesos de cargue y actualización a la BDA de la información de IMEI de equipos importados, iniciarán a partir de la implementación a través del ABD como parte del proceso de aduana y nacionalización de los equipos terminales móviles, proceso que será sustituido a partir de la adecuación del Sistema Informático de la DIAN para que contenga un*

campo codificado para el cargue de cada IMEI de los equipos que se importen legalmente al país.
(…)"

4.3 Modificación del numeral 4.5. del artículo 4 de la Resolución CRC 3128 de 2011

Atendiendo a la expedición del Decreto 2025 de 2015, mediante el cual se establecieron medidas respecto del régimen de importación y exportación de dichos los equipos terminales móviles, fue modificada mediante la Resolución 4813 de 2015, el numeral 4.5 del artículo 4 de la Resolución CRC 3128 de 2011, el cual consagra la obligación para el Administrador de la Base de Datos Administrativa de actualizar diariamente la información de IMEI contenida en la referida base de datos, en relación con los equipos importados legalmente a Colombia.

Ahora bien, de acuerdo con el artículo 13 del Decreto 2025 de 2015, el mismo entró en vigencia el día 1º de diciembre de 2015, por lo tanto, se procede a modificar el numeral 4.5 del artículo 4 de la Resolución CRC 3128 de 2011, el cual quedará así:

"*4.5. Actualizar diariamente la información de IMEI contenida en la BDA, con la información desagregada de los IMEI de los equipos que son importados legalmente al país, a partir del 1º de diciembre de 2015 de acuerdo con lo establecido en el Decreto 2025 de 2015 o el que lo sustituya, adicione o modifique."*

4.4 Inclusión de la delegación dispuesta en el artículo 18b de la Resolución CRC 3128 de 2011, en la Resolución CRC 2202 de 2009

Mediante el artículo 2 de la Resolución CRC 3584 de 2012, fue adicionado el artículo 18b a la Resolución CRC 3128 de 2011, a través del cual se delegó en el Director Ejecutivo de esta Comisión, la expedición previa aprobación del Comité de Comisionados, de los actos administrativos relacionados con la modificación de las condiciones de la implementación y operación de las Bases de Datos positiva y negativa.

Ahora bien, atendiendo a la facultad otorgada por el artículo 9 de la Ley 489 de 1998, según la cual las autoridades administrativas pueden delegar la atención y decisión de los asuntos confiados por la Ley y los actos respectivos, en los empleados públicos de los niveles directivo y asesor vinculados a la Entidad correspondiente; esta Comisión expidió la Resolución CRC 2202 de 2009, la cual contempla la totalidad de los asuntos cuya decisión han sido delegados en el Director Ejecutivo, previa aprobación del Comité de Expertos Comisionados de esta Entidad.

Es así, como en aras de brindar mayor claridad y que dicha norma compile todos los casos en que pueda presentarse la delegación descrita, se procede a incluir un literal en el artículo 1 de la Resolución CRC 2202 de 2009, el cual quedará así:

"l) La expedición de los actos administrativos en relación con la modificación de regulación expedida por la CRC relacionada con las condiciones de implementación y operación de las Bases de Datos Positiva y Negativa, y procedimientos de depuración e identificación de equipos terminales móviles en dichas bases de datos, en desarrollo de lo establecido en la Ley 1453 de 2011, y el Decreto 1630 de 2011, en ejercicio de las facultades legales otorgadas a la CRC."

4.5 Modificación del artículo 2 de la Resolución CRT 1596 de 2006

De conformidad con el Decreto 1078 de 2015[35], en su artículo 2.2.13.3.2, el cual compiló el artículo 9 del Decreto 2696 de 2014[36] las Comisiones deberán hacer públicas en su página web, con una antelación no inferior a treinta (30) días a su expedición, todos los proyectos de resoluciones de carácter general que pretendan expedir.

El parágrafo del mismo artículo señala que las Comisiones de Regulación deberán definir y hacer públicos los criterios, así corno los casos en que dicha publicación no serán aplicables a resoluciones de carácter general.

Es así, como atendiendo a dicho mandato esta Comisión, mediante la Resolución 1596 de 2006, mediante la cual definió los criterios y los casos en los cuales no resulta aplicable la publicidad de que trata el artículo 9 del Decreto 2696 de 2004 (compilado por el Decreto 1078 de 2015 para sus resoluciones de carácter general.

Ahora bien, por otra parte, la CRC al identificar la necesidad de establecer una instancia permanente de carácter consultivo que promueva la correcta implementación por parte de los proveedores de redes y servicios de telecomunicaciones móviles, en relación con las medidas adoptadas frente a las Bases de Datos Positiva y Negativa de que trata la Ley 1453 de 2011, mediante la Resolución CRC 3584, la cual adicionó el artículo 18a a la Resolución CRC 3128 de 2011, creó el Comité Técnico de Seguimiento (CTS).

Es así como el artículo 18a de la Resolución CRC 3128 de 2011, dispone que las propuestas que queden consignadas en las actas que se levanten con ocasión de cada sesión del CTS, serán estudiadas por la CRC para la construcción y elaboración de actos administrativos que puedan llegar a ser requeridos.

De conformidad con lo anterior la discusión que debe surtirse respecto de los actos administrativos de carácter general, se entiende cubierta en las sesiones que se adelantan en el CTS, en el cual los proveedores de redes y servicios de telecomunicaciones, presentan sus observaciones y sugerencias respecto de las posibles medidas que pretende adoptar la CRC frente a aspectos operativos y de implementación de las Bases de Datos Positiva y Negativa. De manera adicional, la presente propuesta

[35] *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*
[36] *"Por el cual se definen las reglas mínimas para garantizar la divulgación y la participación en las actuaciones de las Comisiones de Regulación"*

incorpora procedimientos de identificación y depuración de equipos terminales móviles en dichas bases de datos, por lo que se hace necesario incluir de manera expresa estos aspectos.

Atendiendo a lo previamente expuesto y a los principios dispuestos en el artículo 3 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, específicamente el principio de eficacia[37] y el principio de celeridad[38], se procederá a modificar el artículo 2 de la Resolución CRT 1596 de 2006, en el sentido de adicionar un numeral, el cual dispondrá:

> *"En la expedición de las resoluciones mediante las cuales se determinen condiciones para la implementación y operación de las Bases de Datos Positiva y Negativa, y procedimientos de depuración e identificación de equipos terminales móviles en dichas bases de datos, de acuerdo con lo ordenado por la Ley 1453 de 2011 y el Decreto 1630 de 2011, en ejercicio de las facultades legales otorgadas a la CRC."*

Lo anterior no obsta para que dichos actos administrativos deban dar cumplimiento al deber de información al público consagrado en el artículo 8 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

4.6 Modificación de la Declaración de único responsable del uso y propietario de equipos terminales móviles

El artículo 7a de la Resolución CRC 3128 de 2011, consagra el procedimiento de registro de IMEI, y dispone en su Parágrafo 1 que el proveedor deberá solicitar al usuario la prueba de adquisición del equipo terminal móvil o una declaración en la cual manifieste expresamente su adquisición legal, haciendo uso del formato dispuesto en el Anexo 1 de la Resolución CRC 4119 de 2013, lo cual podrá ser validado por el proveedor en medio físico o electrónico.

Es así como el Anexo 1 de la Resolución 4119 de 2013[39], contiene el formato de la Declaración de único responsable del uso y propietario de equipos terminales móviles, que debe ser empleado por el usuario para surtir el mencionado registro. Dicho formato incluye un campo para que el usuario propietario del equipo imponga su huella dactilar.

---

[37] *"(...) las autoridades buscarán que los procedimientos logren su finalidad y, para el efecto removerán de oficio los obstáculos puramente formales evitarán decisiones inhibitorias, dilaciones o retardos y sanearán, de acuerdo con esté código las irregularidades procedimentales que se presenten, en procura de la efectividad del derecho material objeto de la actuación administrativa"*

[38] *"(…) las autoridades impulsarán oficiosamente los procedimientos, e incentivarán el uso de las tecnologías de la información y las comunicaciones, a efectos de que los procedimientos se adelanten con diligencia, dentro de los términos legales y sin dilaciones injustificadas."*

[39] *"Por la cual se modifica en lo pertinente los artículos 3, 4, 7, 7a, 10 y 11 de la Resolución CRC 3128 de 2011"*

Ahora bien, de conformidad con el Decreto 19 de 2012[40] no se puede requerir la imposición de la huella dactilar en documentos, trámites, procedimientos o actuaciones que se surtan ante las entidades públicas y los particulares que cumplan funciones administrativas.

De acuerdo con lo anterior, será eliminado del formato denominado "Declaración de único usuario responsable del uso y propietario del (los) equipo (s) terminal (es) móvil (es)" contenido en el Anexo 1 de la Resolución CRC 4119 de 2013, el campo dispuesto para la imposición por parte del usuario propietario de su huella dactilar.

Adicionalmente, en aras de brindar mayor claridad y que dicho formato se encuentre en la norma que contiene las condiciones en que se debe llevar a cabo el procedimiento de registro de IMEI, el respectivo anexo hará parte integral de la Resolución CRC 3128 de 2011.

4.7 Factura de venta, comprobante de pago o declaración del usuario propietario

Tal y como se desarrolló en el acápite anterior, el usuario puede acreditar la adquisición legal del equipo presentado la Declaración de único responsable del uso y propietario de equipos terminales, contenida en el Anexo 1 de la Resolución 4119 de 2013.

Por otra parte, mediante la Resolución CRC 4584 de 2014 *"Por la cual se establece el Régimen de Autorizaciones para la Venta con fines comerciales de Equipos Terminales Móviles en Colombia",* se estableció en cabeza de las personas autorizadas para la venta al público de equipos terminales móviles, la obligación de entregar al comprador factura de venta o comprobante de pago, según corresponda a régimen común o simplificado, cumpliendo con los requisitos dispuestos en la normatividad tributaria.

De conformidad con lo anterior, y atendiendo a lo dispuesto en el Parágrafo 1 del artículo 7 a de la Resolución CRC 3128 de 2011, el usuario como prueba de la propiedad respecto del equipo terminal para realizar el registro del respectivo IMEI, puede presentar ante su proveedor la factura de venta, comprobante de pago o la declaración de único responsable del uso y propietario del equipo.

Ahora bien, atendiendo a que en distintas partes de la mencionada Resolución 3128 se hace mención al procedimiento de registro del IMEI, disponiendo en ocasiones que el usuario puede presentar la factura de venta, comprobante de pago o la declaración de único responsable de uso y propietario del equipo; y en otras ocasiones como prueba de la propiedad sólo se menciona la declaración en mención, esta Entidad considera necesario generar unidad de criterio respecto de los soportes que permiten evidenciar la adquisición o procedencia legal de los equipos terminales.

No obstante lo anterior, atendiendo a que la persona que adquirió el equipo terminal y que aparece en la factura o cuenta de cobro como comprador, puede no coincidir con la persona que pretende hacer el registro del respectivo IMEI, esto es con el responsable del uso del equipo, se requiere generar claridad

[40] *Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.*

que en caso que el usuario pretenda acreditar la propiedad del equipo presentado la factura o comprobante de pago, en esta debe constar su nombre como comprador; en caso contrario requiere presentar la declaración contenida en el Anexo 1 de la Resolución CRC 4119 de 2013.

De conformidad con lo previamente expuesto, se procederá a modificar las disposiciones que establecen los casos en que el usuario debe acreditar la propiedad o procedencia legal del equipo terminal, para llevar a cabo el registro del respectivo IMEI, permitiendo que dicha prueba corresponda a la factura o comprobante de pago cuando estos se encuentren a nombre del usuario que realiza el registro, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, que debe ser empleado por el usuario para surtir el mencionado registro en la Base de datos positiva.

Dichas disposiciones de la Resolución CRC 3128 de 2011, quedarán de la siguiente manera:

- **Artículo 3. Numeral 3.29.** *"Realizar el desbloqueo de los ETM que como consecuencia del proceso definido en el numeral 3.10 de la presente resolución se encuentren bloqueados y respecto de los cuales previamente el PRSTM haya verificado y autenticado el propietario del ETM bloqueado. Para que el PRSTM proceda al desbloqueo del ETM, el propietario del mismo deberá presentar la factura o comprobante de pago cuando estos se encuentren a su nombre, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución. Los ETM que se encuentren bloqueados por no registro por más de tres (3) meses, solo podrán ser desbloqueados por el PRSTM con la presentación física del equipo en los centros de atención al cliente del PRSTM o las oficinas del OMV, quienes deberán validar que el IMEI interno coincida con el IMEI externo"*

- **Artículo 7a. Parágrafo 1.** *"De no encontrarse dicho IMEI en la BDA positiva, para el proceso de registro el PRSTM deberá solicitar la factura o comprobante de pago, cuando estos se encuentren a nombre del usuario que realiza el registro, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución, la cual podrá validarse en medio físico o electrónico. Una vez almacenado dicho soporte, se podrá continuar con el proceso de asociación de datos.*

  Para el caso de equipos ingresados al país en la modalidad de viajeros, de que trata el artículo 205 del Decreto 2685 de 1999, y los cuales no estén haciendo uso del Roaming Internacional, el usuario deberá presentar para el registro del IMEI en la BDA Positiva la factura de compra en el exterior ante el PRSTM con quien tiene contratados los servicios de telecomunicaciones."

- **Artículo 11.** *"PROCEDIMIENTO PARA RETIRAR UN IMEI DE LA BASE DE DATOS NEGATIVA. Todo equipo terminal móvil que haya sido reportado como hurtado o extraviado, podrá ser excluido de las Bases de Datos Negativas previo recibo del reporte de recuperación del equipo, actividad que podrá realizar únicamente el PRSTM que incluyó dicho reporte en la base de datos negativa, dando cumplimento a lo establecido en el numeral 3.23a del artículo 3° de la presente resolución.*

Los equipos terminales móviles que hayan sido bloqueados como resultado del proceso establecido en el numeral 3.10 del artículo 3 de la presente resolución, y aquellos que hayan sido bloqueados por no registro a partir del 1° de agosto de 2016, podrán ser excluidos de las Bases de Datos Negativas y registrados en las Bases de Datos Positivas, para lo cual el PRSTM tendrá un plazo máximo de 60 horas continuas contadas a partir de que el usuario presente ante su proveedor, la factura o comprobante de pago, cuando estos se encuentren a su nombre, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución; y siempre que el IMEI pertenezca a un ETM que esté homologado.

Los equipos terminales móviles que hayan sido bloqueados como resultado del proceso de depuración de que trata el artículo 14b de la presente resolución, solo podrán ser excluidos de las Bases de Datos Negativas y registrados en las Bases de Datos Positivas, si el PRSTM que remitió el SMS comprueba que la SIM asociada a dicho equipo no tuvo tráfico de llamadas salientes de voz en los 30 días anteriores al bloqueo del equipo, y el propietario del mismo presente la factura o comprobante de pago, cuando estos se encuentren a su nombre, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución.

Las BDO negativas de los demás PRSTM deberán ser actualizadas de conformidad con la novedad de retiro del IMEI de la BDA negativa.

Para el reporte de retiro del IMEI de las BDO y la BDA negativas, el PRSTM y el ABD deberán proceder de manera inmediata con la actualización de la información en la BDA negativa por parte del PRSTM que recibió el reporte de recuperación del equipo o, la factura o comprobante de pago, cuando estos se encuentren a nombre del usuario que realiza el registro, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución. De igual forma, el PRSTM y el ABD deberán proceder con la actualización de la BDA negativa hacia las BDO negativas de los demás PRSTM, para que el desbloqueo del equipo terminal móvil se realice en un tiempo máximo de veinticinco (25) minutos contados a partir del momento en que el PRSTM informó a la BDA sobre el retiro del ETM. En los casos en los que se reciban varios reportes sobre un mismo IMEI provenientes de diferente PRSTM, el retiro de las bases de datos negativas no se producirá hasta tanto no se reciba el reporte de recuperación en todos los PRSTM donde el IMEI haya sido reportado por hurto o extravío."

- **Articulo 14b. Numeral 4.** "*Si dentro de los quince (15) días calendario contados a partir de la notificación de que trata el numeral 3 del presente artículo, el IMEI del equipo terminal móvil no ha sido registrado por el usuario en la base de datos positiva, el PRSTM deberá incluir en la BDA Negativa dichos IMEI.*

  Para el registro en la base de datos positiva de los IMEI notificados como probables inválidos, el PRSTM deberá solicitar la factura o comprobante de pago, cuando estos se encuentren a

nombre del usuario que realiza el registro, o la Declaración de único responsable del uso y propietario de equipos terminales móviles, contenida en el Anexo No. 1 de la presente Resolución.

En todo caso, los PRSTM no aceptarán el registro de un equipo cuyo IMEI contenga caracteres alfabéticos o una longitud menor a 14 dígitos numéricos."

4.8 Obligación del usuario de registro de equipo terminal móvil

Desde el año 2011 esta Entidad ha adoptado medidas con el objetivo de reducir las cifras de hurto de equipos terminales móviles en Colombia, es así como a través del registro de los equipos ingresados, fabricados o ensamblados legalmente al país, se busca que los equipos que sean reportados como hurtados y/o extraviados sean bloqueados y no puedan ser usados ni en Colombia ni en otros países.

Es así como mediante la Resolución CRC 3128 de 2011 se establecieron las condiciones y reglas de las bases de datos positivas y negativas para la restricción de los equipos reportados como hurtados y/o extraviados. En su artículo 3 (numerales 3.7, 3.8 y 3.10) impuso a los proveedores de telefonía móvil la obligación de informar a los usuarios cuyos equipos no se encuentren registrados en la base positiva, otorgándole un término de 15 días para proceder a dicho registro, y en caso que el usuario no lo haga procederá al bloqueo del respectivo equipo.

Lo anterior no obsta para que en caso que un equipo haya sido bloqueado por no registro, el proveedor deba proceder a desbloquearlo previa verificación y autenticación de la calidad de propietario del mismo, en los términos descritos en el acápite anterior, esto es presentando la factura o comprobante de pago cuando estos se encuentren nombre del usuario que realiza el registro, o la Declaración de único responsable del uso y propietario. Por lo cual una vez esto sea acreditado el proveedor cuenta con 60 horas para que dicho equipo sea retirado de las bases de datos negativas y registrado en las bases de datos positivas, salvo que este se encuentre duplicado, sea invalido o no se encuentre homologado.

Ahora bien, atendiendo a la importancia de la obligación de registro, la cual se encuentra en cabeza del usuario, esta Entidad considera necesario que la misma se encuentre contenida en el Régimen de Protección de los Derechos de los Usuarios de Servicios de Comunicaciones, actualmente contenido en la Resolución CRC 3066 de 2011, el cual de manera integral recoge el catálogo de derechos y obligaciones de los usuarios y los proveedores de servicios de comunicaciones, con ocasión de la prestación de dichos servicios.

Atendiendo a lo anterior, se procederá a adicionar de forma expresa dicha obligación en el respectivo artículo de la Resolución CRC 3066 de 2011, la cual como se explicó previamente, si bien ya se encuentra vigente en virtud del trámite dispuesto en la Resolución CRC 3128 de 2011, se incorporará en el Régimen de Protección de los Usuarios, generando claridad e integrando la totalidad de las obligaciones en cabeza de los usuarios.

Es así como se adicionará un nuevo literal al numeral 10.2 del artículo 10, el cual contiene las obligaciones de los usuarios, el cual dispondrá:

> *"Registrar ante su proveedor el equipo terminal móvil del cual haga uso para la prestación de los servicios contratados, cuando el mismo no haya sido adquirido con dicho proveedor"*

4.9 Nuevos tipos de bloqueo en la BDA Negativa

4.9.1 Bloqueo administrativo

Se han detectado casos de IMEI reportados en la BDA Negativa como hurtados o extraviados y que pueden obedecer a acciones de bloqueo que no necesariamente se originan en un usuario del servicio que ha sufrido el robo o extravío de su ETM, sino a situaciones en la que los PRSTM bloquean ETM como parte o resultado de sus procedimientos de detección y control de fraudes, gestión del riesgo o pérdida de equipos en sus inventarios o instalaciones que aún no han sido vendidos.

Dado que la estrategia del Gobierno Nacional contra el hurto elabora cifras e indicadores sobre el comportamiento del problema sobre los tipos de reporte de hurto principalmente y extravío, se hace necesario que los IMEI reportados en estos 2 tipos de bloqueo reflejen lo más fielmente posible situaciones de hurto a personas.

Por lo anterior, para que los PRSTM apliquen el bloqueo dentro sus procedimientos administrativos, sin que puedan llegar a mezclarse o confundirse con los tipos de bloqueo antes expuestos, y a fin que puedan mantener conciliadas las diferentes etapas de las BDA negativas[41], se propone crear un nuevo tipo de bloqueo denominado "administrativo", dirigido a distinguir, reportar y registrar los bloqueos por causas asociadas al fraude en telecomunicaciones de que son objeto los PRSTM.

Los bloqueos que por este nuevo tipo de reporte realicen los PRSTM deben estar debidamente sustentados y soportados con las respectivas evidencias de una defraudación a sus planes, servicios o procesos internos. Cabe anotar que en aquellos casos en que el proveedor de servicios determina que un equipo ha sido hurtado o extraviado en sus instalaciones o procedimientos internos (por ejemplo, transporte, bodegas, puntos de venta), debe reportarlo con este tipo de bloqueo, y debe estar soportado en la respectiva denuncia o informe interno de extravío.

4.9.2 Bloqueo de IMEI retirado de la BDA Negativa por tiempo de conservación

El artículo 4.20 de la Resolución CRC 3128 de 2011 estableció la obligación al ABD para retirar de las BDA Negativa los IMEI que cumplan unos periodos mínimos de permanencia en dicha base de datos en atención a la limitante en la capacidad del volumen de IMEI que soportan los EIR.

[41] Resolución CRC 3128, artículo 3º, numeral 3.6

De otro lado, los PRSTM tienen la obligación de bloquear y mantener por dichos periodos mínimos los IMEI con reporte en Colombia y en otros países[42], y aquellos que sean retirados luego de cumplido el tiempo mínimo serán remitidos por el ABD a todos los PRSTM para que estos verifiquen en el término de un (1) mes que dichos IMEI no están generando tráfico en la red.

En los casos en que el PRSTM encuentre que alguno de los IMEI retirados de la BDA Negativa se encuentra cursando tráfico, deberá proceder de manera inmediata al bloqueo del mismo en su EIR y envío a la BDA Negativa[43].

Frente a esta situación, si este tipo de IMEI es detectado con actividad, no deberá ser reportado en la BDA Negativa como hurtado o extraviado, sino que se propone que sea utilizado un nuevo tipo de bloqueo denominado "reincidente".

5 PARTICIPACIÓN DEL SECTOR

Atendiendo el procedimiento establecido en el artículo 2.2.13.3.2 del Decreto 1078 de 2015, los documentos publicados son sometidos a consideración del Sector a partir de su publicación por un lapso de 10 días hábiles. Los comentarios a la propuesta regulatoria serán recibidos a través del correo electrónico: medidas.hurto@crcom.gov.co, vía fax al (+57 1) 3198301, a través las redes sociales de la CRC en Twitter (@CRCCol) o en la página de Facebook "Comisión de Regulación de Comunicaciones", o en las oficinas de la CRC ubicadas en la Calle 59A Bis No. 5 – 53 Piso 9, Edificio Link Siete Sesenta, de la ciudad de Bogotá D.C.

No serán tenidos en cuenta los comentarios que se reciban respecto de disposiciones que no estén contenidas en la propuesta publicada.

[42] Res 3128, articulo 7,
[43] Res 3128, art 7, parágrafo 1

6 ANEXO

6.1 EXPERIENCIAS INTERNACIONALES EN BLOQUEO DE INVÁLIDOS

En el presente numeral se hace un resumen de las experiencias internacionales que han sido implementadas en algunos países para el control de equipos terminales móviles con IMEI inválido, no homologados o duplicados:

- En **Brasil**, el Sistema Integrado de Gestión de Dispositivos (SIGA), implementado para controlar equipos terminales móviles falsificados, clonados y no autorizados. El proyecto se basa en el marco regulatorio de ANATEL que establece que los operadores pueden únicamente permitir en la red los dispositivos autorizados. Está liderado por ANATEL con la participación de todos los actores relevantes (Regulador, operadores, ABR Telecom, fabricantes de dispositivos, GSMA, entre otros). El sistema es operado por ABR Telecom, la asociación de operadores de redes y servicios, y está activo desde 2014 recolectando información relevante de todas las redes móviles del país, y está generando reportes y alarmas necesarias para mapear el escenario brasileño de manera tal que el regulador pueda definir las próximas acciones. El sistema tiene como premisas: i) solución centralizada construida conjuntamente e integrada a todos los operadores móviles, ii) solución automatizada que permite la entrada de información con baja intervención humana, iii) escalable, dinámica y flexible que permite expandir el sistema y ajustar las reglas en el tiempo, iv) múltiples escenarios de información que comprende los CDR, sistemas de operadores y bases de datos internacionales, v) confiable y segura: minimiza impactos en usuarios finales.

- En **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. La Ley de las Comunicaciones categorizó los números de IMEI en listas blanca (registrados y no alterados), lista negra (perdidos, robados, alterados), lista gris (no en lista blanca ni negra, pero con comunicaciones autorizadas, los operadores deben analizar las llamadas de estos equipos e informar a ICTA y deben notificar al usuario con un SMS que no están en lista blanca) y lista blanca de números emparejados (números de IMEI clonados con el MSISDN del usuario del equipo genuino o que se define con base en aquel usuario cuyo equipo pagó impuestos de importación, tasa de registro del equipo en el sistema o por la fecha de inicio de la suscripción al servicio).

- En **Egipto**, con el objetivo de frenar la utilización de los teléfonos móviles con un número de IMEI ilegal, falso, inválido o clonado, combatir los robos de los teléfonos móviles, y afrontar los problemas de salud y de seguridad, la Autoridad Nacional de Reglamentación de las Telecomunicaciones (NTRA) estableció un sistema que 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 la cual alimenta la lista blanca de los operadores y es consultada en las solicitudes de conexión de un terminal móvil.

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. Frente a lo cual la primera acción adoptada fue el bloqueo en el país de todos los teléfonos que no poseían un número de IMEI.

- En **Kenya**, la Comisión de Comunicaciones estableció la obligación de homologación de todos los equipos terminales móviles, para de esta forma determinar que aquellos 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, y que estos debían ser desconectados a partir del 30 de septiembre de 2011.

  Al respecto, los operadores informaron al Gobierno sobre la desconexión de aproximadamente dos millones de teléfonos, ante lo cual el Gobierno determinó la conformación de 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 la sociedad civil.

  De esta forma, las normas adoptadas posteriormente estuvieron orientadas al 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.

- En **Sri Lanka**, la Comisión de Reglamentación de las Telecomunicaciones está impulsando desde marzo de 2013 el desarrollo de un registro central de identidad de equipos (CEIR), el cual se encontrará conectado con los EIR de todos los operadores móviles y permitirá identificar los IMEI no asignados por la GSMA, y los IMEI nulos, duplicados o todos ceros.

  Adicionalmente, el CEIR, entre otros, debe poder bloquear los servicios a los abonados con dispositivos registrados con números IMEI inválidos o incluidos en la lista negra, debe tener la capacidad de identificar números IMEI falsificados mediante su comparación con los IMEI suministrados por GSMA, y debe realizar una comprobación del formato del IMEI para verificar si su formato y rango son válidos.

- En **Ucrania**, la Comisión Nacional para la Reglamentación Estatal de las Comunicaciones e Informatización (NCCIR) creó en el año 2009 el Sistema de Información Automatizado para el Registro de los Terminales Móviles en Ucrania (AISMTRU), la cual permite que cuando se realiza

la conexión y se registra un terminal por primera vez en la red de uno de los operadores móviles, éste reenvíe 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".