



Comisión de Regulación
de Comunicaciones

REPÚBLICA DE COLOMBIA

**Condiciones regulatorias para el
control del uso de Equipos
Terminales Móviles hurtados y/o
extraviados y con alteraciones en
sus mecanismos de identificación -
Decreto 1630 de 2011**

**Documento Soporte
Atención al Cliente y Relaciones Externas**

Coordinador: Ricardo Ospina Noguera
Líder: Diana Paola Morales Mora

Fecha: Junio 21 de 2011



Libertad y Orden

TABLA DE CONTENIDOS

1	INTRODUCCIÓN	3
2	ANTECEDENTES.....	4
3	CONDICIONES PARA LA IMPLEMENTACIÓN DE LAS BASES DE DATOS POSITIVA Y NEGATIVA	6
3.1	CONDICIONES DE IMPLEMENTACIÓN DE LAS BASES DE DATOS DE CARA AL PRSTM	7
3.1.1	ESPECIFICACIONES TÉCNICAS PARA LA IMPLEMENTACIÓN DE LAS BASES DE DATOS.....	8
3.1.2	ADMINISTRADOR DE LA BASE DE DATOS – ABD.....	16
3.1.3	ALIMENTACIÓN DE LA BASE DE DATOS POSITIVA	19
3.1.4	ALIMENTACIÓN DE LA BASE DE DATOS NEGATIVA	27
3.1.4.1	Requisitos para los PRSTM.....	27
3.1.5	MECANISMOS PARA EXTRAER UN EQUIPO DE BASE DE DATOS NEGATIVA Y TRASLADARLO A LA POSITIVA.....	28
3.1.6	COMPARTICIÓN DE INFORMACIÓN DE LAS BASES DE DATOS NEGATIVAS CON FILIALES EN EL EXTERIOR.....	29
3.2	CONSIDERACIONES DESEDE LA PERSPECTIVA DEL USUARIO.....	31
3.2.1	Reporte de equipos terminales móviles hurtados y/o extraviados.....	32
3.2.2	Condiciones de activación de equipos terminales móviles	32
4	APLICATIVO PARA LA EXPEDICIÓN DE CERTIFICADOS DE HOMOLOGACIÓN EN LÍNEA.....	33
5	REGULACIÓN SOBRE LA AUTORIZACIÓN PARA LA VENTA DE EQUIPOS TERMINALES MÓVILES	35
5.1	DEFINICIÓN DE REQUISITOS PARA LA VENTA DE EQUIPOS TERMINALES MÓVILES.....	35
5.2	PROCEDIMIENTO PARA LA AUTORIZACIÓN POR PARTE DEL MINISTERIO DE TIC DE PERSONAS INTERESADAS EN LA VENTA DE EQUIPOS TERMINALES MÓVILES.....	37
5.3	PROCEDIMIENTO PARA LA AUTORIZACIÓN POR PARTE DE LOS PRSTM DE PERSONAS INTERESADAS EN LA VENTA DE EQUIPOS TERMINALES MÓVILES.....	38

CONDICIONES REGULATORIAS PARA EL CONTROL DEL USO DE EQUIPOS TERMINALES MÓVILES HURTADOS Y/O EXTRAVIADOS CON ALTERACIONES EN SUS MECANISMOS DE IDENTIFICACIÓN

1 INTRODUCCIÓN

De acuerdo al último informe publicado por la Superintendencia de Industria y Comercio (SIC), a primer trimestre del año 2011 se contaba en Colombia con un total de 45'421.094 líneas activas con los tres proveedores de redes y servicios móviles¹, lo cual representa a esa fecha un nivel de penetración² del 96% en el país.

Si bien este nivel de penetración, ubica a Colombia en una posición privilegiada, por encima de países como Canadá con una penetración de 72%, Perú con el 78%, México con el 81%, República Dominicana con 92%, USA con 96%, Venezuela con 96%, y por debajo de países como Brasil con una penetración de 105%, Ecuador con 107%, Chile con 125%, Argentina 129%, Uruguay 135% y Panamá con 165%³, también hace de Colombia un país donde la gran masificación de la telefonía móvil se encuentra asociada a algunos fenómenos delictivos, como es el caso del hurto de equipos terminales.

Según informes de ASOCEL⁴, en el año 2009 fueron hurtados 2,1 millones de terminales móviles en el país, cifra que, de acuerdo con los registros policiales, aumentó en 900.000 para 2010. Ahora bien, a pesar de los casi 3 millones de dispositivos hurtados en el 2010, de acuerdo a la información entregada por los Proveedores de Redes y Servicios Móviles, las cifras no son para nada comparables, al punto que Movistar informó a la Policía que recibió 170 mil solicitudes de bloqueo por hurto, Tigo 130 mil y por su parte Comcel no reportó datos sobre el particular.

De conformidad con lo anterior, es claro que si bien la regulación actualmente vigente contempla reglas⁵ tendientes a contar con información clara, actualizada y oportuna respecto de la identificación de los terminales que han sido reportados como extraviados y/o hurtados o desactivados por fraude, estas medidas de orden administrativo, no han sido suficientes para combatir el hurto de celulares ni las redes clandestinas de comercialización de equipos terminales móviles que por el contrario van presentando crecimiento en Colombia.

Ahora bien, ante el aumento indiscriminado de teléfonos móviles hurtados y la presencia de casos en los cuales los delincuentes han terminado con la vida de personas que han sido objeto del hurto de teléfonos celulares, el Gobierno Nacional expidió el Decreto 1630 de 2011 *"Por medio del cual se adoptan medidas para restringir la operación de equipos terminales hurtados que son utilizados para la prestación de servicios de telecomunicaciones móviles"*, el cual establece medidas legales y técnicas para restringir la utilización de equipos terminales móviles que han sido reportados como hurtados y/o extraviados en Colombia, entre las que se encuentra la implementación, consulta y mantenimiento de bases de datos negativas y positivas; la definición de unos requisitos exigibles a todo establecimiento comercial que tenga venta al público de Equipos Terminales Móviles; y el cumplimiento de unas condiciones mínimas que deberá tener en cuenta el comercializador en el momento de realizar la venta de todo terminal móvil.

¹ Cifras correspondientes a los proveedores **COLOMBIA MÓVIL S.A. E.S.P.**, **COMCEL S.A.** y **TELFÓNICA MÓVILES COLOMBIA S.A.**

² Número de cuentas móviles reportadas por operadores al final de año como porcentaje de la población total

³ www.pyr.com

⁴ Asociación de la Industria Celular en Colombia.

⁵ De acuerdo con el régimen de Usuarios, los proveedores deben constituir una base de datos de los terminales reportados como extraviados, robados o desactivados por fraude.

Dentro del mencionado Decreto, se establece que la Comisión de Regulación de Comunicaciones – CRC-, será la encargada de expedir las disposiciones regulatorias para el ejercicio de los derechos de los usuarios, así como la definición de aspectos técnicos y operativos derivados de las medidas establecidas en el citado decreto. Lo anterior, se precisa en el numeral 3° del Artículo 3° y en el Artículo 7° del mismo, en los siguientes términos:

“ARTÍCULO 3°. VENTA DE EQUIPOS TERMINALES MÓVILES EN COLOMBIA. (...)

Son personas autorizadas: (...)

3. *Cualquier persona que el Ministerio de Tecnologías de la Información y las Comunicaciones autorice, conforme a lo previsto en el artículo 4° del presente Decreto y a la regulación que para el efecto expida la CRC.”*

(...)

“ARTÍCULO 7°. BASE DE DATOS POSITIVA. (...)

iii) para el caso de los Equipos Terminales Móviles nuevos fabricados o ensamblados en el país, serán los fabricantes o ensambladores los responsables de registrar el IMEI de dichos equipos en la Base de Datos Positiva, de conformidad con la regulación que para este fin establezca la Comisión de Regulación de Comunicaciones”

Por otra parte, cabe mencionar que luego de la aprobación en la plenaria de la Cámara de Representantes en último debate y la respectiva conciliación de su texto por parte de la Comisión Conciliadora respectiva, el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara “*Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las Reglas sobre Extinción de Dominio y se dictan otras disposiciones en materia de Seguridad*”, se encuentra en espera de sanción presidencial.

En el citado proyecto de Ley sobre seguridad ciudadana, el legislador colombiano otorga a la Comisión de Regulación de Comunicaciones -CRC- la función de regular las condiciones para la elaboración de las bases de datos positiva⁶ y negativa⁷, condiciones que deberán ser establecidas regulatoriamente máximo tres (3) meses después de que la citada ley entre en vigencia.

El presente documento incluye consideraciones relativas a los antecedentes de la temática abordada, para luego exponer las condiciones para la implementación de las bases de datos negativa y positiva, y posteriormente se presentan consideraciones respecto de las condiciones específicas para la alimentación de las mismas. De igual modo, se incluyen los análisis relativos a las obligaciones de los proveedores de redes y servicios de telecomunicaciones móviles – en adelante PRSTM- y de los usuarios sobre el particular, así como también las condiciones para la solicitud de la autorización para la venta de equipos terminales móviles.

2 ANTECEDENTES

El gran auge y crecimiento de la telefonía móvil ha estado acompañado con el incremento considerable en el número de teléfonos hurtados, pero esto no sólo representa una cifra más en las estadísticas de hurto del país, sino que adicionalmente se ha evidenciado el crecimiento de un modelo de negocio que tiene como objetivo reintroducir en el mercado los Equipos Terminales Móviles que fueron hurtados. Es así como este *mercado ilegal* de Equipos Terminales Móviles se

⁶ Relación de los equipos terminales móviles identificados por su IMEI ingresados o fabricados legalmente en el país.

⁷ Relación de los IMEI de todos los equipos terminales móviles que han sido reportados como hurtados y/o extraviados en Colombia como en el exterior

nutre de equipos hurtados que posteriormente se manipulan para que puedan ser usados en la red de cualquier PRSTM, y de esta forma, los mismos reingresan a prestar su funcionalidad en el mercado lícito de la telefonía móvil.

A la fecha son numerosos los países de África, Latinoamérica y Europa que han adoptado medidas técnicas y jurídicas para acabar con el *mercado ilegal* de Equipos Terminales Móviles a los que se les ha alterado o duplicado el número de identificación del equipo terminal (IMEI – International Mobile Equipment Identifier, por su sigla en inglés).

De acuerdo con lo expuesto, con el fin de luchar contra esta práctica delictiva en el país, la cual además ha cobrado vidas humanas, se determinó la adopción de medidas para restringir la operación de Equipos Terminales Móviles hurtados, con la expedición del Decreto 1630 del 19 de mayo de 2011. En particular el artículo 9° del citado decreto define que es la Comisión de Regulación de Comunicaciones –CRC-, quien con base en sus facultades legales, expedirá la regulación que se requiera para la definición de aspectos técnicos y operativos derivados de las medidas adoptadas en el mismo.

En el mismo sentido, el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara "*Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las Reglas sobre Extinción de Dominio y se dictan otras disposiciones en materia de Seguridad*", adiciona en la Ley 1341 de 2009, la siguiente función a cargo de la CRC:

"21. Definir las condiciones en las cuales los operadores de comunicaciones, comercializadores y distribuidores deberán garantizar que las bandas de los terminales móviles estén desbloqueadas para que el usuario pueda activarlos en cualquier red, así como definir las condiciones y características de bases de datos, tanto positivas como negativas, que contengan la información de identificación de equipos terminales móviles, así como establecer las obligaciones de los proveedores de redes y servicios de comunicaciones, comercializadores, distribuidores o cualquier comerciante de equipos terminales móviles, y las relativas al reporte de la información de identificación de dichos equipos ante la CRC y al suministro de esta información a los usuarios. Las bases de datos de que trata el presente numeral, deberán ser implementadas y administradas de manera centralizada, a través de un tercero, por parte de los proveedores de redes y servicios de comunicaciones y la información consignada en dichas bases de datos tendrá carácter público, sin perjuicio de la información que contenga datos personales, la cual será protegida de conformidad con lo establecido por la ley".

Por su parte, el artículo 106 de la ley de seguridad ciudadana entrega a la CRC las siguientes funciones adicionales:

- Definir las condiciones para garantizar que las bandas de los terminales estén desbloqueadas.
- Definir las condiciones de las bases de datos positivas y negativas
- Establecer las obligaciones de los proveedores de redes y servicios, comercializados, distribuidores o cualquier comerciante de equipos.
- Establecer las obligaciones relativas al reporte de información.

Adicionalmente, el artículo bajo análisis dispone que las bases de datos tanto positiva como negativa deben ser implementadas y administradas de manera centralizada **a través de un tercero por parte de los proveedores de redes y servicios de telecomunicaciones.**

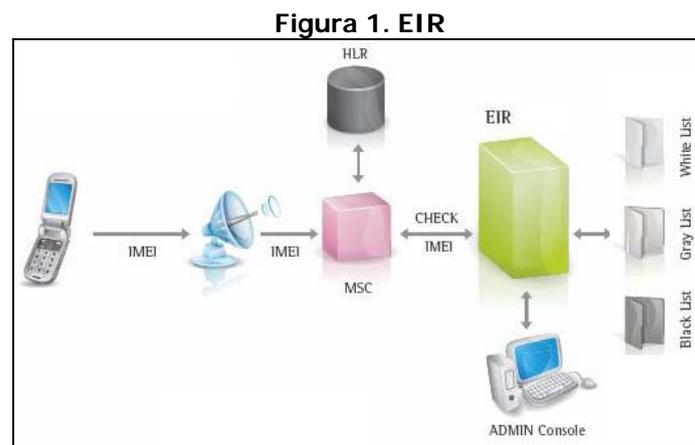
También, dispone que la información es pública y está sometida a las reglas de protección de datos personales.

En virtud de lo anterior, en esta ocasión se plantea la propuesta regulatoria de la CRC, en relación con las condiciones bajo las cuales los PRSTM deberán realizar la implementación, administración, operación y mantenimiento de las bases de datos a las cuales hace referencia el Decreto 1630 de 2011, además de la normatividad aplicable a los establecimientos de comercio que soliciten autorización ante el Ministerio de Tecnologías de la Información y las Comunicaciones -MINTIC- y el procedimiento que deben cumplir dichos comercializadores para acceder al certificado de homologación al realizar la venta de un Equipo Terminal Móvil.

3 CONDICIONES PARA LA IMPLEMENTACIÓN DE LAS BASES DE DATOS POSITIVA Y NEGATIVA

A nivel mundial existe una aplicación desarrollada en las redes GSM, conocida con el nombre de Equipment Identity Register -EIR-, la cual tiene como finalidad disminuir el riesgo de fraude en los equipos que son utilizados para la comunicación en la red de telecomunicaciones móviles.

Dentro del EIR se instala, configura y aprovisiona una base de datos, en la cual se almacena información referente al estado de los teléfonos móviles, indicando **i)** si dichos equipos pueden cursar tráfico en la red de telefonía móvil, **ii)** deben ser monitoreados por un lapso de tiempo o **iii)** están impedidos para cursar tráfico en la red.



FUENTE: <http://infotelecommil.webcindario.com/eir/EIR.pdf>

Es así, como en la base de datos del EIR existen tres listas de IMEI, denominadas así:

- a) Lista blanca, en la cual se encuentra la identificación de todos los Equipos Terminales Móviles que están autorizados para recibir y realizar llamadas a través de la red del operador.
- b) Lista gris, que identifica los equipos que pueden hacer y recibir llamadas, pero que además deben ser monitoreados para determinar la identidad del usuario.
- c) Lista negra, en la cual se establece la identificación de los equipos que no se encuentran autorizados para cursar tráfico en la red del operador móvil.

Ahora bien, una consulta a la base de datos del EIR permite determinar el estado del equipo (autorizado o no) para cursar tráfico, ya que éste es el encargado de informar a los demás nodos

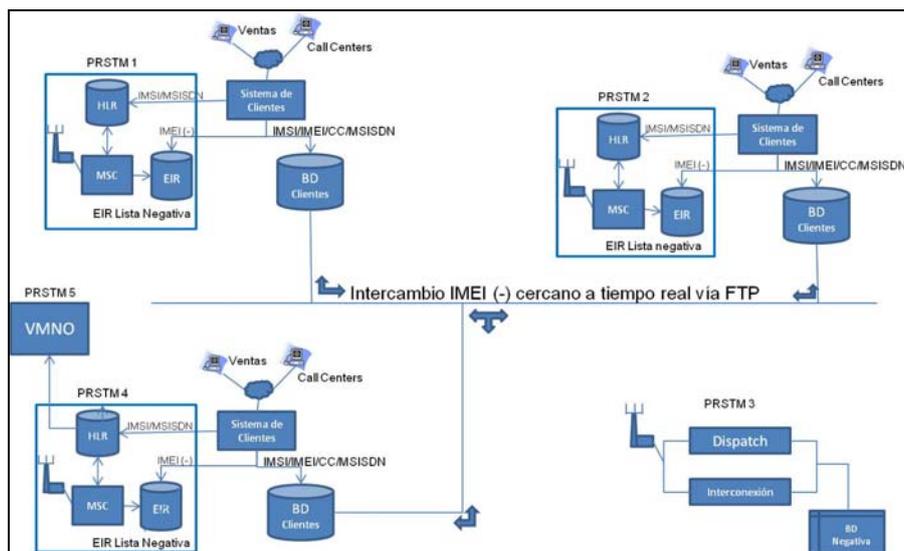
de la red de GSM (MSC⁸, HLR⁹, AuC¹⁰, VLR¹¹, SGSN¹²) si deben bloquear o no el tráfico que será cursado por la red.

En la siguiente sección se presenta la manera como opera actualmente el EIR en las redes de los PRSTM en Colombia, las propuestas de implementación de las bases de datos positiva y negativa, el modelo para el cargue y actualización de la información en dichas bases de datos considerando todos los actores (PRSTM, usuarios, importadores y fabricantes nacionales/ensambladores). Posteriormente, la sección 3.2 incluye las consideraciones de cara al usuario frente a la temática presentada.

3.1 CONDICIONES DE IMPLEMENTACIÓN DE LAS BASES DE DATOS DE CARA AL PRSTM

En la actualidad en Colombia operan cinco (5) PRSTM¹³ que ofrecen a sus usuarios servicios GSM, Acceso Troncalizado y UMTS. Cuatro de estos PRSTM cuentan con infraestructura de red, propia, la cual guarda ciertas diferencias en cuanto al reporte de hurto y/o extravío de equipos terminales móviles. Así, el PRSTM que ofrece servicios de Acceso Troncalizado maneja la información de reporte de quipos hurtados y/o extraviados dentro de su propia red, mientras que los demás cuentan con el EIR como entidad funcional dentro de su propia red e intercambian la información de equipos hurtados y/o extraviados.

Figura 2. Situación actual intercambio listas negativas



FUENTE: Elaboración propia

⁸ Mobile Switching Center. Central de conmutación celular del PRSTM.

⁹ Home Location Register. Base de datos en la central celular donde se almacenan los datos de la línea del cliente y registra su última ubicación.

¹⁰ Authentication Center.

¹¹ Visitor Location Register.

¹² Servidor para la conmutación de paquetes.

¹³ COLOMBIA MÓVIL S.A. E.S.P., COMCEL S.A., TELEFÓNICA MÓVILES COLOMBIA S.A., Avantel S.A y UFF móvil.

Como se expresó en el numeral anterior, si bien el EIR tiene la funcionalidad de manejar tres listas independientes (lista negra, lista gris y lista blanca), en Colombia, de acuerdo a la tecnología implementada a la fecha, los PRSTM sólo manejan la lista negra de sus EIR (Base de datos negativa) para hacer el bloqueo de los IMEI reportados como hurtados/extraviados, provisionando los registros en línea desde sus sistemas de información de clientes, con el evento del reporte de sus usuarios, pero ninguno hace uso de la lista blanca (Base de datos positiva) implementada en el EIR.

Adicionalmente y en cumplimiento a la normatividad establecida por la CRC¹⁴ y la Superintendencia de Industria y Comercio¹⁵, los tres PRSTM tienen implementado un intercambio de IMEI reportados como hurtados y/o extraviados por los usuarios, intercambio que se realiza en un periodo de tiempo comprendido entre 5 y 25 minutos, y que debe ser auditado a través de mecanismos externos a la compañía¹⁶.

En ese sentido, pareciera que el bloqueo efectuado por el EIR a los IMEI que han sido reportados como hurtados y/o extraviados y que son incluidos en la base de datos negativa del PRSTM es efectivo, toda vez que la central de telefonía móvil valida en tiempo real el IMEI de los equipos que intentan cursar tráfico en la red, comparándolos con la lista negra o base de datos negativa y, tras dicho proceso, en caso que el IMEI del Equipo Terminal Móvil se encuentre reportado en la base de datos negativa, no se le permite cursar tráfico por la red del PRSTM.

Además, el intercambio entre proveedores de los IMEI reportados como hurtados y/o extraviados genera dos bloqueos: **i)** no permite el uso del equipo terminal móvil a nivel de la red en ninguno de los tres PRSTM una vez es recibido e incluido el IMEI en cada EIR, y **ii)** no permite que en los puntos de venta o de atención a clientes se active el equipo terminal móvil en una línea nueva.

No obstante los controles llevados a cabo por los PRSTM en relación con los equipos terminales móviles que son reportados como hurtados y/o extraviados, el intercambio constante de equipos y el bajo índice de reporte de equipos hurtados y/o extraviados por parte de los usuarios, han propiciado que la medida de implementación de la base de datos negativa no se constituya en una herramienta completa y/o suficiente para frenar el hurto de Equipos Terminales Móviles -ETM-, ya que existe un *mercado ilegal* de dichos equipos, a los cuales se les ha alterado o duplicado el IMEI, siendo esta situación totalmente inadvertida en el proceso de autenticación del equipo en la red móvil¹⁷.

3.1.1 ESPECIFICACIONES TÉCNICAS PARA LA IMPLEMENTACIÓN DE LAS BASES DE DATOS

De acuerdo con el análisis presentado en el numeral anterior, es necesario complementar las medidas adoptadas en la actualidad por los PRSTM para evitar que los ETM no autorizados cursen tráfico en la red de telefonía móvil. Sobre el particular, el Gobierno Nacional a través del Decreto 1630 de 2011 estableció en el artículo 5° la obligación de implementación de las bases de datos indicando que “[l]os PRSTM deberán realizar la contratación y asumir los costos de implementación,

¹⁴ Artículo 107, Resolución 1732 de 2007

¹⁵ CIRCULAR ÚNICA de la SIC, Capítulo Activación de abonados, TITULO III, capítulo 2, numeral 2.6.

¹⁶ La obligación de compartir la base de datos será aplicable a los operadores que utilicen sistemas de acceso troncalizado, Trunking, cuando los equipos terminales usados para la provisión de dichos servicios, puedan ser utilizados en las redes de los operadores de TMC y PCS.

¹⁷ A manera de referencia, cabe anotar que en la actualidad las redes realizan procesos de autenticación de la SIM y de verificación de que el equipo no está en la lista negra. Esto último es conocido como “autenticación del equipo”, y es lo que menciona el Decreto 1630 de 2011.

administración, operación y mantenimiento de un sistema centralizado que soporte las bases de datos positiva y negativa, (...)". En ese sentido, la Comisión procederá a definir las opciones de modelos a realizar para la implementación de las bases de datos tanto positiva como negativa, evidenciando en cada una de las opciones las ventajas y desventajas asociadas a su implementación y utilización.

3.1.1.1 Modelos técnicos para implementar las bases de datos positiva y negativa

El artículo 5° del Decreto 1630 de 2011, establece: *"Los PRSTM deberán realizar la contratación y asumir los costos de implementación, administración, operación y mantenimiento de un sistema centralizado que soporte las bases de datos positiva y negativa (...)"* y adicionalmente el artículo 9 deja en función de la CRC expedir la regulación que sea requerida para la definición de los aspectos técnicos y operativos, derivados de las medidas establecidas en el citado decreto

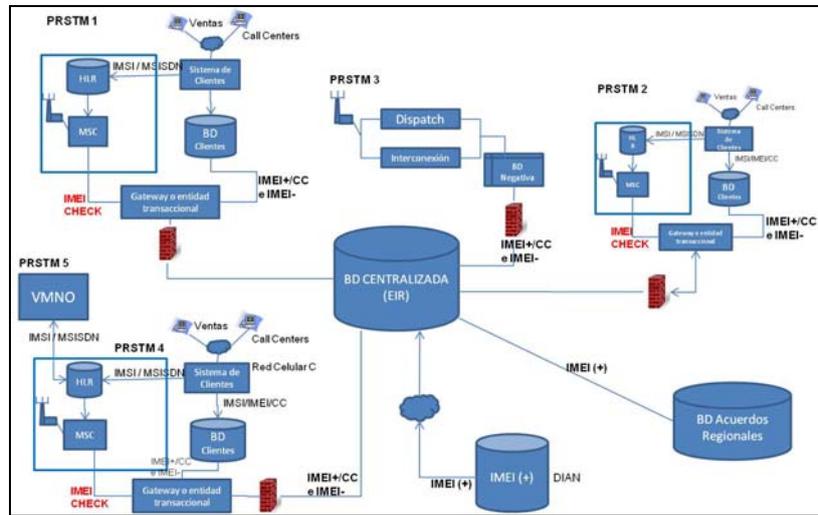
En ese sentido, es claro para la Comisión que la obligación del sistema centralizado ya fue definida en el decreto, y ahora es obligación de la CRC establecer cuál es el modelo técnico-operativo más apropiado para realizar la centralización de la información, la cual permitirá realizar el intercambio de información y efectuar las consultas necesarias tendientes a restringir el uso de Equipos Terminales Móviles hurtados y/o extraviados en la red de los PRSTM.

Así las cosas y a efectos de definir el modelo que mejor se adapte al estado actual de las redes de telefonía móvil, y que sea coherente con el objeto establecido en el Decreto 1630 de 2011 varias veces referido en el presente documento, a continuación se presentan tres (3) opciones de implementación y validación centralizada, enfatizando las respectivas implicaciones técnicas y operativas, así como el proceso de compartición a nivel internacional de la información de IMEI reportados -luego de la suscripción de los acuerdos correspondientes-, y los potenciales riesgos que se pueden presentar, para finalmente poder concluir con el modelo que representa la mejor opción en el cumplimiento del objeto establecido en el Decreto 1630 de 2011.

3.1.1.1.1 Opción 1. Sistema centralizado

En esta primera opción de implementación de bases de datos positiva y negativa, se establece la obligación de que exista un único sistema central, que almacenaría tanto la base de datos positiva como la base de datos negativa, con lo cual los PRSTM estarían obligados a realizar todo tipo de validación hasta las bases de datos centralizadas.

Figura 3. Opción 1. Centralización de la validación



FUENTE: Elaboración propia

A. Implicaciones técnicas:

- La base de datos centralizada permite realizar el proceso de validación de las condiciones de los equipos –habilitados o no para su funcionamiento–, según los procedimientos establecidos al interior de cada uno de los PRSTM.
- La base de datos centralizada debe ser un EIR, con el fin de mantener la funcionalidad de las listas positiva y negativa y el protocolo con los MSC/SGSN.
- Se requiere que el MSC del PRSTM permita la conexión con un tercero (BDA – Base de Datos Administrativa), lo cual implica acuerdos, máxima seguridad en redes e interconexión, etc.
- Podrían verse afectados los indicadores de grado de servicio de los PRSTM, toda vez que la consulta de las bases de datos negativa y positiva implicaría que los PRSTM accedieran a la base de datos centralizada, con lo que se podrían presentar tiempos de respuesta mayores.
- La infraestructura de EIR de cada PRSTM podría quedar fuera de servicio, y en esa medida no sería necesario mantenerla. .

B. Implicaciones operativas

Al ser el sistema centralizado el único centro de validación, se tendría una carga bidireccional de IMEI positivos, número de identificación del usuario e IMEI negativos, tanto para equipos y/o usuarios nuevos como sus actualizaciones.

C. Acuerdos Internacionales:

Futuros acuerdos regionales implicarían, por una parte, la implementación de un sistema que reúna a los países participantes y, por otra parte, conectar varias bases de datos centralizadas y/u operadores directamente. Esto en razón a que la base de datos de IMEI administrada por GSMA sólo permite la conexión con operadores miembros de tal asociación, y no conecta con terceras bases de datos centralizadas de países o regiones.

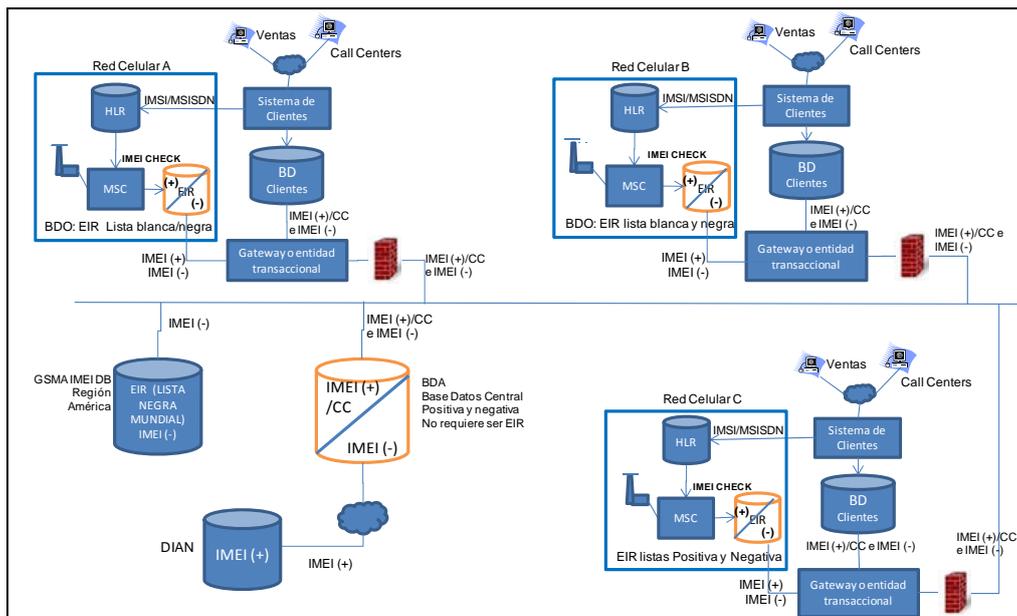
D. Riesgos

- Posibles sabotajes informáticos, físicos o a las interconexiones, toda vez que se requiere ingresar a la misma cada vez que sea necesario validar un terminal.
- Los equipos terminales hurtados y/o extraviados seguirían cursando tráfico en la red de los PRSTM puesto que, una vez son bloqueados, es posible que les alteren nuevamente el IMEI en el *mercado ilegal*, utilizando un IMEI que se encuentre incluido en la base de datos positiva (es sencillo calcular un IMEI válido, o el mismo cliente podría suministrarlo) y debido a que en el protocolo de autenticación no es posible verificar la cédula del usuario, el único dato identificable correspondería al IMEI.

3.1.1.1.2 Opción 2. Base de datos administrativa y base de datos operativa con validación de IMEI

La segunda opción define una base de datos administrativa (BDA), la cual funcionaría como un repositorio de toda la información que deberá ser almacenada de manera centralizada en una base de datos positiva y una base de datos negativa, y adicional cada PRSTM tendrá una base de datos operativa (BDO) la cual debe ser consultada de conformidad con lo establecido en el numeral 3.1.1.2.1. Adicionalmente, en este modelo solo se establece la verificación del IMEI en los procesos de validación.

Figura 4. Opción 2. BDA / BDO, SOLO IMEI CHECK



FUENTE: Elaboración propia

A. Implicaciones técnicas:

- Cada PRSTM deberá habilitar en su EIR la lista blanca para validación de los IMEI positivos.
- Cada PRSTM continuará usando su EIR y llevará a cabo las validaciones de IMEI en sus bases de datos positiva y negativa (lista blanca y lista negra) localmente, con lo que no se verá afectado su grado de servicio.

- La Base de Datos Administrativa –BDA- se usará para almacenar los IMEI de los equipos que han ingresado legalmente al país, es decir todos aquellos que serán utilizados para realizar activaciones nuevas o realizar cambios de equipo en una línea ya activa en el PRSTM. Así mismo será empleada para almacenar los IMEI reportados como hurtados y/o extraviados, los cuales son reportados o retirados por un PRSTM. A partir de ahí se debe actualizar el evento en todos los PRSTM.
- La BDA deberá ser implementada, administrada y mantenida por un tercero, previo acuerdo de los PRSTM.
- Esta distribución no permite que el MSC quede expuesto a una conexión con un tercero.

B. Implicaciones operativas

- La verificación de los equipos (transacciones críticas en tiempo) se continúan realizando al interior de la red de cada PRSTM, mientras que la actualización con los estados y controles de la BDA se llevará a cabo en línea. Esto permite reducir las exigencias en interconexión, volumen de información a intercambiar, maximizar las seguridades y por ende beneficia tiempos y costos de implementación.
- El usuario debe informar al PRSTM cada vez que cambie de equipo, a efectos del que el nuevo IMEI haga parte de la lista blanca del EIR y se le permita cursar tráfico en la red.

C. Acuerdos Internacionales/Regionales.

Permite usar los beneficios ofrecidos en la GSMA¹⁸, los cuales no consideran ningún costo adicional, dado que cada operador teniendo su EIR puede conectarse a la base de datos de IMEI administrada por GSMA para establecer un hosting virtual a un grupo de países o regiones. De esta forma, se agiliza el intercambio entre filiales y no filiales independiente y sin perjuicio de las normas y acuerdos a ser promulgados.

D. Riesgos/costo

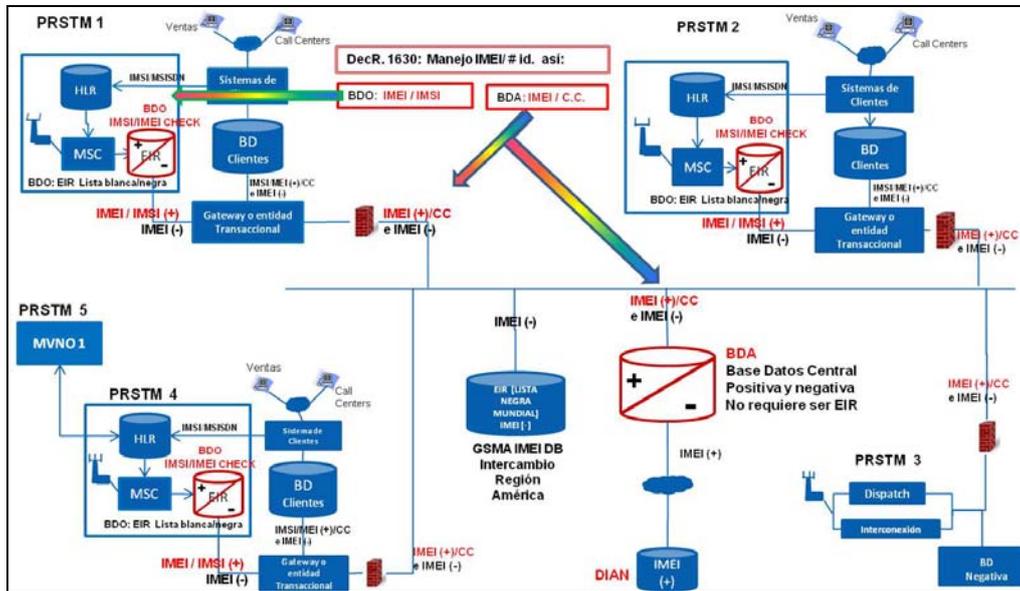
Los equipos terminales hurtados y/o extraviados seguirían cursando tráfico en la red de los PRSTM, debido a que una vez son bloqueados, en el *mercado ilegal* les alterarían nuevamente el IMEI, utilizando un IMEI que se encuentre incluido en la base de datos positiva (es sencillo calcularlo o el mismo cliente lo suministra) y debido a que en el protocolo de autenticación no es posible verificar la cédula del usuario el único dato identificable correspondería al IMEI.

3.1.1.1.3 Opción 3. Base de datos administrativa y base de datos operativa con validación de IMEI - IMSI¹⁹

¹⁸ Este tema se define con detalle en el numeral 3.1.5 del presente documento.

¹⁹ Identificador Internacional de Abonado Móvil.

Figura 5. Opción 3. BDA / BDO, IMEI – IMSI CHECK



FUENTE: Elaboración propia

La tercera opción, al igual que la anterior, define una base de datos administrativa (BDA), la cual se emplearía para almacenar toda la información que deberá ser almacenada, y adicionalmente cada PRSTM tendrá una base de datos operativa -BDO- que será consultada de conformidad con lo establecido en el numeral 3.1.1.2.1. Como punto adicional, en este modelo se establece la verificación de la pareja IMEI- IMSI ²⁰.

El IMSI es la Identidad Internacional de un Suscriptor o Abonado Móvil, el cual se asigna por el PRSTM a cada usuario cumpliendo un estándar internacional, es único para dicho usuario en el mundo y se almacenada en la SIM (Subscriber Identity Module, en el sistema GSM la tarjeta electrónica o chip que se inserta en el equipo o teléfono móvil). El IMSI forma parte del proceso de autenticación del servicio móvil y por lo tanto, es manejado con máxima seguridad entre la estación móvil (MS o Mobile Station, que es el conjunto de SIMcard y el equipo) y la central celular (MSC o Mobile Switching Center), para evitar la clonación de la SIM o del servicio y el uso por parte de terceros ajenos al suscriptor o abonado.

El IMSI y el IMEI se diferencian en que mientras el primero distingue unívocamente al usuario, el segundo distingue unívocamente el equipo usado por éste.

Para el presente caso, las implicaciones técnicas y operativas sólo se modifican teniendo en cuenta que, en esta opción la validación que lleva a cabo el EIR corresponde a la de la pareja IMEI – IMSI.

Por otra parte, entre los beneficios y riesgos, cabe anotar que los equipos hurtados y/o extraviados dejarían de cursar tráfico en las redes de los operadores móviles, ya que en el evento en que se altere un IMEI de un equipo hurtado y/o extraviado con un IMEI valido que se encuentre en la base de datos positiva e intente usarse con una SIM activa de cualquier operador, ya no tendría servicio

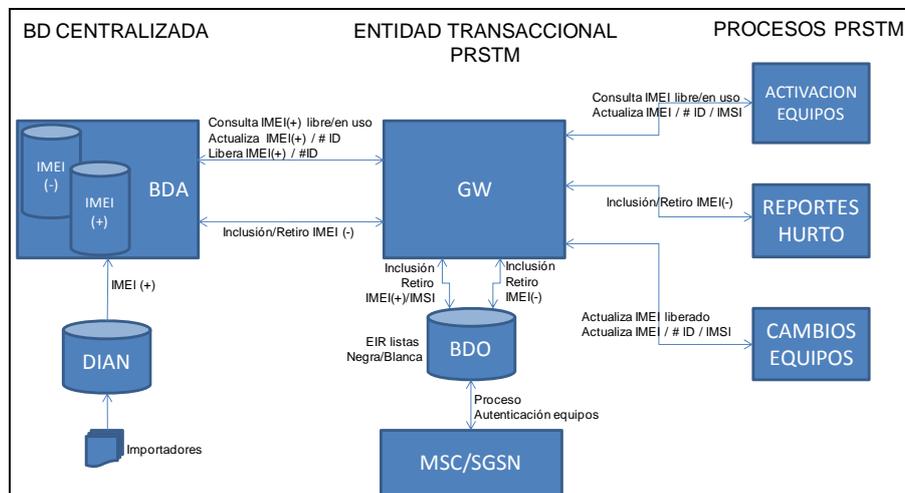
²⁰ Código Internacional de Identificación de Usuario Móvil (International Mobile Subscriber Identity)

puesto que la red accedida verificará el par IMEI/IMSI en el EIR lista blanca (BDO positiva) emitido por el equipo hurtado alterado y al no coincidir no será permitido su conexión a dicha red.

De este modo, y de conformidad con los análisis realizados al interior de la CRC, en cumplimiento de las obligaciones encomendadas en el Decreto 1630 de 2011 se encuentra pertinente la implementación del modelo especificado en el numeral 3.1.1.1.3 -Opción 3-, toda vez que dicho modelo propicia el escenario más completo de restricción para el funcionamiento de equipos terminales móviles hurtados y/o extraviados o con alteraciones en sus mecanismos de identificación, lo cual guarda coherencia con el espíritu de la normatividad definida por el Gobierno Nacional en el Decreto 1630 de 2011.

3.1.1.2 Responsabilidades técnicas de los PRSTM para el intercambio de información con la BDA y la BDO.

Figura 6. Modelo de consulta a la BDA y BDO



FUENTE: Elaboración propia

De acuerdo al modelo identificado como el que mejor lograría el cumplimiento de los objetivos de la presente propuesta regulatoria y considerando que el mismo debe beneficiar a los usuarios, quienes son los directamente afectados con el aumento indiscriminado en el número de Equipos Terminales Móviles hurtados y/o extraviados, es importante recordar que como bien lo indica el Decreto 1630 de 2011, los PRSTM tienen la responsabilidad de realizar todas las adecuaciones necesarias al interior de su red para garantizar que la consulta a las bases de datos negativa y positiva se realice, tanto en cada proceso definido en el numeral 3.1.1.2.1., como en la activación de una línea nueva.

Adicionalmente, los PRSTM deberán disponer de los equipos y medios de transmisión necesarios y suficientes para la comunicación con la BDA, con el fin de que en cada proceso de activación o cambio de equipo que solicite el usuario, el PRSTM consulte la BDA Positiva y valide que el IMEI se encuentre en la lista de IMEI positivos en estado libre (validando así que fue legalmente importado/adquirido y no tiene ningún número de identificación asociado) y que no esté en la BDA negativa.

Además de los procesos de validación de los datos en la BDA, a los que hace referencia el acápite anterior, se deben realizar las siguientes verificaciones:

- Cuando el usuario adquiere una nueva línea con un nuevo equipo en el PRSTM, o lleva el equipo para comprar una línea nueva o para cambiar el equipo de la línea ya activa, el PRSTM verifica que el equipo traído por el cliente no tenga alteración en el IMEI, y no esté en la base de datos negativa de la BDO (consulta a su EIR lista negra).
- Finalizado el proceso de venta o cambio de servicio para equipos comprados en el PRSTM o llevados allí por el usuario, el IMEI queda asociado a un número de identificación (CC, CE, NIT), el cual tiene que ser actualizado por el PRSTM en la BDA positiva.

Los PRSTM deberán disponer de los medios necesarios para mantener actualizada la BDO, a partir de la información contenida en la BDA, y garantizar la integridad de la información contenida en la BDO y el adecuado funcionamiento de las interfaces para el intercambio de información con la BDA. Para efecto de la actualización de la BDO a la BDA, el ABD y el PRSTM deberán establecer periodos fijos de actualización en las horas de menor tráfico.

3.1.1.2.1 Procesos de consulta de las bases de datos por parte del PRSTM

De acuerdo con los procedimientos de seguridad establecidos en una red GSM la unión del Equipo Terminal Móvil con la tarjeta SIM, conocida como "estación móvil" (MS), es decir la dupla IMEI²¹ – IMSI²², se actualiza en los siguientes eventos:

- Conexión/desconexión a la red.
- Cambio de área de cobertura del MSC.
- Actualización periódica de la localización.

Ahora bien, para el cumplimiento de la obligación establecida en el párrafo tercero del artículo 5° del Decreto 1630, el cual establece que "*(...) [l]as consultas a las bases de datos positiva y negativa deberán ser realizadas por los PRSTM al momento de la activación de un Equipo Terminal Móvil y cada vez que el equipo realice el proceso de autenticación en la red*", es importante resaltar que el PRSTM deberá realizar la consulta a la BDA (bases de datos positiva y negativa), en todos los procedimientos que tengan como objetivo la activación inicial de un nuevo usuario en la red móvil, cuando medie solicitud de cambio de equipo terminal móvil con la línea activa o cuando es el operador receptor de un proceso de portabilidad.

Adicionalmente, se deberá cumplir con la consulta a la BDO (bases de datos positiva y negativa), cada vez que se presente un proceso de registro tras la desconexión/conexión a la red de telefonía móvil, es decir, cada vez que el usuario realice el apagado y encendido de su MS, de acuerdo con lo establecido en la Recomendación GSM 03.12²³.

Durante el proceso de conexión (attach), el MS debe enviar un mensaje a la red para conectarse, dicho mensaje servirá para dar inicio a la consulta en la BDO (base de datos positiva y negativa),

²¹ IMEI: TAC: Type Approval Code (6 dígitos)
 FAC: Factory Assembly Code (2 dígitos)
 SNR: Serial Number (6 dígitos)
 SP Spare (1 dígito)

²² IMSI: MCC: Mobile Country Code (3 dígitos)
 MNC: Mobile Network Code (2 dígitos)
 MSIN: Mobile Subscriber Identification Number (10 dígitos)

²³ Digital celular telecommunication system. Location registration procedures.

de la misma forma durante la desconexión (detach) el MS envía a la red un mensaje que le indica que debe suprimir la inscripción en el respectivo VLR.

El proceso de apagado/encendido de un MS se encuentra conformado por las siguientes fases:

1. La MS realiza un barrido de portadoras para seleccionar la más fuerte, proceso que es conocido como barrido de frecuencias.
2. La MS intenta extraer en el intervalo 0 los canales BCH²⁴, de no ser posible se intenta con la siguiente portador en intensidad.
 - Cuando se detectan los canales anteriores se decodifican las señales de control de frecuencia y temporización FCCH²⁵ y SCCH²⁶.
 - Mediante la recepción del BCCH²⁷ se determina si la transmisión captada pertenece al operador deseado.
 - MS extrae del BCCH el código de Identificación del Área de cobertura de la MSC.
3. El MS envía hacia la BTS el código del Área de Localización y un mensaje de petición de registro, incluido el IMSI/TMSI²⁸.
 - El mensaje se encamina hacia la MSC asociada.
 - La MSC le comunica al VLR la activación de la MS y registrará su Área de Localización.
 - Cuando la MS es nueva en ese VLR, éste procede a comunicarle al HLR correspondiente analizando su IMSI.
4. Se realiza el proceso de Autenticación.
5. Se le informa a la MS de la correcta realización del proceso
6. Por el canal BCCH se transmite la lista de frecuencias BCCH de las estaciones vecinas, con el fin que la MS realice el monitoreo de las condiciones de recepción de dichas frecuencias.

De acuerdo con lo anterior, durante el paso tres (3) antes mencionado, en el cual se realiza la petición de registro, se debe hacer la consulta a la BDO/EIR (base de datos positiva y negativa), con el fin de determinar el estado de autorizado o no del equipo para cursar tráfico, ya que es el EIR el encargado de informar a los demás nodos de la red de GSM si deben bloquear o no el tráfico que será cursado por la red.

3.1.2 ADMINISTRADOR DE LA BASE DE DATOS – ABD

El Administrador de la Base de Datos Administrativa será el responsable por el dimensionamiento, contratación, planeación de los equipos y sistemas necesarios para la implementación y operatividad de las bases de datos centralizada, de conformidad con el modelo técnico adoptado.

3.1.2.1 Condiciones de administración de la base de datos administrativa

El administrador de la Base de Datos Administrativa debe implementar la infraestructura técnica de la base de datos conforme a los plazos de implementación que se encuentran definidos en el Decreto 1630 de 2011, es decir, luego de seis (6) meses de expedir la regulación que se publica en la presente propuesta. En todo caso, es importante tener en cuenta que una vez sea sancionada la

²⁴ Canal de difusión (Broadcast Channels)

²⁵ Canal de Control de frecuencia (Frequency Control Chanel, FCCH)

²⁶ Canal de Control de Sincronismo (Synchronization Control Chanel)

²⁷ Canal de Control Broadcast (Broadcast Control Chanel)

²⁸ Temporary Mobile Subscriber Identity

ley asociada al proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, este plazo no podrá superar el término máximo de implementación de las bases de datos según el cual las mismas deberán estar operativas a más tardar el 1 de enero de 2012. A su vez, debe garantizar el intercambio periódico de información entre la BDA y las BDO de cada PRSTM, por medio del uso de interfaces y sistemas de soporte de arquitecturas abiertas con protocolos comunes estandarizados.

El administrador de la Base de Datos tiene la responsabilidad de dimensionar el hardware y software necesarios para el almacenamiento, el dimensionamiento, especificaciones, planificación y administración de las estructuras de hardware y software para la implementación, funcionamiento y accesibilidad de la base de datos centralizada que se usará como repositorio de control, transacciones y actualizaciones entre PRSTM y consultas externas autorizadas, de IMEI para equipos terminales "libres" e IMEI "en uso", en tiempo cercano al real. Igualmente, el administrador de la Base de Datos es el responsable de la administración, monitoreo, mantenimiento y control de calidad de la base de datos administrativa, por lo tanto debe suministrar una infraestructura de hardware y software tal que de forma continua garantice las funciones mencionadas.

Al ser la BDA un recurso compartido por diferentes agentes, el administrador de la Base de Datos debe proporcionar los estándares, guías de manejo, procedimientos de acceso y control y toda la documentación necesaria para garantizar el acceso, actualización y la disponibilidad permanente a/de la BDA.

El dimensionamiento deberá considerar que la BDA pueda ser accedida de manera permanente y simultánea desde cualquier PRSTM, por lo que el sistema de concurrencias deberá estar perfectamente definido por parte del administrador de la Base de Datos.

El administrador de la Base de Datos debe garantizar que la información almacenada en la misma se encuentre disponible los siete (7) días a la semana, las veinticuatro (24) horas al día, por lo que debe disponer de un sistema completamente redundante. Por otro lado, ante cualquier error presentado tanto en el hardware como en el software de la BDA, el sistema debe ser lo suficientemente robusto para recuperarse en el menor tiempo posible y por lo tanto el administrador de la BDA debe tener definidas e implementadas políticas de respaldo de la información, tales que se minimice el riesgo de daño o pérdida de la misma.

Así mismo, el administrador de la Base de Datos debe garantizar la confidencialidad de la información almacenada en ella. Dicha información sólo podrá ser utilizada para los fines establecidos en el presente marco normativo y no podrá ser divulgada, compartida ni utilizada para otros fines.

Por otro lado es necesario que el administrador de la BDA disponga de mecanismos que permitan tener trazas de auditoría completas y automáticas relacionadas con el acceso a las bases de datos, incluyendo la capacidad de generar alertas con el objetivo de mitigar los riesgos asociados con el manejo inadecuado de la información, apoyar el cumplimiento de las disposiciones regulatorias aplicables y satisfacer los requerimientos de auditoría.

El administrador de la Base de Datos debe suministrar las herramientas e interfaces adecuadas para que el Ministerio de TIC, la CRC y demás organismos autorizados para acceder a la BDA, consulten en línea, registro a registro, la información almacenada en la BDA.

3.1.2.2 Requisitos Mínimos del Administrador de la Base de Datos (ABD)

De acuerdo a las experiencias internacionales, es conveniente que el regulador defina unos requisitos mínimos a cumplir por parte del administrador de la base de datos centralizada, que aseguren la idoneidad del mismo y la independencia de sus decisiones frente a los PRSTM. Estos requisitos deben ser tenidos en cuenta en las condiciones establecidas por los PRSTM para la selección del ABD.

Entre dichas condiciones, deberá contemplarse que el ABD esté constituido de acuerdo con la legislación colombiana, que no se encuentre inhabilitado y que no presente incompatibilidades. Por otra parte, se deben incluir exigencias que garanticen la transparencia e independencia del ABD, entre otras, que sea independiente administrativa y financieramente del PRSTM, que no tenga participación societaria de los PRSTM y de sus vinculadas, controladas, matrices y subordinadas, y que los empleados del ABD no provean servicios o tengan vínculo laboral con los mismos.

3.1.2.3 Contrato del Administrador de la Base de Datos con los Proveedores de Servicios de Telecomunicaciones

Se considera conveniente establecer los contenidos mínimos del contrato que han de suscribir los PRSTM con el Administrador de la Base de Datos, con el fin de garantizar los elementos esenciales para el buen funcionamiento del sistema centralizado que soporta las bases de datos positiva y negativa.

Entre dichos elementos esenciales se identifican los siguientes:

- Especificaciones técnicas y operativas.
- Nivel de calidad y disponibilidad.
- Mecanismos de seguridad.
- Garantías
- Duración del contrato.
- Esquemas de remuneración.
- Procedimientos de intercambio de información.
- Servicio de atención y soporte.
- Mecanismos de solución de controversias.

El modelo de contrato deberá hacer parte de las condiciones contractuales para la selección del Administrador.

3.1.2.4 Obligaciones del Administrador de la Base de Datos

El Administrador de la Base de Datos debe asegurar la correcta implementación y operación de la BDA que contiene, tanto la relación de los IMEI de todos los equipos móviles que han sido reportados como hurtados y/o extraviados en Colombia y en el exterior (cuando se suscriban los acuerdos interadministrativos para el intercambio de información), como la relación de los equipos terminales móviles ingresados o fabricados legalmente en el país, incluyendo los procedimientos para la actualización de las mismas y la integridad de la información, entre otras.

Dichas obligaciones deberán ser incluidas por los PRSTM en el contrato a suscribir con el Administrador de la Base de Datos y las mismas estarán claramente definidas con anterioridad al inicio del proceso de selección del Administrador.

Los PRSTM deben definir las condiciones para la contratación del Administrador de la BDA teniendo en cuenta los criterios establecidos en el presente documento, dentro de los plazos determinados por el Decreto 1630 de 2011, además de las condiciones incluidas en el Proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara *"Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las Reglas sobre Extinción de Dominio y se dictan otras disposiciones en materia de Seguridad"*, el cual se encuentra actualmente en trámite de sanción presidencial. Igualmente, deben suscribir los respectivos contratos con el administrador de la BDA seleccionado, dentro del plazo determinado para ello.

3.1.2.4.1 Autoridades competentes (administrativas, policivas o judiciales) para acceder a las BD

De acuerdo con lo dispuesto en el segundo inciso del artículo 6 del Decreto 1630 de 2011, es clara la responsabilidad que tienen los PRSTM de mantener actualizada la información de la BDA, así como de garantizar la consulta en línea, registro a registro, por parte de las autoridades administrativas, policivas o judiciales.

Para el efecto, es de reiterar que cada PRSTM dispone de una BDO negativa que se alimenta de conformidad con los reportes que generen sus usuarios en relación con los equipos hurtados o extraviados, y a su vez es claro que dicha BDO negativa de cada PRSTM se replica en la Base de Datos Administrativa Centralizada. De lo anterior, se desprende la necesidad de aclarar que el acceso que deben permitir los PRSTM a las autoridades, de que trata el artículo 6 del citado Decreto, corresponde a la Base de Datos Administrativa Centralizada.

Teniendo en cuenta lo anterior, ejerciendo facultades constitucionales y legales, las autoridades administrativas tales como el Ministerio de Tecnologías de la Información y las Comunicaciones, la Superintendencia de Industria y Comercio, y la CRC, así como las autoridades policivas y judiciales, podrán consultar en línea la información consignada en la Base de Datos Negativa en forma exacta y actualizada. En lo que se refiere al Ministerio de Tecnologías de la Información y las Comunicaciones y la CRC, tal acceso será permitido por parte de los PRSTM, especialmente, para el cumplimiento de sus competencias legales previstas en la Ley 1341 de 2009.

En todo caso, teniendo en cuenta que la Base de Datos Negativa puede contener datos que eventualmente llegarían a identificar a un individuo, por tratarse del IMEI como pieza de información que de alguna manera se asocia a un propietario, bien sea persona natural o jurídica, el manejo de la información deberá observar lo dispuesto por la normatividad vigente en materia de protección de datos personales y la misma no podrá ser divulgada ni puesta en conocimiento de terceros no autorizados por las normas vigentes.

De este modo, para que las autoridades puedan efectuar las consultas en línea que requieran para el ejercicio de sus funciones, debe tenerse en cuenta que dichas consultas por parte de las autoridades sólo podrá efectuarse registro a registro. Para garantizar lo anterior, el administrador de la Base de Datos debe disponer de una interfaz WEB GUI utilizando HTTPS en complemento con SSL, para permitir el acceso vía WEB a la información contenida en la Base de Datos Negativa de la BDA.

3.1.3 ALIMENTACIÓN DE LA BASE DE DATOS POSITIVA

De acuerdo con lo señalado en el artículo 7 del Decreto 1630 de 2011, la base de datos positiva será alimentada por:

- Los PRSTM.
- Los importadores de equipos terminales nuevos.
- Los fabricantes o ensambladores de equipos terminales nuevos nacionales.

3.1.3.1 Obligaciones y rol de los PRSTM

3.1.3.1.1 En el periodo de transición

De acuerdo con lo establecido en el artículo 7 del Decreto 1630 de 2011, los PRSTM tienen un periodo de 6 meses contados a partir de la expedición de la regulación por parte de la CRC, para incluir en la base de datos positiva los IMEI de los equipos terminales móviles, así como el número de identificación de cada propietario de dichos equipos, activos en las redes de telecomunicaciones al momento de la expedición de la citada regulación. En todo caso, este plazo se encuentra sometido a lo que sobre el particular disponga la ley que sea sancionada con ocasión del proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, según el cual el plazo máximo de implementación y puesta en marcha de las bases de datos es el 1 de enero de 2012.

Para este periodo de transición cada PRSTM debe elaborar una lista en la que se asocien IMEI y número de identificación de todos sus usuarios activos. Posteriormente, los PRSTM en conjunto deben elaborar una lista que consolide la información de todos los PRSTM. Al respecto, se identifican los siguientes casos:

- **CASO 1: Un IMEI asociado con un número de identificación de usuario en un PRSTM:** En este caso, el PRSTM debe registrar en la base de datos positiva de la BDA, el IMEI con el número de identificación del usuario. En su BDO, el PRSTM debe registrar en su base de datos positiva el IMEI y el IMSI del usuario. Además deberá notificar al usuario que en la red de PRSTM, el IMEI registrado tendrá servicio exclusivamente con su número celular de ese PRSTM.
- **CASO 2: Un IMEI asociado con varios números de identificación de usuario en un mismo PRSTM.** En este caso se detecta que existen equipos con IMEI repetido. El PRSTM debe informar a los usuarios que deben acercarse, en un tiempo no mayor a ocho (8) días hábiles, para verificar que el IMEI del equipo no ha sido alterado. El PRSTM deberá contar con los mecanismos pertinentes para poder determinar la legitimidad de los Equipos Terminales Móviles analizados. Una vez se surta dicho proceso, el PRSTM debe, de acuerdo a lo establecido en el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, retener el (los) equipo(s) y denunciar ante las autoridades competentes. Una vez se identifique el usuario que tiene el equipo con IMEI válido, el PRSTM debe proceder a registrar en la Base de Datos positiva de la BDA, el IMEI con el número de identificación del usuario. En su BDO, el PRSTM debe registrar en la Base de Datos Positiva el IMEI y el IMSI del usuario.
- **CASO 3: Un IMEI asociado con un número de identificación de usuario en distintos PRSTM.** En este caso, los PRSTM deben registrar en la base de datos positiva de la BDA, el IMEI con el número de identificación del usuario. Por otra parte, cada PRSTM en su BDO, debe registrar en la base de datos positiva el IMEI y el IMSI del usuario. Además cada PRSTM, deberá notificar al usuario que el IMEI registrado del Equipo Terminal Móvil podrá ser utilizado con los números celulares asociados en cada PRSTM.
- **CASO 4: Un IMEI asociado con varios números de identificación de usuario en distintos PRSTM.** En este caso se detecta que existen equipos con IMEI repetidos o que un

mismo equipo tiene diferente suscriptor en más de un PRSTM. Cada PRSTM deben informar a los usuarios de su red que deben acercarse, en un tiempo no mayor a ocho (8) días hábiles, para verificar que el IMEI del equipo no ha sido alterado. Los PRSTM deberán contar con los mecanismos pertinentes para poder determinar la legitimidad de los Equipos Terminales Móviles analizados. Una vez se surta dicho proceso, los PRSTM deben, de acuerdo a lo establecido en el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, retener el (los) equipo(s) y denunciar a las autoridades competentes. Una vez se identifique el usuario que tiene el equipo con IMEI válido, ese PRSTM deben proceder a registrar en la Base de Datos positiva de la BDA, el IMEI con el número de identificación del usuario. En su BDO, cada PRSTM debe registrar en la Base de Datos Positiva el IMEI y el IMSI del usuario.

Para efecto de la actualización de la BDO a la BDA en los casos 1 a 4, el ABD y el PRSTM deberán establecer periodos fijos de actualización en las horas de menor tráfico.

3.1.3.1.2 Luego del periodo de transición

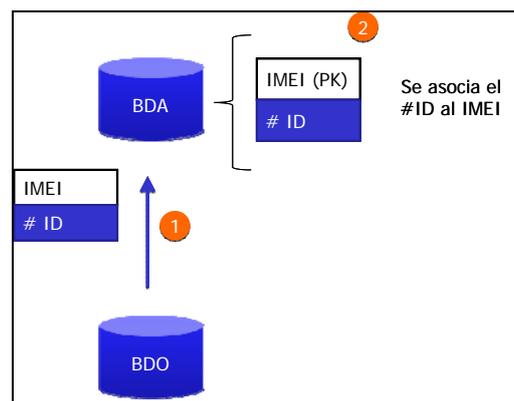
Cargue y actualización de la base de datos positiva por solicitud del usuario

Luego del periodo de transición establecido en el artículo 7 del Decreto 1630 de 2011 y cada vez que el usuario desee utilizar un equipo por primera vez en la red de un PRSTM, debe demostrar que el mismo es de su propiedad. Se identifican los siguientes casos:

- **IMEI sin número de identificación asociado en la BDA.** Si el IMEI del equipo del usuario no tiene asociado un número de identificación en la base de datos positiva de la BDA, el PRSTM debe solicitar al usuario la factura de compra del equipo, la cual debe incluir el IMEI del equipo y debe ser expedida por las personas autorizadas según el artículo 3 del Decreto 1630 de 2011, y corroborar que el equipo se encuentre homologado por la CRC.

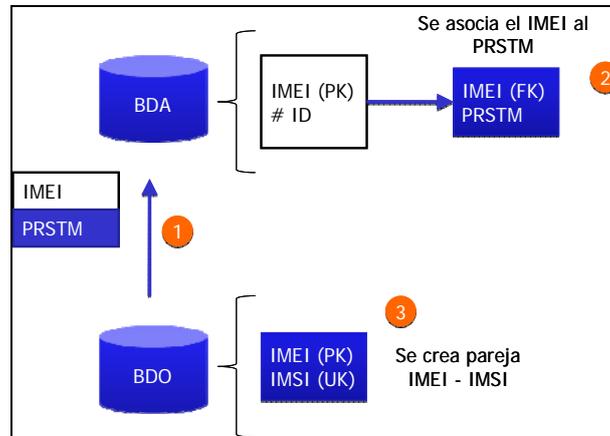
Luego de verificar dichos documentos, el PRSTM procederá a asociar al IMEI, el número de identificación del usuario en la base de datos positiva de la BDA, en la cual deberá quedar un registro en el que se indique el IMEI está siendo usado por el PRSTM.

Figura 7. Cargue del número de identificación de usuario en la BDA



FUENTE: Elaboración propia

Posteriormente, el PRSTM debe crear el par IMEI-IMSI en la base de datos positiva de su BDO, teniendo en cuenta que un IMEI solo puede estar asociado a un IMSI del PRSTM y viceversa.

Figura 8. Creación de par IMEI-IMSI en BDO


FUENTE: Elaboración propia

Cuando el PRSTM elimine el par IMEI-IMSI de su BDO, debe informarlo al administrador de la BDA, para que se elimine el registro que indica que el IMEI estaba siendo usado por dicho PRSTM.

- **IMEI con número de identificación asociado en la BDA.** Si el IMEI del equipo del usuario tiene asociado un número de identificación en la base de datos positiva de la BDA, el PRSTM debe verificar que ese mismo número de identificación es el que está solicitando la activación. Luego de verificar esto, el PRSTM procederá a asociar al IMEI, el IMSI en la base de datos positiva de su BDO, teniendo en cuenta que un IMEI solo puede estar asociado a un IMSI del PRSTM y viceversa. En la BDA deberá quedar un registro en el que se indique que el IMEI está siendo usado por el PRSTM.

▪

En caso de que en la BDA figure un número de identificación diferente al del usuario que está solicitando la activación, el equipo no podrá ser activado, a menos que el titular del IMEI registrado en la BDA autorice el cambio de titularidad, mediante los mecanismos señalados en el parágrafo del artículo 8 del Decreto 1630 de 2011.

Ahora bien, en caso que el usuario pudiendo demostrar la compra legal de su Equipo Terminal Móvil, el IMEI de dicho equipo existe en la BDA asociado a un número de identificación diferente, el PRSTM deberá iniciar un proceso para identificar cuál de los 2 equipos tiene el IMEI alterado.

Una vez surtido dicho proceso, si el usuario que solicitó la activación es el tenedor del equipo con IMEI válido, el PRSTM debe proceder a eliminar el actual par IMEI-IMSI y actualizar la nueva información en la BDA y en su BDO, y deberá denunciar ante la respectiva autoridad el hecho presentado. Por el contrario, si el usuario que solicitó la activación tiene en su posesión el equipo con IMEI alterado, el PRSTM debe, de acuerdo a lo establecido en el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, retener dicho equipo y denunciar a las autoridades competentes.

- **IMEI no registrado en la BDA.** Si el IMEI no se encuentra registrado en la BDA, quiere decir que el equipo fue adquirido en el exterior o que no se realizó el proceso de cargue de la información durante la etapa de transición, razón por la cual, el usuario deberá presentar la

factura de compra del mismo, a fin de que el PRSTM verifique el origen legal del respectivo equipo.

Luego de verificar dicho documento, el PRSTM informará al usuario que debido a que el equipo que desea activar fue comprado en el exterior, no se encuentra parametrizado con todas las funcionalidades propias de las redes móviles colombianas, por lo que es necesario que suscriba un documento en el cual acepta activar el equipo terminal móvil a su cuenta y riesgo y que renuncia a cualquier reclamación que tenga referencia a la calidad del servicio prestado y al uso de aplicaciones.

Una vez el usuario suscriba el documento anteriormente citado, el PRSTM debe registrar en la base de datos positiva de la BDA, el IMEI del equipo y el número de identificación del usuario, y en la base de datos positiva de su BDO debe asociar el IMEI y el IMSI del usuario. En la BDA deberá quedar un registro en el que se indique que el IMEI está siendo usado por el PRSTM.

Para efecto de la actualización de la BDO a la BDA de los puntos anteriores, el ABD y el PRSTM deberán establecer periodos fijos de actualización en las horas de menor tráfico.

- **IMEI incluidos por solicitud de los fabricantes.** Los fabricantes de equipos terminales móviles pueden solicitar al ABD el registro de IMEI en la BDA positiva, una vez alleguen la información que permita confirmar al ABD que dichos IMEI corresponden a equipos que son traídos al país para realizar un cambio por garantía, que son equipos prototipo que serán utilizados para realizar pruebas en la red o que son equipos a los cuales fue necesario realizar una modificación del IMEI durante el proceso de reparación.
- **IMEI registrado en la base de datos negativa.** Si el usuario presenta un equipo cuyo IMEI se encuentra registrado en la base de datos negativa, el PRSTM debe retener dicho equipo si comprueba que su IMEI ha sido alterado y debe denunciar a las autoridades competentes, lo cual guarda coherencia con lo el contenido del proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara. Sin embargo, si el usuario puede demostrar que dicho equipo fue adquirido legalmente, el PRSTM debe informarle al usuario quién lo incluyó en la base de datos negativa de la BDA, para que éste se dirija a dicho PRSTM. Una vez el usuario presente el caso ante el PRSTM que lo reportó en la base de datos negativa, y en caso de que éste pueda determinar que el IMEI no fue alterado, el PRSTM debe proceder a activarlo en las bases de datos positivas de la BDA y de su BDO, y a retirarlo de la base de datos negativa. En la BDA deberá quedar un registro en el que se indique que el IMEI está siendo usado por el PRSTM.

Cargue y actualización de la base de datos positiva por solicitud del administrador de la BDA

Cuando el administrador de la BDA le informe a un PRSTM que un IMEI reportado por un importador que va a ser ingresado a la BDA se encuentra duplicado, dicho PRSTM debe informar al usuario registrado con dicho IMEI en su red que debe acercarse, en un tiempo no mayor a ocho (8) días hábiles, para verificar que el IMEI de su equipo no ha sido alterado. El PRSTM debe contar con los mecanismos pertinentes para poder determinar la legitimidad de los Equipos Terminales Móviles analizados. En este proceso, se presentan los siguientes casos:

- Si el PRSTM determina que el equipo del usuario tiene el IMEI alterado, debe, de acuerdo a lo establecido en el proyecto de Ley No. 164 de 2010 Senado - 160 de 2010 Cámara, retener el equipo y denunciar a las autoridades competentes. Así mismo, debe informar al administrador

de la BDA que proceda a liberar el IMEI en la base de datos positiva, es decir que borre el número de identificación que tiene asociado.

- Si el PRSTM determina que el equipo del usuario tiene el IMEI válido, debe informar al administrador de la BDA que no puede registrar el IMEI del importador, y a su vez, el administrador debe denunciar este hecho a las autoridades competentes.

Cargue y actualización de la base de datos positiva por solicitud de un fabricante o ensamblador nacional

Cuando un fabricante o ensamblador nacional solicita al ABD la inclusión de un IMEI en la base de datos positiva de la BDA, el ABD debe verificar que el IMEI no se encuentre ya contenido en la BDA. Si al momento de registrar el IMEI en la BDA el ABD detecta que ya existe, debe iniciar un proceso para determinar si el IMEI informado por el fabricante o ensamblador nacional es válido, para lo cual debe informar el hecho al respectivo PRSTM, con el fin de que éste informe al usuario registrado con dicho IMEI en su red que debe acercarse, en un tiempo no mayor a cinco (5) días hábiles, para verificar que su equipo no ha sido alterado. El ABD debe contar con los mecanismos pertinentes para poder determinar la legitimidad de los Equipos Terminales Móviles analizados.

Aspectos a tener en cuenta por los PRSTM para todos los casos

El PRSTM sólo podrá activar un equipo si el mismo ha sido homologado por la CRC, para lo cual debe consultar el sitio Web dispuesto por la Comisión para tal fin.

Adicionalmente, el PRSTM debe verificar:

- Que el IMEI del equipo programado en el equipo terminal móvil cumple con la lógica de validación definida en el estándar GSM (algoritmo de Luhn).
- Que el IMEI programado en el equipo terminal móvil corresponda al impreso en la etiqueta del mismo.
- Que el IMEI corresponda con la marca y modelo contenidos en el mismo.

Cuando un PRSTM reporta al administrador de la BDA un cambio en el número de identificación personal de un usuario, asociado a un IMEI ya incluido en la base de datos positiva de la BDA, relacionado con otro número de identificación de usuario, el administrador debe proceder a cambiar los registros asociados a tal modificación en la base de datos positiva de la BDA, actualizándolo con el nuevo número de identificación personal de usuario. Las bases de datos positivas de las BDO de los demás PRSTM serán actualizadas de acuerdo con el nuevo registro en la BDA, eliminando el par IMSI-IMEI asociado al usuario antiguo. Para el efecto, la BDA reporta automáticamente la nueva información a las demás bases de datos de los PRSTM. Para efecto de la actualización de la BDO a la BDA, el ABD y el PRSTM deberán establecer periodos fijos de actualización en las horas de menor tráfico.

Equipos terminales móviles que son desactivados con la entrada en operación de las bases de datos

Una vez entre en operación la base de datos positiva, quedarán inhabilitados los equipos terminales móviles cuyos IMEI no fueron incluidos en la BDA. Los PRSTM deberán adelantar todas las actividades que sean requeridas para que los Equipos Terminales Móviles que se encuentren fuera

de operación sean incluidos en la base de datos positiva dentro de los dos (2) meses siguientes a la entrada en operación del sistema.

3.1.3.1.3 Requisitos de comprobación de la adquisición legal de los terminales una vez finalizado el período de transición

Para efectos que el PRSTM pueda determinar que un equipo terminal móvil presentado por un usuario es de su propiedad, se presentan 2 casos:

- **Equipo adquirido en el país:** en este caso el usuario debe presentar ante el PRSTM la factura de compra expedida por las personas autorizadas según el artículo 3 del Decreto 1630 de 2011. En caso de que el equipo no haya sido adquirido en uno de los establecimientos de las personas autorizadas, este no podrá ser activado por el PRSTM y el caso será puesto en conocimiento de la autoridad competente.
- **Equipo adquirido en el exterior:** en este caso el usuario deberá presentar la factura original de compra del establecimiento o comprobante de pago en efectivo, cheque o tarjeta débito o crédito, a fin que el PRSTM verifique el origen legal del respectivo equipo. Así mismo, el PRSTM debe verificar que el equipo se encuentre homologado por la CRC. De no cumplirse los anteriores criterios, el equipo no podrá ser activado por el PRSTM.

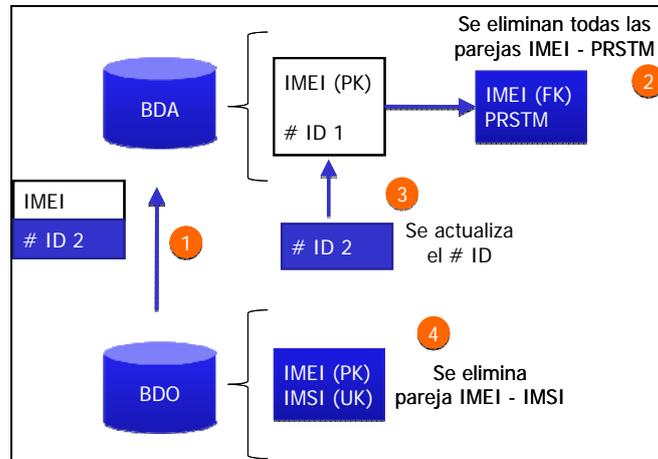
3.1.3.1.4 Mecanismos para el cambio de titular de un Equipo Terminal Móvil

Para realizar el cambio de titular de un equipo terminal móvil, el Decreto 1630 de 2011 establece que el propietario debe presentarse ante el PRSTM. Así las cosas, la presente iniciativa toma en consideración que el usuario titular deba presentarse en una oficina de atención al cliente de alguno de los PRSTM que le presta servicio, en donde debe informar la nueva cédula que estará asociada al IMEI del equipo. En caso de que el equipo tenga 2 o más IMEI, el proceso deberá realizarse para cada uno de ellos.

Adicionalmente, y de acuerdo a lo establecido en el parágrafo del artículo 8, dado el caso que el usuario titular del equipo terminal móvil no pueda presentarse en una oficina de atención al cliente, la persona que solicita el cambio de titularidad del equipo terminal móvil deberá presentar la factura del mismo y una carta del propietario del equipo solicitando el cambio de su titularidad.

Una vez surtidos cualquiera de los anteriores trámites el PRSTM debe proceder a actualizar el número de identificación del usuario asociado con el IMEI en la base de datos positiva de la BDA, en la cual se deberán eliminar los registros de los PRSTM que están haciendo uso de ese IMEI, y posteriormente, el PRSTM debe eliminar el par IMSI- IMEI de su BDO. Así mismo, el administrador de la BDA debe informar este cambio a los PRSTM que estaban haciendo uso del IMEI, para que también eliminen el par IMEI-IMSI en la base de datos positiva de su BDO. En caso que el PRSTM, al que el usuario solicita el cambio de titularidad de equipo, no tenga registrado en la BDA el uso del IMEI, no podrá realizar el cambio de titularidad de equipo en la BDA, a menos que ningún PRSTM tenga asociado en la BDA a dicho IMEI. Para efecto de la actualización de la BDO a la BDA, el ABD y el PRSTM deberán establecer periodos fijos de actualización en las horas de menor tráfico.

Figura 9. Proceso de cambio de titular de un Equipo Terminal Móvil



FUENTE: Elaboración propia

3.1.3.2 Importadores

Al momento de ingresar los equipos terminales móviles al país, los importadores deben registrarlos ante la DIAN. En dicho registro, los importadores deberán informar los IMEI de todos los equipos, los cuales son introducidos al sistema MUISCA²⁹. En este proceso se debe verificar que los equipos que están siendo ingresados al país son nuevos y están homologados por la CRC. Así mismo, los importadores deben presentar, para su ingreso al país, una certificación expedida por el fabricante de los equipos, en la cual, los autorice para la importación de equipos terminales móviles a Colombia.

Para el cargue y actualización de la información en la base de datos positiva de la BDA, ésta se debe conectar diariamente con el sistema MUISCA de la DIAN y descargar de allí la información de los IMEI de los equipos que están siendo ingresados al país. En este proceso debe verificar que los IMEI no se encuentren incluidos en la BDA. En caso de identificar que algún IMEI se encuentra en la BDA, se deberá iniciar un proceso para determinar cuál de los equipos tiene el IMEI alterado, en el que el administrador de la BDA deberá informar a los PRSTM que están haciendo uso del IMEI para que lo verifiquen. Si el IMEI del equipo importado resulta ser el alterado, no será registrado en la BDA. Si por el contrario, el IMEI del equipo importado es el válido, éste debe ser registrado en la BDA en estado libre.

3.1.3.3 Fabricantes o ensambladores nacionales

Para efectos de registrar los IMEI de los equipos terminales móviles en la base de datos positiva de la BDA, los fabricantes o ensambladores nacionales deben realizar la solicitud al administrador de la BDA, acreditando que dichos equipos han sido homologados por la CRC. El ABD tiene la obligación de verificar que la información contenida en el IMEI corresponda al fabricante que solicita el cargue de los IMEI en la BDA.

Una vez verificado lo anterior, el administrador de la BDA debe proceder a registrar los IMEI en la base de datos positiva de la BDA. En este proceso deberá verificar que los IMEI no se encuentren

²⁹ Modelo Único de Ingresos, Servicio y Control Automatizado.

ya incluidos en la BDA. En caso de identificar que algún IMEI se encuentra en la BDA, el administrador debe informar a los PRSTM que están haciendo uso del IMEI, para que de esta forma el PRSTM proceda a utilizar los mecanismos pertinentes para determinar la legitimidad del IMEI de los Equipos Terminales Móviles objeto de análisis..

3.1.4 ALIMENTACIÓN DE LA BASE DE DATOS NEGATIVA

3.1.4.1 Requisitos para los PRSTM

Las bases de datos negativas tienen como objeto mantener actualizada la información de los IMEI que han sido reportados como hurtados y/o extraviados, para que de esta forma y luego de su consulta el PRSTM pueda bloquear el servicio a los equipos terminales móviles que hacen parte de dicha lista. Sin perjuicio de las medidas y procedimientos que ya se llevan a cabo para el manejo de estas bases de datos, es obligación de los PRSTM:

1. Habilitar todos sus sistemas de atención para que el usuario y las autoridades policivas, judiciales y administrativas puedan realizar los respectivos reportes de hurto o pérdida de equipos terminales móviles que se encuentren en servicio o estén fuera de éste.
2. Validar la titularidad de quien hace el reporte a nivel de líneas activas o la titularidad de la tenencia para el caso de equipos terminales móviles aún no activos o no asociados a un número de identificación.
3. En los casos de líneas prepago en que el usuario no sea el titular o no conozca quién es el titular, el reporte debe recibirse y se accionarán los bloqueos a que haya lugar tanto de la SIM como del equipo terminal móvil, y en todos los casos el PRSTM deberá agotar los medios que se encuentren a su alcance para verificar que quien hace el reporte si sea el usuario que hace uso de la línea móvil. En ese sentido, ninguna llamada o asistencia personal en centros de atención con el objeto de reportar un equipo del que no se posee la titularidad debe ser desatendida y se debe generar el bloqueo y reporte de él o los equipos informados.
4. Acto seguido al reporte de hurto o perdida por parte de un usuario, autoridad policiva, judicial o administrativa, el PRSTM debe suspender todos los servicios asociados tanto a la SIM como al equipo, es decir debe proceder a bloquear la SIM y el IMEI a nivel de sistemas de ventas y activación de nuevas líneas o cambios de servicio, bloquear el IMEI a nivel de uso en la red celular y reportar el IMEI objeto de bloqueo a la BDA negativa.
5. El PRSTM deberá adecuar sus procesos y sistemas para garantizar que el bloqueo que se aplique a raíz de un reporte, se haga sobre el equipo terminal móvil correcto, esto es, no puede errar el equipo a bloquear en razón a la múltiple actividad de equipos que un usuario pueda registrar o a la desactualización del equipo usado en sus sistemas de información, y en todos los casos el bloqueo se debe aplicar sobre el equipo que corresponda al usado en la línea en la fecha y hora del hurto o extravío reportado por el usuario.
6. El PRSTM tiene la obligación de bloquear todos los servicios, facilidades, accesos, etcétera, que estén asociados a un equipo terminal móvil sin importar que quien los suministre es un tercero que no se encuentra en territorio Colombiano. El PIN de servicios de chat prestados en el país y/o en el exterior deberá quedar desactivado o deshabilitado de inmediato o como máximo al mismo tiempo en que se bloquean los demás servicios y el IMEI, y su desactivación, deshabilitación o bloqueo debe ser no sólo a nivel nacional sino a nivel internacional o incluso mundial o en la cobertura en que tal servicio se puede usar con dicho PIN, el cual, como su término lo indica, es un Número Personal de Identificación del propietario del Equipo Móvil que soporta el servicio y quien es el titular y propietario del equipo. El PRSTM deberá responder por los daños y perjuicios causados a los propietarios de estos PIN por el incumplimiento de esta obligación o el no bloqueo o desactivación del PIN.

7. El PRSTM debe reportar a la Policía Nacional, por el medio que estime conveniente y que garantice la seguridad, las líneas, el número de identificación del usuario y los hechos informados por éste cuando se realiza el respectivo reporte del equipo hurtado. Estas dos instituciones podrán acordar los términos de periodicidad y medios utilizados para tal reporte.
8. El PRSTM debe mantener actualizada en línea su base de datos negativa que para tal fin se crean a la luz del Decreto 1630 de 2011 y tomar de inmediato las acciones de inclusión y retiro de IMEI en dicha base de datos según los reportes recibidos de sus usuarios, autoridades policivas, administrativas y judiciales y las provenientes de los otros PRSTM por medio de la Base de Datos centralizada.
9. El PRSTM deberá prever y dimensionar las capacidades necesarias en su base de datos negativa con la entrada en operación de las medidas establecidas en el Decreto 1630 de 2011 para intercambio nacional e internacional de estas bases de datos y adecuarlas para no tener que borrar registros anteriores o incluir registros inoficiosos en las mismas que eviten o impidan la inclusión de nuevos registros.

Para la alimentación de un IMEI con reporte de hurto y/o extravío en las bases de datos negativas de la BDO a la BDA, el PRSTM y el ABD deberán proceder de inmediato tanto en la actualización de la novedad a la BDA por parte del PRSTM que recibió el reporte de hurto y/o extravío, como en la actualización hacia las BDO de los demás PRSTM por parte de la BDA para que el bloqueo del equipo terminal móvil se realice en un tiempo máximo de 25 minutos.

3.1.5 MECANISMOS PARA EXTRAER UN EQUIPO DE BASE DE DATOS NEGATIVA Y TRASLADARLO A LA POSITIVA

De acuerdo a lo consignado en el párrafo 2 del artículo 6º del Decreto 1630 de 2011, sólo es posible que un equipo terminal móvil que haya sido reportado como hurtado y/o extraviado sea excluido de la Base de Datos negativa, únicamente por el PRSTM que realizó el registro del mismo en dicha base de datos. El PRSTM tendrá la responsabilidad de informar al administrador de la base de datos centralizada, el retiro del IMEI de la base de datos negativa y su correspondiente inclusión en la base de datos positiva, así como también el número de identificación al cual debe estar asociado dicho IMEI.

A su vez, el PRSTM deberá excluir el IMEI de su BDO negativa, y cuando así lo requiera el usuario, incluirlo en la base de datos positiva de su BDO, asociando al nuevo registro el respectivo IMSI del usuario.

Las bases de datos positiva y negativa de las BDO de los demás PRSTM serán actualizadas de acuerdo con el nuevo registro en la BDA. Para el efecto, la BDA y el PRSTM deberán establecer el intercambio de esta novedad de inmediato por parte del PRSTM que recibe el reporte de recuperación hacia la BDA, como también por parte de la BDA hacia las BDO de los demás PRSTM

Debido a que un IMEI solo puede ser excluido de la base de datos negativa por el PRSTM que lo registró, para el caso de números portados hacia otros PRSTM es necesario que todos los PRSTM dispongan de un sistema de información que almacene el historial de los IMEI que han operado en su red de tal modo que, cuando un usuario portado hacia otra red le reporte la recuperación del equipo terminal, el PRSTM que actuó como donante en el proceso de portación, informe al ABD el retiro del IMEI de la base de datos negativas y su correspondiente inclusión en la base de datos positiva, independientemente de la existencia o no de un vínculo contractual con el usuario.

3.1.6 COMPARTICIÓN DE INFORMACIÓN DE LAS BASES DE DATOS NEGATIVAS CON FILIALES EN EL EXTERIOR

El problema de hurto de equipos terminales móviles debe su auge en gran parte a la facilidad con que se envían los equipos a otros países para su comercialización. Frente a esta situación, existen dos factores que propician este *mercado ilegal*: **i)** Equipos terminales móviles cuyo IMEI es alterado en un sitio determinado y **ii)** La expedición de normatividad propia de cada país que busca desestimular la comercialización de equipos terminales móviles hurtados, ante lo cual el siguiente paso de este *mercado ilegal* es llevar dichos equipos a otros países donde no exista regulación y/o leyes contra la comercialización y uso de estos terminales.

Para llevar a cabo esta fase del negocio, los encargados de este *mercado ilegal* recurren a enviar los equipos completos superando los controles en las fronteras y en los puntos aduaneros. Estos equipos son recibidos en otro país, y vendidos al público como equipos refaccionados o reciclados, sin ningún tipo de garantía, afectando a los usuarios en la medida en que estos equipos están parametrizados para usar servicios en redes de otros países, y parte de sus funcionalidades pueden no servir en el país a donde son llevados. Sumado a lo anterior, cabe destacar que los fabricantes tampoco prestan garantía de servicio a este tipo de equipos.

En los casos en donde los controles en los puntos mencionados de salida/entrada a un país son estrictos, se recurre a desensamblar los equipos en el país donde se origina su hurto o pérdida, dejando allí únicamente las carcasas, pantallas y teclados, y enviando únicamente la tarjeta electrónica madre o principal donde se encuentra programado el IMEI. Estas partes que dejan son usadas luego con las tarjetas electrónicas recibidas por la misma vía y del mismo origen (hurto o extravío) de otros países, evitando así ser detectados al constituir menos volumen o engañar a las autoridades aduciendo que son repuestos o partes usadas para servicio técnico.

Con el fin de contener este fenómeno a nivel internacional y conseguir que los controles de restricción al uso de equipos terminales móviles hurtados y/o extraviados que estipula el Decreto 1630 de 2011 también sean efectivos a nivel internacional, el artículo 6º BASE DE DATOS NEGATIVAS, en su PARÁGRAFO 1, establece: “ (...) *La Base de Datos Negativa deberá compartirse por los PRSTM que operan en el territorio nacional con sus filiales que operen en el exterior. Así mismo, los PRSTM podrán generar acuerdos con otros proveedores distintos a sus filiales que operen en el exterior, tendientes a la prevención del comercio de estos Equipos Terminales Móviles en el país que permitan la obtención de IMEIs de Equipos Terminales Móviles reportados como hurtados o extraviados en otros países.*”

Así las cosas, a continuación se analiza cómo se puede llevar a cabo dicho intercambio o compartición de bases de datos..

3.1.6.1. Análisis del intercambio entre operadores de bases de datos negativas

Consiste en el envío y/o recepción de los IMEI reportados como hurtados o extraviados de un PRSTM a varios PRSTM del exterior, en formato digital vía enlace electrónico (interconexión directa, VPN, WEB), según los acuerdos definidos entre éstos. Los PRSTM tienen la potestad de intercambiar la información de IMEI reportados entre sus filiales, sin embargo estos son acuerdos de buena voluntad y el bloqueo puede estar aplicándose o no a discreción del país receptor de los reportes según exista o no regulación de intercambio internacional y obligación de bloquear el servicio y las activaciones de los equipos reportados en esos intercambios.

Este esquema se facilita entre operadores filiales a un mismo grupo o marca de operación móvil, dado que se aprovechan los canales de comunicación ya establecidos, la rapidez en los acuerdos, las vías de intercambio y los métodos de bloqueo. Ahora bien, para hacer mejor y más funcional esta forma de intercambio, al haber varios puntos de origen y destino en grupos de gran número de filiales y para establecer el intercambio con operadores distintos a sus filiales en otros países, se pueden buscar acuerdos y sistemas centralizados regionales que deben ser gestionados por los Gobiernos o hacer uso de sistemas centralizados proveídos por la industria, tal y como ocurre en el escenario de la GSMA, el cual se ilustra a continuación.

3.1.6.2. CEIR (IMEIDB³⁰ de la GSMA)

La Asociación Mundial de Operadores GSM (GSMA) mantiene un sistema único conocido como IMEI DB, el cual es una base de datos global centralizada que contiene la información básica de millones de rangos de Equipos Terminales Móviles GSM y tecnología 3G que están en uso por parte de los operadores GSM de todo el mundo. Al ser el IMEI un número único para cada equipo en el mundo, se necesita una tarea de clasificación y ubicación de prefijos para los fabricantes, de tal manera que no haya 2 equipos con el mismo serial, tarea realizada por la GSMA. Cuando se reserva un prefijo para un fabricante de equipos determinado, GSMA almacena la información básica asociada con el IMEI, la cual incluye el nombre del fabricante, un identificador del modelo para el equipo asociado y algunas capacidades técnicas del mismo (por ejemplo Las bandas de frecuencias soportadas).

GSMA provee el acceso a la IMEI DB a sus miembros, que son los operadores GSM y 3G alrededor del mundo, y a las partes autorizadas de la industria (fabricantes). La red de operadores usa la información de la IMEI DB para determinar qué tipo de dispositivos están siendo utilizados por sus usuarios y qué características soportan, de tal suerte que pueden ofrecerles soporte en los últimos servicios a través de sus redes.

La IMEI DB también soporta lo que se conoce como la "lista negra", la cual es la lista de IMEI que está asociada con equipos GSM y 3G que no deberían tener servicio en las redes de sus operadores porque han sido reportados como hurtados o extraviados, con fallas o inhabilitados para su uso.

Conocida antes como el CEIR (Central Equipment Identity Register), la IMEI DB actúa como un sistema central para los operadores de redes móviles para compartir sus listas negativas individuales de tal forma que los equipos bloqueados incluidos allí por una red en particular no funcionaran en otras redes incluso si la SIM en el equipo es cambiada.

Los operadores de redes móviles que cuentan con EIR locales en sus redes, las usan para guardar su propia base o lista negativa para equipos hurtados o extraviados. Dichos EIR se conectan automáticamente al sistema de la IMEI DB para compartir los últimos equipos incluidos en lista negativa con los demás operadores. Todos los días desde 1996 la IMEI DB ha tomado todas las listas negativas de diferentes operadores alrededor de todo el mundo y las ha consolidado en una lista global negativa. Cuando un EIR se conecta subsecuentemente a la IMEI DB, ésta descarga la última actualización de la lista negativa global a dicho operador (o un subconjunto nacional o regional de la lista negativa global) para su propio uso. Cargando la lista negativa de la IMEI DB en un EIR local, todos los equipos reportados como hurtados y/o extraviados en otras redes conectadas hasta el día anterior son ahora también bloqueados en esa red.

³⁰ Base de Datos de Administración de IMEI – GSM Association.

A medida que los equipos GSM y 3G se han vuelto más sofisticados y onerosos, resultan ser más atractivos para los delincuentes, es así como a partir del 2002 ha habido una necesidad creciente de usar la IMEI DB como herramienta para combatir el hurto de equipos. Muchos operadores de redes móviles han respondido a este problema empleando EIRs en sus redes y conectándolas a la IMEI DB. El compromiso de los gobiernos y autoridades competentes y policivas con la comunidad de sus operadores de redes móviles continua en un número de mercados cada vez mayor donde el robo de equipos terminales móviles se ha convertido en problema crítico y la GSMA los exhorta a usar la IMEI DB como la plataforma de intercambio de equipos robados y acoge a los operadores en dicha conexión.

Los usuarios que han sido víctimas de hurto de su equipo deben saber que GSMA no recibe y adiciona reportes a su lista negativa de IMEI DB ni asiste en incidentes de hurtos. El equipo hurtado y/o extraviado debe ser reportado al operador de servicios de redes móviles y a las autoridades.³¹

La conexión de un PRSTM a la IMEI DB no tiene costos. La GSMA ofrece sin costo el servicio de hosting virtual para los países o grupos de países o de operadores que deseen hacer el intercambio de sus listas.

Según el anterior análisis, se puede concluir que la forma más acertada y eficiente para proceder con el intercambio o compartición de bases de datos negativas es la IMEI DB de GSMA, pues no requiere tiempos y/o plazos, ni costos de implementación de bases centralizadas y de interconexión entre ellas. Cada PRSTM con EIR y miembro de GSMA se conecta y determina qué subconjunto de listas quiere actualizar, permitiendo y facilitando los acuerdos en materia de intercambio, normas y regulación a los países miembros de las organizaciones anteriormente mencionadas. Permite de igual manera facilitar y exhortar a todos los países que no pertenezcan a dichos acuerdos para que también se conecten y cerrar así las brechas que para el mercado negro constituyen países que no intercambien listas negativas. Esta solución estará disponible para los PRSTM que sean miembros de la GSMA y dispongan de un EIR, por lo que dado el escenario que algún proveedor no cumpla con esta condiciones, el intercambio internacional se verá de todas formas alimentado con el intercambio nacional que se hace entre todos los PRSTM de los cuales la mayoría podrían conectarse a la IMEI DB de GSMA.

3.2 CONSIDERACIONES DESEDE LA PERSPECTIVA DEL USUARIO

Teniendo en cuenta que las medidas que se encuentran en etapa de implementación impactan de manera directa al usuario de los servicios de telefonía móvil, es preciso reiterar algunas situaciones que deben ser observadas por éste, de conformidad con lo expuesto a lo largo del presente documento. De manera general, los usuarios deben adquirir los Equipos Terminales Móviles en puntos autorizados para el efecto, en observancia de lo establecido en el Decreto 1630 de 2011, para lo cual sólo podrán adquirir equipos con los PRSTM, las personas autorizadas por ellos, ó las personas autorizadas por el Ministerio de TIC. Para el efecto, el comercializador autorizado tendrá un certificado que lo acredite como tal y se podrá consultar la lista de establecimientos autorizados en las páginas Web de los proveedores, de la Comisión de Regulación de Comunicaciones y en la página Web del Ministerio de Tecnologías de la Información y las Comunicaciones.

Así mismo, habida cuenta que próximamente estará operativa en Colombia la Portabilidad Numérica, y a partir de los análisis realizados al interior de la CRC, debe aclararse que las condiciones antes expuestas para las situaciones de reporte de hurto y/o pérdida, además de los

³¹ Fuente: http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/imei_database.htm

escenarios de activación de terminales, serán realizados por el usuario ante el PRSTM que en la actualidad se encuentre prestando el servicio al usuario. Es decir, no deben existir variaciones en la gestión realizada por el PRSTM en virtud de la portación de un número. Sin embargo debe reiterarse que los procesos de reactivación de equipos que hayan sido reportados como hurtados y/o extraviados, debe ser realizada ante el PRSTM que efectuó el reporte a la base de datos negativa.

Por otro lado, es preciso resaltar que, en virtud de lo establecido en el artículo 5° del Decreto 1630 de 2011, los PRSTM deberán realizar la adecuación de sus redes y sistemas, y asumir los costos de dicha adecuación que implique el intercambio de información entre los PRSTM y la BDA. En tal sentido, es claro que las medidas que se prevén en la presente iniciativa no deben reflejarse en mayores costos para el usuario por concepto de la prestación de los servicios de telecomunicaciones.

En relación con lo anterior, en esta sección se presentan aspectos específicos relativos al reporte de equipos robados y/o extraviados y las posibles situaciones bajo las cuales puede darse la activación de equipos para la prestación del servicio de telefonía móvil.

3.2.1 Reporte de equipos terminales móviles hurtados y/o extraviados

En este punto, en primer lugar debe tenerse en cuenta que los usuarios se encuentran en la obligación de reportar las eventualidades de pérdida y/o hurto de los equipos terminales móviles, sin importar que sean o no titulares de la línea telefónica y, en tal sentido el Decreto 1630 de 2011 define claramente que los PRSTM podrán implementar mecanismos para que los usuarios realicen tales actividades.

Así mismo, de acuerdo con la información presentada por el Ministerio de TIC ³², en caso de hurto y/o pérdida, deben tenerse en cuenta los siguientes aspectos:

- Es necesario informar el hecho (pérdida y/o hurto) al proveedor.
- Para efectos de lo anterior, debe marcarse a la línea de atención del PRSTM. En el menú debe seleccionarse la opción "hurto".
- Dentro del proceso de reporte del evento, deben ser respondidas las preguntas de validación del sujeto que realiza el reporte, con el fin de poder confirmar que si bien no es el titular de la línea si es la persona que la utiliza constantemente.
- A continuación es necesario realizar el registro de la información del hurto y del modelo del equipo. En particular, es necesario señalar la fecha, hora y lugar del evento. Así mismo, es preciso indicar si se trata de un evento de pérdida o hurto, y en este último caso debe indicarse claramente el lugar de los hechos, así como particularidades de tal eventualidad.
- Con base en lo anterior, se ingresa a la base de datos negativa la información correspondiente al equipo, de tal modo que el IMEI del teléfono quede bloqueado en la red del proveedor.
- Dentro de los 5 minutos siguientes a la realización del reporte, el usuario podría verificar que la línea reportada se encuentra inactiva.

3.2.2 Condiciones de activación de equipos terminales móviles

A continuación se exponen las principales situaciones en que se puede encontrar el usuario al momento de interactuar con el PRSTM para efectos de habilitar un MS (Mobile Station –unión física de la SIM y el terminal) para la prestación del servicio de telefonía móvil. Es necesario mencionar

³² <http://www.mintic.gov.co/news.asp?articleId=352>

que, en los casos en que se encuentre una duplicación de IMEI, los PRSTM deberán adelantar la investigación correspondiente que permita definir la legalidad de uno de ellos, a partir de lo cual se mantendrá su inclusión en la base de datos positiva.

- **Adquisición de nueva línea de telefonía móvil y equipo terminal vendido por el PRSTM.** En este caso no se encuentra un registro previo de correspondencia de un código IMEI con una línea telefónica, por lo que el PRSTM procederá a registrar la información correspondiente a la identificación del usuario en la BDA y BDO.
- **Registro de equipo nuevo vendido por el PRSTM para su utilización con una línea telefónica existente.** En este caso, teniendo en cuenta que sólo puede relacionarse una línea telefónica del PRSTM y un IMEI, es necesario que el PRSTM realice la modificación en la base de datos positiva, para que sea habilitado el equipo/IMEI que se desea utilizar.
- **Registro de una nueva línea telefónica con un equipo terminal móvil existente.** Cuando un usuario adquiera una SIM, y no requiera el suministro de un terminal por parte del comercializador, se deberán adelantar las gestiones ante el PRSTM para que, tanto la SIM como el equipo/IMEI que decide utilizar, sean relacionados con el número de identificación del usuario en la BDO.
- **Solicitud de una nueva línea para su uso en un equipo legalmente adquirido en otro país.** Frente a esta situación, el PRSTM validará la documentación que el usuario presente para soportar la legalidad de la adquisición del terminal, y posteriormente deberá proceder a su inclusión en la BDA positiva asociando el IMEI al número de identificación del usuario y en la BDO positiva asociará el IMEI al IMSI del usuario.
- **Equipo nuevo legalmente adquirido en otro país, para su uso con una línea telefónica existente.** Al igual que en el caso anterior, teniendo en cuenta que sólo puede relacionarse una línea telefónica del PRSTM y un IMEI, es necesario que el usuario solicite al PRSTM la modificación en la base de datos positiva, para que sea habilitado el equipo/IMEI que se desea utilizar. Sin embargo, debe tenerse en cuenta que el PRSTM validará la documentación que el usuario presente para soportar la legalidad de la adquisición del terminal, y posteriormente deberá proceder a su inclusión en la base de datos positiva.
- **Uso de una línea telefónica con varios equipos terminales.** Sobre este aspecto, la CRC considera que el usuario debe solicitar al PRSTM la inclusión del equipo en la base de datos positiva, cada vez que realice el cambio del mismo. Lo anterior por cuanto sólo se permite que exista un IMEI habilitado por cada línea telefónica del PRSTM e identificación de usuario.
- **Uso de varias líneas telefónicas con un único equipo terminal.** De igual modo que en el caso anterior, habida cuenta que debe existir una relación directa entre la línea telefónica del PRSTM y el terminal móvil, el usuario debería solicitar ante el PRSTM la modificación de la información existente en la base de datos positiva, cada vez que se requiera realizar un cambio de línea telefónica del PRSTM.

4 APLICATIVO PARA LA EXPEDICIÓN DE CERTIFICADOS DE HOMOLOGACIÓN EN LÍNEA

En atención al mandato establecido por el artículo 4 del Decreto 1630 de 2011, las personas autorizadas para la venta de equipos terminales móviles nuevos y usados deberán entregar al

comprador, entre otros documentos, un certificado obtenido de la página web de la Comisión de Regulación de Comunicaciones en el cual conste que el equipo terminal móvil se encuentra debidamente homologado al momento de la venta al público.

Teniendo en cuenta lo anterior, a continuación se describirá brevemente la aplicación mediante la cual se expedirán los certificados de homologación por parte de la CRC a las personas autorizadas, se indicará el procedimiento de registro de las personas autorizadas en la aplicación, y se especificará el contenido del certificado y los mecanismos de verificación de los mismos.

En primera medida, es importante aclarar que el procedimiento de homologación de equipos terminales móviles es independiente de la aplicación que se describirá a continuación, dado que dicho procedimiento está establecido en el Capítulo I del Título XIII de la Resolución CRT 087 de 1997 y en la Circular 60 de 2007 y 76 de 2009 sin perjuicio de las modificaciones que la CRC realice al mismo como resultado de una revisión interna. En este sentido, se entiende que uno de los insumos fundamentales para el funcionamiento de la aplicación es precisamente la base de datos de modelos de terminales móviles que han sido homologados por la CRC hasta la fecha, y los que en un futuro se homologuen, información que será ingresada a la aplicación por la CRC al momento de la homologación de un nuevo modelo de equipo terminal móvil.

El aplicativo de expedición de certificados contendrá, además de la base de datos de modelos de equipos terminales móviles homologados mencionada, el listado de personas autorizadas tanto por los PRSTM como por el Ministerio de Tecnologías de la Información y las Comunicaciones, teniendo en cuenta que el aplicativo no expedirá certificados de homologación genéricos sino que serán específicos para cada modelo de equipo terminal móvil y para cada persona autorizada para la venta de equipos terminales móviles nuevos y usados.

Por lo anterior, las personas que sean autorizadas para la venta de equipos terminales móviles deberán ingresar al aplicativo y registrarse haciendo uso del número de registro que el Ministerio de Tecnologías de la Información y las Comunicaciones o el PRSTM le haya asignado. Al momento del registro de la persona en el aplicativo, se le solicitará un nombre de usuario y una contraseña que serán requisito para el ingreso al momento en que se requiera la descarga de un certificado. Es importante aclarar en este punto que cuando un PRSTM actúe como persona autorizada para la venta de equipos terminales móviles, éstos deberán surtir el mismo proceso de registro en el aplicativo.

Una vez se ingrese al aplicativo por la persona autorizada, ésta podrá generar certificados nuevos o consultar un histórico de los certificados expedidos. Para la expedición de certificados nuevos, la persona autorizada deberá ingresar la información correspondiente a la marca, el modelo y el IMEI del equipo terminal móvil que va a comercializar.

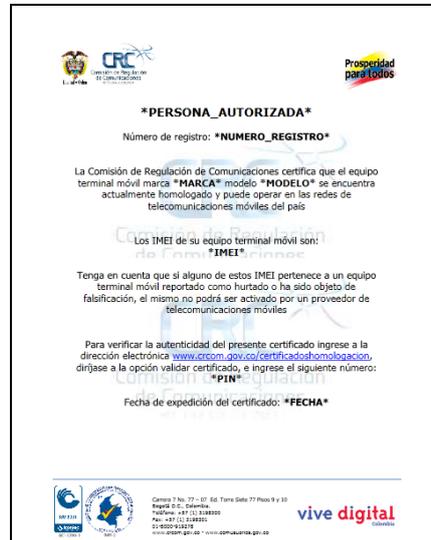
En consecuencia, cada certificado que expida el aplicativo contendrá la siguiente información:

- Nombre de la persona autorizada o establecimiento de comercio.
- Número de registro de la persona autorizada ante el Ministerio de Tecnologías de la Información y las Comunicaciones o ante un PRSTM.
- Marca y modelo del equipo terminal móvil.
- Los IMEI del equipo terminal móvil vendido, los cuales deben ser digitados en la aplicación por la persona autorizada al momento de la expedición del certificado. (Considerando que un equipo terminal móvil puede tener varios IMEI).
- Pin de verificación en línea del certificado

- Fecha de la venta del equipo terminal móvil

Un ejemplo del certificado que será expedido por el aplicativo es el que se observa en la Figura 10.

Figura 10. Ejemplo genérico de certificado de homologación



Fuente: Elaboración propia

Finalmente, los certificados tendrán un mecanismo de verificación en línea que permitirá a los compradores de los equipos terminales móviles corroborar la autenticidad de los mismos. El mecanismo de verificación se conforma de un número único por certificado que es generado automáticamente por la aplicación (PIN que se mencionó anteriormente), y mediante el cual una persona, entidad administrativa, policiva o judicial puede corroborar un certificado, accediendo a la dirección web www.crcm.gov.co/certificadoshomologacion e ingresando el número en comentario.

5 REGULACIÓN SOBRE LA AUTORIZACIÓN PARA LA VENTA DE EQUIPOS TERMINALES MÓVILES

5.1 DEFINICIÓN DE REQUISITOS PARA LA VENTA DE EQUIPOS TERMINALES MÓVILES

El artículo 3° del Decreto 1630 de 2011 establece de manera taxativa quiénes son las únicas personas autorizadas para la venta al público de equipos terminales móviles en Colombia, nuevos y usados, señalando lo siguiente: i) Los PRSTM; ii) Cualquier persona que los PRSTM autoricen en virtud de lo señalado en el artículo 4 del Decreto 1630 citado; iii) Cualquier persona que el Ministerio de Tecnologías de la Información y las Comunicaciones autorice, conforme a lo dispuesto en el artículo 4° del Decreto 1630 mencionado y a la regulación que para el efecto expida la CRC.

Por su parte, el artículo 4° del Decreto 1630 citado se ocupó de señalar, de manera determinable, los requisitos que deben cumplir quienes conforme al artículo 3° citado ostentan la calidad de personas autorizadas en Colombia para la venta al público de los equipos terminales móviles, nuevo y usados, enunciando los requisitos de la siguiente manera: i) Los previstos en la Ley 232 de 1995 o aquella que la modifique, sustituya o adicione; ii) Dar cabal cumplimiento a toda la normatividad

aplicable a las actividades comerciales, en especial la tributaria y aduanera; y iii) A la expedida por la CRC.

Al respecto, de manera preliminar, se quiere destacar que la regulación que expedirá esta Comisión en cumplimiento del artículo 4° del Decreto 1630, se circunscribirá a la autorización de las personas que venden o desean vender equipos terminales móviles en Colombia, y de ninguna manera se trata del establecimiento de requisitos nuevos o adicionales a los consagrados legalmente para la apertura o funcionamiento de los establecimientos de comercio de que trata el artículo 515 del Código de Comercio, esto último objeto de la legislación comercial colombiana, en consonancia con lo dispuesto en el artículo 1° de la Ley 232 de 1995.

De acuerdo con lo anterior, en primer lugar, resulta importante señalar que el mismo artículo 4° del Decreto 1630 reconoce el cumplimiento del lleno de los requisitos previstos en el artículo 2° de la Ley 232 de 1995, que debe dar toda persona que se dedica a las actividades comerciales de que trata el Código de Comercio, y en este caso concreto los comerciantes dedicados a la venta de equipos terminales móviles en Colombia respecto de sus establecimientos de comercio en donde se ofrecen al público tales equipos terminales. Para mayor ilustración, a continuación se transcribe el artículo 2° de la Ley 232 de 1995, de la siguiente manera:

“ARTÍCULO 2o. (...) es obligatorio para el ejercicio del comercio que los establecimientos abiertos al público reúnan los siguientes requisitos:

a) Cumplir con todas las normas referentes al uso del suelo, intensidad auditiva, horario, ubicación y destinación expedida por la autoridad competente del respectivo municipio. Las personas interesadas podrán solicitar la expedición del concepto de las mismas a la entidad de planeación o quien haga sus veces en la jurisdicción municipal o distrital respectiva;

b) Cumplir con las condiciones sanitarias descritas por la Ley 9a de 1979 y demás normas vigentes sobre la materia;

c) Para aquellos establecimientos donde se ejecuten públicamente obras musicales causante de pago por derechos de autor, se les exigirá los comprobantes de pago expedidos por la autoridad legalmente reconocida, de acuerdo con lo dispuesto por la Ley 23 de 1982 y demás normas complementarias;

d) Tener matrícula mercantil vigente de la Cámara de Comercio de la respectiva jurisdicción;

e) Comunicar en las respectivas oficinas de planeación o quien haga sus veces de la entidad territorial correspondiente, la apertura del establecimiento”.

En segundo lugar, el artículo 4° del Decreto 1630 de 2011, establece la obligación que tienen las personas autorizadas para vender equipos terminales móviles en Colombia de dar cabal cumplimiento a toda la normatividad vigente y aplicable a las actividades comerciales, haciendo énfasis en las normas tributarias y aduaneras, entre las cuales, se entiende que el comerciante que ofrece al público tales equipos terminales debe cumplir con sus obligaciones tributarias, así como cumplir con los procesos de importación y de nacionalización de bienes no producidos en el país, cuando al cumplimiento de estas últimas normas haya lugar, en especial, respecto de las normas y procedimientos que rijan el ingreso al país de equipos terminales móviles, por cualquiera de sus fronteras, de conformidad con lo que para el efecto establece la legislación vigente sobre la materia. No obstante, quien no siendo importador, ofrezca al público equipos terminales móviles producidos en el exterior, debe en todo caso cerciorarse de la procedencia legal de los mismos y conservar los soportes que evidencien el ingreso legal de dichos equipos al país.

En tercer lugar, teniendo en cuenta que el artículo 4° citado, señala como requisito adicional a los anteriormente descritos, aquéllos que expida la Comisión de Regulación de Comunicaciones, se identifica como condición previa para la venta de equipos terminales móviles en Colombia, el cabal cumplimiento del proceso de homologación ante la CRC que debe surtirse de acuerdo con lo dispuesto en el Capítulo I del Título XIII de la Resolución CRT 087 de 1997, en la Circular 60 de 2007 y aquéllas disposiciones que la modifiquen, adicionen o sustituyan.

Además de lo anterior, el párrafo 2 del artículo 3° del Decreto 1630, contempla el plazo máximo de dos meses contado a partir de la expedición de la regulación por parte de la CRC en cumplimiento de lo previsto en el Decreto 1630 de 2011, para que los comercializadores o establecimientos de comercio, que con corte al 19 de mayo 2011, fecha en que se expidió el Decreto 1630, ya se encontraban establecidos y ofrecían para la venta al público equipos terminales móviles, obtengan la autorización para la venta de sus equipos y den cabal cumplimiento a los requisitos previstos en los artículos 3° y 4° del Decreto 1630 de 2011.

5.2 PROCEDIMIENTO PARA LA AUTORIZACIÓN POR PARTE DEL MINISTERIO DE TIC DE PERSONAS INTERESADAS EN LA VENTA DE EQUIPOS TERMINALES MÓVILES

Teniendo en cuenta que en cumplimiento de lo dispuesto en el numeral 3° del artículo 3° del Decreto 1630 de 2011, corresponde a la CRC expedir la regulación por medio de la cual se establezca la manera como el Ministerio de TIC va a proceder con la autorización de personas jurídicas para vender equipos terminales móviles, esta Comisión identifica la necesidad de establecer un procedimiento tendiente a determinar las actividades que orientarán el análisis que deberá efectuar el Ministerio de TIC en cumplimiento del numeral 3° citado, sobre las solicitudes que dicha Entidad reciba sobre el particular, y la respectiva decisión de autorizar o no autorizar a las personas que le presenten tales solicitudes.

Adicionalmente, y en cumplimiento de lo dispuesto en el párrafo 1 del artículo 3°, el cual establece: *“La información sobre las personas autorizadas para la venta de equipos terminales móviles en Colombia deberá estar disponible y ser permanentemente actualizada para consulta del público en general, a través de las páginas Web de cada proveedor de redes y servicios de telecomunicaciones móviles y del Sistema de Información Integral administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones (...)”*, es necesario identificar el mecanismo a través del cual se estructurará la información a publicar.

En este orden de ideas, a continuación se enuncian las siguientes actividades que adelantará el Ministerio de TIC en desarrollo de dicho proceso de autorización, así:

- a. El Ministerio de TIC deberá crear una opción en su página Web, que permita la realización integral del trámite, de que trata el presente procedimiento, referente a la autorización para la venta de equipos terminales móviles.
- b. El Ministerio de TIC asignará un número de radicado a la solicitud tramitada en línea, con el fin que la persona interesada en conocer de su trámite, pueda comunicarse telefónicamente al Ministerio de TIC para obtener información sobre el estado del respectivo trámite.
- c. A través de dicho aplicativo la persona que solicite la autorización para la venta de equipos terminales móviles, deberá consignar la información requerida en el formato establecido para tal fin y adjuntar electrónicamente la documentación que acredite cada uno de los datos aportados en la inscripción.

- d. Una vez llevada a cabo la comprobación de la información suministrada con los documentos aportados, el Ministerio de Tecnologías de la Información y las Comunicaciones comunicará vía correo electrónico al interesado, en un plazo no superior a quince (15) días hábiles contados a partir del día siguiente de la radicación de la solicitud, si ha sido autorizado o no para la venta de equipos terminales móviles, y si es procedente su inscripción en el Registro de Autorizaciones para la Venta de Equipos Terminales Móviles.
- e. El Ministerio de TIC asignará un número único de verificación del certificado de autorización, el cual deberá incorporarse en el certificado de autorización y permitir la identificación del mismo así como la realización de las consultas públicas en línea del certificado de autorización, a través de la página Web del Ministerio de TIC.
- f. El Ministerio de TIC emitirá la certificación de autorización utilizando el formato que, como anexo al proyecto de resolución que se somete a discusión con el sector, establezca la CRC y su verificación deberá estar disponible para consulta de cualquier interesado, registro a registro, a través de la página Web del Ministerio de TIC.
- g. Para dar cumplimiento a lo establecido en el numeral (d) el Ministerio de TIC implementará El Registro de Autorizaciones para la Venta de Equipos Terminales Móviles, el cual deberá contener como mínimo la siguiente información:
 - 1. Razón social..
 - 2. Marca y/o enseña comercial..
 - 3. Número de Identificación Tributaria – NIT.
 - 4. Dirección(es) del (los) Establecimiento(s) de Comercio en donde se ofrecerán los equipos terminales móviles por parte de la persona autorizada.
 - 5. Número de Código de Autorización para la Venta de Equipos Terminales Móviles.

5.3 PROCEDIMIENTO PARA LA AUTORIZACIÓN POR PARTE DE LOS PRSTM DE PERSONAS INTERESADAS EN LA VENTA DE EQUIPOS TERMINALES MÓVILES

Los PRSTM en cumplimiento del numeral 2° del artículo 3° del Decreto 1630 de 2011, para efectos de atender las solicitudes que eleven a través de sus oficinas físicas o virtuales, las personas interesadas en vender equipos terminales móviles, deberán observar el cumplimiento del siguiente procedimiento, sin perjuicio de los tiempos y procedimientos que han estipulado contractualmente en el marco de sus negociaciones privadas con sus agentes o distribuidores, así:

- a) Recibir y radicar las solicitudes que presenten las personas interesadas en obtener la autorización para la venta de equipos terminales móviles en Colombia, por medios físicos o electrónicos a través de sus oficinas físicas o virtuales de que trata la Resolución CRT 1732 de 2007 (vigente hasta el 30 de septiembre de 2011 y que será sustituida por la Resolución CRC 3066 de 2011).
- b) Estudio de documentos que se presentan con la solicitud, a través de medios físicos o electrónicos, así como verificar el cumplimiento del lleno de los requisitos previstos en el artículo 4° del Decreto 1630 de 2011.
- c) En un plazo no superior a quince (15) días hábiles contados a partir del día siguiente de la radicación de la solicitud, expedir la certificación de autorización, si a ello hay lugar. En caso

contrario, dar respuesta al solicitante, informando las razones de la negativa. El PRSTM emitirá la certificación de autorización utilizando el formato que, como anexo al proyecto de resolución que se somete a discusión con el sector, establezca la CRC y su verificación deberá estar disponible para consulta de cualquier interesado, registro a registro, a través de la página Web del PRSTM, conforme lo ordena el parágrafo 1° del artículo 3° del Decreto 1630 de 2011.

- d) Publicación del listado que contenga el nombre o la razón social de todas las personas autorizadas por el respectivo PRSTM para vender equipos terminales móviles, la ciudad, la dirección, teléfonos de contacto y correo electrónico, así como el nombre del representante legal de la persona autorizada. Dicho listado deberá ser remitido por cada PRSTM al Ministerio de Tecnologías de la Información y las Comunicaciones en las condiciones técnicas que éste último defina y deberá estar disponible para consulta de cualquier interesado a través de la página Web de cada PRSTM, asistido por herramientas que permitan al menos la búsqueda por ciudad.
- e) Utilización del número único de verificación que establezca el Ministerio de Tecnologías de la Información y las Comunicaciones para incorporar a cada Certificado de Autorización. Certificado que deberá exhibir en lugar visible toda persona autorizada (por parte del Ministerio de Tecnologías de la Información y las Comunicaciones o de los PRSTM) que ofrece al público equipos terminales móviles, en cumplimiento de lo dispuesto por el parágrafo 1° del artículo 3° del Decreto 1630 de 2011.
- f) Asignación de un número único de verificación del certificado de autorización, el cual deberá incorporarse en el certificado de autorización y permitir la identificación del mismo así como la realización de las consultas públicas en línea del certificado de autorización, a través de la página Web del Ministerio de Tecnologías de la Información y las Comunicaciones y a través del PRSTM que lo expidió.

El trámite a través del Ministerio de Tecnologías de la Información y las Comunicaciones y de los PRSTM, a que se ha hecho referencia, deberá realizarse sin excepción por parte de todas las personas que a 19 de mayo de 2011, se encontraban establecidos u ofreciendo al público equipos terminales móviles. A elección del interesado se presentará la solicitud de autorización, ante el Ministerio de Tecnologías de la Información y las Comunicaciones o ante los PRSTM de su elección.

Por su parte, la regulación establece un trámite que garantiza el cumplimiento del debido proceso de la solicitud, el cual se surtirá en forma idéntica tanto por parte del Ministerio de Tecnologías de la Información y las Comunicaciones como por parte de los PRSTM.

Ahora bien, en lo que a las personas jurídicas extranjeras interesadas en la obtención de solicitudes de autorización se refiere, es claro que éstas podrían obtener tal certificado de autorización si cumplen con las normas establecidas en el Decreto 1630 de 2011 o aquéllas que lo modifiquen, adicionen o sustituyan, así como en lo dispuesto por la regulación que expida la Comisión de Regulación de Comunicaciones sobre la materia.

Finalmente, en cuanto al certificado de autorización, es claro que por el hecho de iniciarse un trámite ante el Ministerio de Tecnologías de la Información y las Comunicaciones o ante los PRSTM, no le permite al interesado considerarse como persona autorizada hasta tanto no se expida la respectiva autorización, y en tal sentido, no podrá vender equipos terminales móviles hasta tanto no ostente la calidad de persona autorizada para tal venta.

6. MODIFICACIONES AL NUEVO RÉGIMEN DE PROTECCIÓN DE LOS DERECHOS DE LOS USUARIOS DE LOS SERVICIOS DE COMUNICACIONES

En relación con las disposiciones tendientes a proteger al usuario de los servicios de comunicaciones, resulta importante destacar que esta Comisión desde el año 2007 incorporó en la Resolución CRT 1732 de 2007 una disposición tendiente a la prevención del uso, por parte de los usuarios, de equipos terminales móviles hurtados y/o extraviados en la red de los PRSTM, norma que contempló en su oportunidad la obligación de los PRSTM de llevar una base de datos de los equipos terminales que hubieran sido reportados como extraviados, hurtados o desactivados por fraude o por no pagar ninguna factura recibida con posterioridad a la venta del equipo, base de datos que debía ser compartida y actualizada entre PRSTM diariamente.

Es así como, considerando la importancia que reviste la medida regulatoria antes descrita, la CRC mantiene dicha disposición en la reciente expedición del régimen integral de protección de los derechos de los usuarios de los servicios de comunicaciones contenida en la Resolución CRC 3066 de 2011, cuya implementación inicia el 1° de octubre de 2011.

En este orden de ideas, si bien ya existe en el Nuevo Régimen de Usuarios una medida que establece la obligación que tienen los PRSTM de gestionar una Base de Datos Negativa, se ha identificado la necesidad de modificar la reciente Resolución CRC 3066 de 2011, en el sentido de fortalecer la medida asociada a la Base de Datos Negativa, así como de generar algunas adiciones específicas al numeral 10.2 del artículo 10 de la Resolución CRC 3066 de 2011 relativos a las obligaciones de los usuarios, de manera que sean claros los deberes de los usuarios de reportar de inmediato el hurto y/o extravío de sus equipos terminales móviles, no sólo a las autoridades policivas y judiciales, sino de manera prioritaria al PRSTM que le presta el servicio.

Por último, se identifica la necesidad de modificar el artículo 4° que establece el principio de libre elección, en virtud del cual se hace necesario contemplar que si bien el usuario es el único que puede elegir libremente el equipo de su preferencia, de acuerdo a sus necesidades, debe garantizarse el correcto funcionamiento del equipo de elección del usuario, razón por la cual, dicho equipo deberá ser adquirido a través de las personas autorizadas o puntos de venta autorizados por el Ministerio de Tecnologías de la Información y las Comunicaciones o los PRSTM, de conformidad con la publicación que realice de manera permanente y actualizada el Ministerio de Tecnologías de la Información y las Comunicaciones en su página Web.