COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Simplificación del marco regulatorio para la restricción de equipos terminales hurtados

Documento de Formulación del Problema

Planeación Estratégica

Abril de 2019

El futuro es de todos
Gobierno de Colombia

CONTENIDO

Simplificación del marco regulatorio para la restricción de equipos terminales hurtados

1. INTRODUCCIÓN

El impacto que genera el hurto de teléfonos móviles representa costos enormes y constantes a la sociedad. Solo en Estados Unidos se estima que la cifra asciende a los $ 30 mil millones de dólares anuales[1]. En principio dicha cifra puede parecer alta, sin embargo, resulta fácil concebirla cuando se considera que los costos pueden incluir no solo el reemplazo de los teléfonos, sino también los costos relacionados con la pérdida de datos personales y financieros, las reparaciones de automóviles y hogares donde ocurren los robos, los costos de los servicios médicos y de salud, los costos emocionales y otros asociados a la salud psicológica y victimización, así como lesiones a las víctimas y sus familias, el costo para la sociedad de la pérdida de productividad, el incremento en la vigilancia policial y el sistema de justicia penal.

Para hacer frente a los impactos mencionados, el Gobierno Nacional en cabeza de la Presidencia de la Republica, con el acompañamiento del Ministerio de TIC, la CRC, El Ministerio de Defensa, el Ministerio de Justicia y del Derecho, el Ministerio de Hacienda, el Ministerio de Comercio, Industria y Turismo, la Fiscalía General de la Nación y la industria móvil del país, han desarrollado desde el 2011 una estrategia para combatir esta problemática. Sin embargo, si bien el impacto que genera el hurto de teléfonos proporciona un marco general, el enfoque específico de este documento será el análisis de la eficiencia de las medidas adoptadas en Colombia para restringir la operación de equipos que han sido reportados como hurtados y extraviados. De ahí que, el presente documento no busca plantear medidas adicionales para la mencionada estrategia, sino indagar sobre la eficiencia de las medidas adoptadas por la CRC para hacer frente a esta problemática.

[1] Mailley, J, Garcia, R, Whitehead, S, & Farrell, G. (2008). Phone theft index. Security Journal, 21(3), 212–227.

Con respecto a las medidas adoptadas por la CRC, hay que mencionar que las mismas se desarrollan en su mayor parte en torno al control de los identificadores únicos de los teléfonos móviles. Así las cosas, para entender cómo estos identificadores pueden utilizarse para restringir el uso de teléfonos hurtados, debe considerarse que, de manera similar a la forma en que los ciudadanos tenemos un número de identificación único denominado Cédula de Ciudadanía, cada teléfono tiene un número de identificación único de 15 dígitos denominado IMEI[2]. Así, cuando se enciende un teléfono, el mismo utiliza el número IMEI para iniciar sesión en la red, además de iniciar sesión en la tarjeta SIM[3]. Ahora bien, la identificación de la tarjeta SIM determina quién recibe la factura por los cargos de la red, y es independiente de la identificación IMEI del teléfono; a su vez, las tarjetas SIM pueden cambiarse de un teléfono a otro, ya que tanto la tarjeta SIM como los teléfonos retienen sus identidades separadas. Por lo tanto, en teoría, cuando se informa de un dispositivo robado, se producen dos cosas: el proveedor de la red bloqueará, por un lado, la tarjeta SIM para que el suscriptor no reciba cargos adicionales de red (independientemente del teléfono que se use con esa tarjeta SIM) y por otro lado el teléfono robado. Surtido este proceso, el número IMEI se agrega a una lista (lista negra) de dispositivos a las que no se les permite acceder a la red que se conoce como la base de datos negativa.

El esquema planteado por la CRC se complementa con una lista blanca que incluye todos los IMEI asociados con teléfonos que han sido importados y adquiridos legalmente, y con otra lista blanca de dispositivos que han sido homologados y aprobados para su conexión a las redes locales. Estas listas son conocidas como la base de datos positiva y la base de datos de equipos homologados, de modo que, durante el proceso de inicio de sesión se valida, no solo si el teléfono ha sido reportado como robado o extraviado, sino si el mismo ingresó de manera legal al país y si se trata de un dispositivo idóneo para la conexión en las redes nacionales.

Posteriormente, para fortalecer el esquema de control, la CRC expidió una serie de medidas que permiten la detección de teléfonos a los que se les ha practicado alguna forma de alteración del IMEI. La implementación de estos controles implica una validación diaria de todos los IMEI con actividad en

[2] De las siglas en inglés de *International Mobile Equipment Identity*, Identidad Internacional de Equipo Móvil.
[3] De las siglas en ingles de S*ubscriber Identity Module*, Módulo de identidad del suscriptor.

las redes nacionales. Para las tipologías de alteración más sofisticadas, la validación puede implicar el procesamiento de diversos parámetros de red como la ubicación del dispositivo, la estación base asociada, la fecha y hora de conexión, entre otros.

La formulación de problema presentada en este documento inicia en la sección 2 con un análisis de los elementos que limitan la efectividad del esquema de control a través de listas negras, dichos elementos se sintetizan en un árbol de problema al final del capítulo. Las secciones 3 y 4 analizan las causas y consecuencias del problema identificado respectivamente; finalmente la sección 5 presenta un análisis de los agentes involucrados en la problemática identificada.

Abreviaturas

AIN:	Análisis de Impacto Normativo
CDR:	Charging Data Record
CRC:	Comisión de Regulación de Comunicaciones
DANE:	Departamento Administrativo Nacional de Estadística
ETM:	Equipo Terminal Móvil
EIR:	(Equipment Identity Register) Registro de la Identidad de Equipos.
GSM:	(Global System for Mobile communications) Sistema Global para Comunicaciones Móviles, por su sigla en inglés.
GSMA:	(GSM Association) Agremiación global de operadores de comunicaciones
IMEI:	(International Mobile Equipment Identity), identidad internacional de equipo móvil
IP:	Internet Protocol
ISP:	Proveedores de Servicios de Internet
MinTIC:	Ministerio de Tecnologías de la Información y las Comunicaciones
OCDE:	Organización para la Cooperación y el Desarrollo Económicos
OMV	Operador Móvil Virtual
PRST:	Proveedores de Redes y Servicios de Telecomunicaciones
PRSTM	Proveedores de Redes y Servicios de Telecomunicaciones Móviles
UIT:	Unión Internacional de Telecomunicaciones

2. DEFINICIÓN DEL PROBLEMA

La literatura especializada ha establecido que la industria está mejor posicionada que los gobiernos para desarrollar medidas contra la delincuencia para sus propios productos y servicios[4]. Esto se debe a que la industria relevante tiene el conocimiento técnico y la información de mercado. Sirve de ejemplo la industria automotriz, donde el robo de automóviles se incrementó rápidamente durante los años 60, 70 y 80, lo cual derivó en una serie de sistemas de seguridad considerablemente mejorados en las décadas siguientes, introduciendo tecnologías de inmovilización[5], autenticación cifrada de las llaves, rastreo remoto, entre otras. Sin embargo, la adopción de estas medidas requirió de un periodo de tiempo considerable, y con frecuencia fue el resultado de escándalos públicos como el generado por la publicación de un índice de robo de automóviles[6], o la implementación de regulación. Así mismo, la sincronización temporal en la implementación de inmovilizadores electrónicos en diferentes países sugiere que la regulación, o la señal de una eventual expedición de regulación, tiende a desempeñar un papel clave en la adopción de medidas[7].

En el caso de la industria de telecomunicaciones, también es posible encontrar evidencia de que los agentes de mercado pueden responder de manera eficiente y efectiva. Por ejemplo, en el caso de las llamadas fraudulentas que utilizaban "clones" de teléfonos, y que en su momento costaron a la industria millones de dólares (en el mercado estadounidense se estima que este tipo de fraude tenía impactos fiscales de cerca de 800 millones de dólares anuales) la respuesta fue certera y efectiva[8] e involucró la introducción de medidas tecnológicas como la autenticación de tarjetas SIM. Sin embargo, cuando se trata del hurto de teléfonos, algunos autores[9] han planteado que no existen incentivos suficientes para

---

4 Clarke, RV, & Newman, G. (2005). Modifying criminogenic products: What role for government?'. In R. V. Clarke & G. Newman (Eds.), Designing out crime from products and systems. Monsey, NY: Criminal Justice Press.
5 Brown, R. (2004). The effectiveness of electronic immobilization: Changing patterns of temporary and permanent vehicle theft'. In M. G. Maxfield & R. V. Clarke (Eds.), Understanding and Preventing Car Theft.
6 Laycock, G. (2004). The UK Car Theft Index: An example of government leverage'. In M. G. Maxfield & R. V. Clarke (Eds.), Understanding and Preventing Car Theft
7 Ibid.
8 Clarke, RV, Kemper, R, & Wyckoff, L. (2001). Controlling cell phone fraud in the U.S. Security Journal, 14.
9 Farrel G. (2015). Preventing phone theft and robbery: The need for government action and international coordination, Crime Science An Interdisciplinary Journal.

que el sector privado genere de manera autónoma esquemas de control. Lo anterior, sugiere que el gobierno y el marco regulatorio juegan un papel importante a la hora de proteger a los consumidores.

Ahora bien, aun cuando se han propuesto diversas medidas contra el hurto de teléfonos en otros lugares del mundo, entre las que se cuentan medidas como seguros físicos y cordones atados al propietario, instalación de herrajes dedicados en cafeterías y otros lugares donde puede presentarse el delito, entre muchos otros, una revisión de la literatura dedicada revela que la mayor parte de estas medidas no han sido evaluadas en términos del impacto en la prevención del delito[10]. Otras tácticas policiales incluyen redadas en comercios donde se venden teléfonos robados y medidas para enfrentar a los grupos de delincuencia organizada. Otro grupo de medidas que ha sido propuesto es el dedicado al uso de sensores biométricos (introducidos recientemente en la mayor parte de los smartphones como el lector de huellas dactilares) y otras características de diseño de los teléfonos[11], sin embargo, no se ha llegado aún a conclusiones acerca de su efectividad. No obstante, la principal actividad preventiva implementada en varios países y estandarizada por la industria ha sido el uso de "listas negras", y es el esquema sobre el cual la CRC basó sus medidas de control.

El esquema de listas negras parte de la premisa que cada teléfono tiene un número de identificación único de 15 dígitos denominado IMEI, por lo tanto, en teoría, al momento de iniciar sesión en la red es posible validar y restringir la operación de un dispositivo, si el mismo ha sido reportado como robado, y si se cuenta con un registro (lista negra) centralizado de dichos números IMEI.

Sin embargo, resulta evidente que un teléfono reportado como robado en una red podría ser usado en una red diferente. Así, la implementación de un sistema de lista negra efectiva requiere de coordinación nacional e internacional. Para ser más específicos, a nivel nacional, una vez que todos los proveedores de red aceptan utilizar un sistema de lista negra, los operadores deben compartir sus listas negras actualizadas diariamente en un registro nacional de identidad de equipos - EIR[12]. No obstante, para

---

10 Whitehead, S, Mailley, J, Storer, I, McCardle, J, Torrens, G, & Farrell, G. (2008). Mobile phone anti-theft designs: A review. *European Journal on Criminal Policy and Research*

11 McCardle, J, Storer, I, Whitehead, S, Mailley, J, Torrens, G, & Farrell, G. (2011). Offending users: Designing in deterrence with mobile phones'. The Design Journal, 14(3), 323–342

12 De las siglas en ingles de Equipment Identity Register.

garantizar la efectividad del sistema, cada EIR nacional debe incorporarse internacionalmente a través de la base de datos internacional de IMEI. Luego, la base de datos internacional y los EIR nacionales combinan las listas negras y devuelven las listas completas a todos los proveedores de red, para que todos puedan incluir en la lista negra todos los teléfonos robados, de modo que, en teoría, esto debería eliminar por completo el incentivo para el hurto de celulares porque un teléfono robado no funcionaría en ninguna parte.

De la forma en que fue ideado, el sistema de lista negra es un medio en principio eficaz para abordar el hurto de teléfonos. Sin embargo, existe una brecha entre la teoría y la práctica, brecha que se sustenta generalmente en las debilidades tecnológicas para asegurar que un identificador único sea inmodificable.

La base de datos internacional de IMEI ha sido implementada desde hace dos décadas, sin embargo, el hurto de teléfonos continúa, sin que se evidencien cambios significativos en las cifras, o sin que se pueda contener la adaptabilidad de las conductas delictivas a los controles implementados. A continuación, se exploran algunas de las limitaciones del sistema de listas negras e introducen el problema que se crea al tratar de superar dichas limitaciones.

2.1 Baja adopción internacional de sistemas de EIR y de compartición de listas negras.

La implementación global de sistemas de EIR es un obstáculo frecuente en la adopción de sistemas de listas negras. Si bien la base de datos de IMEI (IMEI DB[13]) es mantenida y recomendada por la asociación mundial de GSM desde el 2002, el número de países que la usan sigue siendo pequeño. Para febrero de 2019[14] alrededor de 119 operadores en 41 países se encontraban conectados a la base de datos de IMEI.

[13] IMEI database: disponible para los stakeholders involucrados en: https://imeidb.gsma.com/imei/loginpage
[14] Comunicado de la GSMA sobre la base de datos de IMEI: https://www.gsma.com/services/wp-content/uploads/2019/02/imei_bl_a5_web_2_02_19.pdf

Si bien desde el 2015 más operadores se han conectado a la base de datos, la cobertura internacional de la lista negra sigue siendo limitada, y un estudio de la *Canadian Wireless Telecommunications Association* evidenció que los países identificados como los principales países de destino en África y Asia, tienen poco despliegue de esquemas de lista negra y bloqueo[15].

En Colombia la información aportada por las autoridades evidencia que los principales países de destino son los países dentro del continente americano los cuales, en su mayoría, están vinculados a la base internacional de IMEI, sin embargo, no puede desconocerse que mientras existan mercados internacionales que no implementen sistemas de listas negras la efectividad del sistema en general puede verse afectada.

Gráfica 1 Países con algún operador móvil conectado a la IMEI DB.

Fuente: GSMA

2.2 Reprogramación.

La reprogramación es una respuesta adaptativa de los delincuentes a la implementación de listas negras. Para ser más específicos, en algunos teléfonos robados es posible modificar el identificador único para

[15] CWTA (2012), Comparison of International Handset Security Measures, https://www.cwta.ca/wp-content/uploads/2011/09/Comparison-of-International-Handset-Security-Measures-2012-08-13.pdf

que estos puedan volver a ingresar al mercado y el software del teléfono puede ser reprogramado para cambiar el IMEI a uno que no se encuentre en la lista negra y que sea válido en la red.

Para comprender mejor el alcance del problema, debe considerarse que actualmente se encuentran disponibles en el mercado diferentes herramientas que permiten la reprogramación de teléfonos. La investigación de Krishan Kumar (2015)[16] encontró que es posible modificar el IMEI con técnicas basadas en hardware y técnicas basadas en software:

i. Técnicas basadas en hardware: Se utiliza principalmente en teléfonos antiguos (vulnerabilidad prevalente en dispositivos Nokia), basta con reemplazar el chip RX12 en el teléfono móvil[17].
ii. Técnicas basadas en software: Para cambiar los IMEI existen varias herramientas móviles y flashers de hardware, para los siguientes fabricantes de chipset es posible encontrar herramientas de reprogramación pagadas o gratuitas:

Tabla 1. Lista de herramientas disponibles para cambiar el IMEI

S. No.	Fabricante de chipset	Herramientas usadas para cambiar el IMEI	Fabricantes de teléfonos que usan el Chipset
1	MediaTek (MTK)	MTK Droid Root and Tools, MobileUncletool, SP flash tool, SigmaKey.	Samsung, HTC, LG, Motorola, Micromax, Lava, Lenovo, Panasonic etc.
2	QualComm Snapdragon	NV- items_Reader_Writer_tool Sigmakey.	Samsung, NOKIA, HTC, LG, Lenovo, Xiaomi, Micromax etc.
3	Broadcom	Sigmakey, Repair 3G tool, BrcmFlashTool, MultiFun Tool.	Samsung, Lava, Karbonn, Micromax, etc.
4	Apple A4, A5, A6.	Ziphone	Apple iPhone, iPad

Fuente: *International Journal of Computer Science and Mobile Computing Science.*

La reprogramación de algunos teléfonos se ha vuelto más complicada, y algunos fabricantes han introducido medidas para evitar el acceso por software al chipset. De otra parte, algunos teléfonos inteligentes tienen una batería interna no extraíble y la carcasa es más difícil de abrir incrementando

[16] Krishan Kumar et al, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, May- 2015, pg. 527-533
[17] Ibid.

así la experiencia y pericia necesaria para reemplazar físicamente un chip en lugar de alterar el software. Sin embargo, hay páginas web que ofrecen instrucciones sobre cómo cambiar el identificador en la mayor parte de los modelos disponibles en el mercado, más aún si se considera que, según datos de Device Atlas en Colombia para el 2018, alrededor del 75% de los smartphones funcionan con el sistema operativo Android[18] donde los controles adicionales para prevenir el acceso al chipset dependen de cada fabricante y no se encuentran estandarizados.

Considerando lo expuesto hasta ahora, es necesario analizar las consecuencias de la reprogramación de terminales en el funcionamiento del sistema de control a través de lista negra. Resulta entonces evidente que, la premisa de que el identificador de cada teléfono es único, se ve comprometida por la reprogramación, por lo que no bastará con validar el IMEI contra la lista negra de dispositivos sino que será necesario realizar validaciones adicionales para verificar que el mismo no haya sido alterado. Para ser más precisos, la alteración de un IMEI resultará en tres tipologías distintas de reprogramación:

i. *Sin formato:* Es la más simple de las alteraciones. En este caso el delincuente realiza una reprogramación de IMEI sin respetar los estándares definidos por la industria[19], una validación de los caracteres, longitud y dígitos del identificador resultan suficientes para detectar la reprogramación y proceder al control.
ii. *Inválido:* En este tipo de alteración la reprogramación del IMEI respeta el formato definido en los estándares de industria, sin embargo, una validación de los dígitos que identifican la marca y el modelo del dispositivo, revelarán que se trata de un identificador que no ha sido asignado por la industria.
iii. *Duplicado:* Es el más sofisticado de los modos de reprogramación. En este caso el delincuente replica un número de IMEI válido. En algunos casos los delincuentes replican directamente números de IMEI ya validados, pero en otros casos utilizan números de identificación casi idénticos pero plausibles que solo son detectados como duplicados al momento en que el

[18] Share de dispositivos por SO: https://deviceatlas.com/blog/android-v-ios-market-share#colombia
[19] 3GPP TS 22.016- Technical Specification Group Services and System Aspects- International Mobile station Equipment Identities (IMEI) y 3GPP TS 23.003 - Technical Specification Group Core Network and Terminals - Numbering, addressing and identification

dispositivo original es registrado en las redes. Este tipo de alteración es la más complicada de detectar y requiere de una validación del conjunto de identificadores tanto del dispositivo como de la tarjeta SIM. La dupla de identificadores debe luego verificarse en los registros diarios de llamadas en busca de inconsistencias, bien sea de un IMEI realizando una llamada con dos SIM cards al mismo tiempo, o de un mismo IMEI realizando llamadas en lugares geográficos incompatibles con el tiempo de análisis.

2.3 Mercado de partes.

El siguiente aspecto trata del mercado de partes de teléfonos móviles. En noviembre de 2018 SquareTrade una de las empresas aseguradoras más importantes del mercado norteamericano reveló que en EE.UU. durante el 2017 los propietarios de smartphones rompieron accidentalmente más de 50 millones de pantallas de teléfonos (casi dos por segundo), cuyo reemplazo costó a la sociedad cerca $3.4 mil millones de dólares[20]. El estudio encontró que el 66% de los propietarios de smartphones dañaron sus teléfonos en el último año, siendo el daño de pantallas el daño más común (56%) seguido de los problemas de batería (22%). Adicionalmente, si se tiene en cuenta que en promedio, el costo de reparación de pantallas fue de $170 dólares y que dicha cifra puede alcanzar los $329 para los equipos de alta gama, resulta claro que aún si los controles diseñados para prevenir la reconexión de teléfonos alcanzaran la máxima efectividad y garantizaran la imposibilidad del uso de teléfonos robados a nivel mundial, existiría una demanda remanente de dispositivos hurtados por la rentabilidad del mercado secundario de partes. Una evidencia adicional de este fenómeno son los cientos de anuncios diarios de smartphones de la línea iPhone vendidos en portales como ebay.com donde se especifica que los dispositivos no funcionan por bloqueo en la base de datos iCloud, pero que aun así son transados por un porcentaje considerable de su valor de mercado.

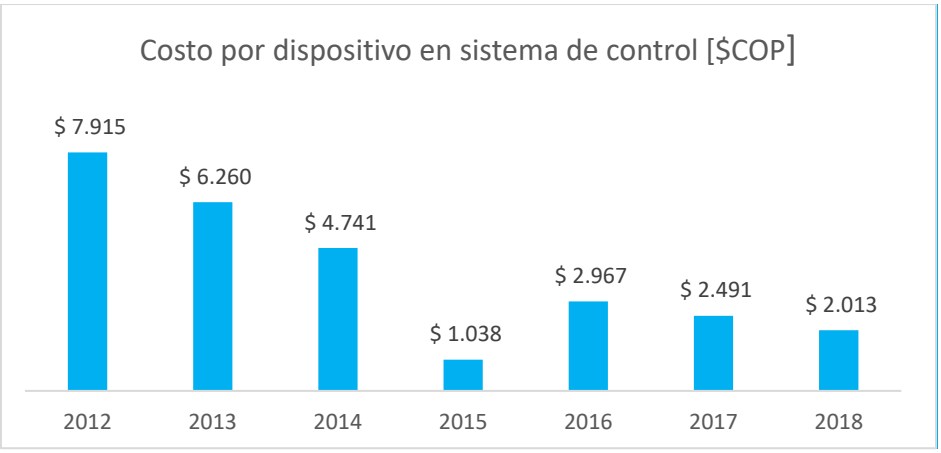
[20] https://www.squaretrade.com/press/Mobile-myths-cost-consumers-dearly-Americans-report-spending-3.4-billion-replacing-millions

2.4 Síntesis del problema

Una vez analizados los desafíos que deben ser superados cuando se implementa un sistema de control a través de listas negras, los cuales incluyen el bajo porcentaje de compartición global de la base de datos internacional de IMEI de la GSMA, la alteración de IMEI y el mercado de partes secundarias, es posible entender por qué el sistema ha requerido de una extensa reglamentación y de ajustes periódicos continuos. Por lo tanto, resulta pertinente introducir en este análisis una medida de eficiencia de la normatividad expedida en la materia. Para este estudio se considera como un indicador de eficiencia de las medidas el número de dispositivos identificados y sujetos a control, dividido entre el costo diferencial de implementación de las medidas.

Para construir el indicador se tomaron los datos reportados por los operadores en el marco del análisis de impacto del marco regulatorio 2015-2017. Estos datos fueron el resultado de una solicitud de información dirigida a los operadores de servicio móvil celular PRSTM y OMV con el propósito de establecer los costos totales imputados a las resoluciones de hurto de la CRC. El indicador representado en la Gráfica 2 se construye entonces utilizando los datos de dicho reporte y los datos del consolidado de dispositivos bloqueados que monitorea mensualmente la CRC.

Gráfica 2 Promedio de los costos por dispositivo bloqueado para cada año, incurridos por los operadores debido a la implementación del sistema para bloqueos IMEI y bases de datos[21]



Fuente: Elaboración propia CRC.

Así las cosas, se evidencia una progresiva reducción del costo por dispositivo durante la primera fase de implementación de las medidas (2011 a 2015), un comportamiento positivo que se ve interrumpido por la implementación de la segunda fase de medidas (2016 a 2018). Si bien la medida de eficiencia retoma un comportamiento positivo hasta el 2018, la eficiencia no retorna a los valores mínimos alcanzados en el 2015. Una preocupación adicional es que se repita la necesidad de adaptar las medidas para responder a otras dinámicas de hurto en el futuro, pues, como se verá más adelante, la literatura especializada concluye que la necesidad continua de adaptar las medidas de control es una característica común en el desarrollo de políticas de lucha contra el crimen.

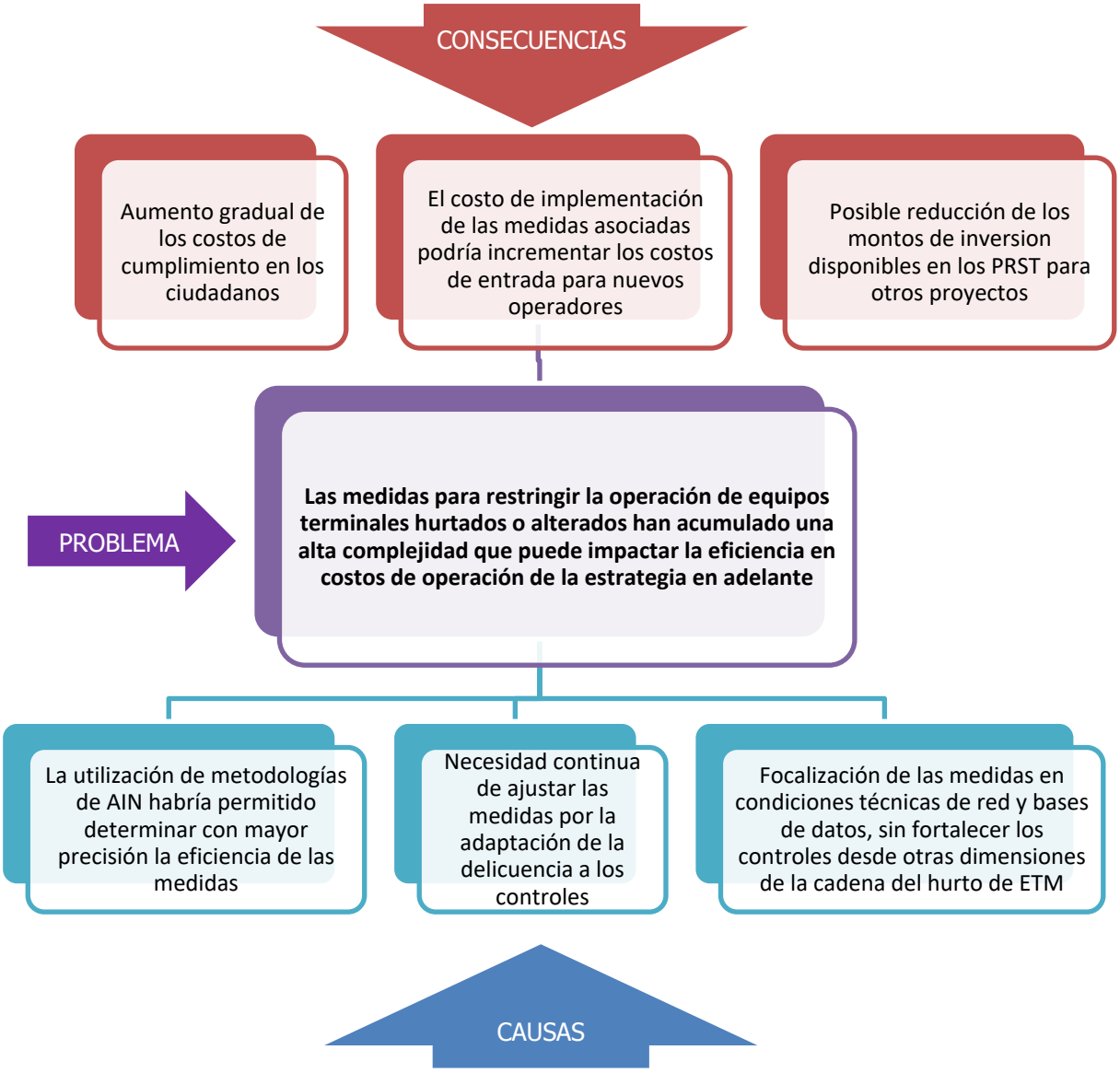
En conclusión, los ajustes continuos realizados al esquema de control para suplir las limitaciones del sistema (Alteración de IMEI, mercado de partes, compartición global), han conducido a un alto nivel de complejidad en su operación lo que a su vez a impacto negativamente en la eficiencia respecto al costo diferencial de implementación de las medidas.

[21] Solo se tuvieron en cuenta los PRSTM, no todos los operadores reportaron los mismos años, para el 2012, 2013 y 2014 los datos corresponden a un solo operador, para el 2015 a 2, para el 2016 en adelante a 3, el numero de dispositivos bloqueados se ajustó por operador para mantener la coherencia del indicador.

Esta problemática evidencia la necesidad no solo de buscar formas de simplificación del marco normativo vigente, sino también de que a futuro la CRC logre minimizar el impacto en la eficiencia generado por los ajustes realizados al sistema de control.

Las causas y consecuencias de la problemática se resumen en el siguiente diagrama y serán evaluadas en detalle en las siguientes secciones del documento.

Ilustración 1. Árbol de problema



Fuente: Elaboración propia CRC

3. CAUSAS DEL PROBLEMA

3.1 Necesidad continua de ajustar las medidas

Las investigaciones alrededor de las medidas para la prevención del crimen demuestran que los delincuentes suelen adaptarse a las medidas preventivas existentes. En este sentido, algunos autores[22] plantean que tales adaptaciones y contra-adaptaciones *de la "lucha contra el crimen"*, pueden modelarse como luchas evolutivas prolongadas, o como carreras armamentísticas. En este tipo de dinámicas, es necesario "correr" simplemente para permanecer en el mismo lugar. Ejemplos clásicos son la evolución de la caja fuerte, las monedas y billetes, y más recientemente los medios de pago electrónico. Una vez iniciadas, las carreras de armas pueden desarrollarse a un ritmo irregular. En cualquier punto de la secuencia criminal evolutiva, podemos encontrar brotes o "*ataques sorpresa evolutivos*", donde una nueva táctica, herramienta o arma estará disponible y, al menos durante un tiempo, sobrepasan las defensas de la oposición.

La experiencia en la implementación de las medidas para la restricción de equipos terminales móviles hurtados en Colombia no difiere de este modelo y las diferentes tipologías de alteración de IMEI pueden ser entendidas como una forma de adaptación. Adicionalmente, algunos investigadores en el campo de la seguridad digital han planteado otras formas de ataque a través del protocolo SS7[23][24], que permitirían el desbloqueo de dispositivos. A raíz de esta dinámica, la CRC y la institucionalidad involucrada en la estrategia de restricción de la operación de equipos terminales móviles hurtados se ve en la necesidad constante de responder a las adaptaciones desarrolladas por la criminalidad organizada. Un posible indicador del desarrollo constante que requieren las medidas es el número de precisiones y propuestas que ha surtido el marco regulatorio asociado, las cuales ya acumulan 23 Resoluciones desde el año 2011 hasta el año 2018.

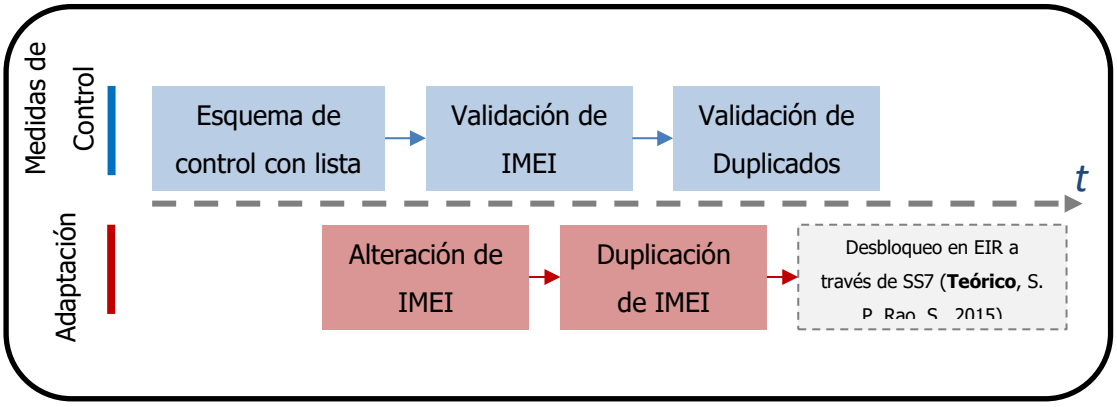
---

22 Ekblom, Paul. (2017). Technology, Opportunity, Crime and Crime Prevention: Current and Evolutionary Perspectives. 10.1007/978-3-319-27793-6_19.

23 Nokia (2016), The known unknowns of SS7 and beyond, disponible en: https://www.ernw.de/download/TSD2016_Known_Unknowns_of_SS7.pdf

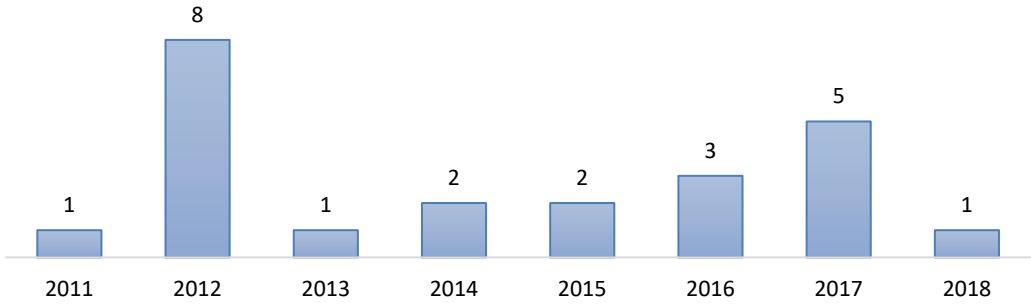
24 S. P. Rao, S. Holtmanns, I. Oliver and T. Aura, "Unblocking Stolen Mobile Devices Using SS7-MAP Vulnerabilities: Exploiting the Relationship between IMEI and IMSI for EIR Access," 2015 IEEE Trustcom/BigDataSE/ISPA.

Ilustración 2 Adaptación de la delincuencia a las medidas de control



Fuente: Elaboración propia CRC.

Gráfica 3 Número de Resoluciones Expedidas por la CRC en el marco de la estrategia contra el hurto de ETM



Fuente: Elaboración propia CRC.

3.2 Uso de metodologías de AIN

El Análisis de Impacto Normativo (en adelante AIN) es una herramienta y un proceso concebido para mejorar la toma de decisiones de política pública y regulatoria con el fin de alcanzar objetivos concretos. La OCDE define el AIN como *"una herramienta que ayuda al proceso decisorio porque sistemáticamente examina los impactos potenciales de las acciones gubernamentales, haciendo preguntas sobre costos y beneficios, sobre cuán efectiva será la acción gubernamental en alcanzar los objetivos y si hay otras alternativas viables para los gobiernos. Como un proceso decisorio, el AIN está integrado a sistemas de consulta, desarrollo de políticas y procesos regulatorios dentro del gobierno, sirviendo para comunicar y dar información ex ante sobre los efectos esperados de las propuestas gubernamentales y ex post en la medida en que ayuda a los gobiernos a evaluar las regulaciones existentes"*[25].

El objetivo principal de esta herramienta es saber si una intervención se justifica y si es proporcionada. Para ello se analiza la relación costo - beneficio de la intervención, entendiendo que toda intervención va a crear impactos: los positivos, que se entienden como beneficios, son los que permiten que una persona o grupo de valor mejore sus condiciones, trayendo con ello mejoras en el bienestar colectivo; por el contrario, los negativos, que se denominan costos, provocan que una persona o un grupo de valor obtenga peores condiciones, lo que acarrea una reducción en el bienestar de la sociedad.

De esta manera, una intervención regulatoria sólo es oportuna cuando el regulador tiene buenas razones, basadas en evidencia concreta, que demuestran que su intervención traerá beneficios para la sociedad que justifican los costos que dicha acción gubernamental puede causarle a la sociedad en su conjunto, o a un determinado grupo de valor. En Colombia esta buena práctica de producción normativa, fue promovida a través del documento CONPES[26] 3816 de 2014, el cual tuvo como objetivo sentar las bases para institucionalizar el AIN en la etapa temprana del proceso de creación de normas, como herramienta dirigida a fortalecer la confianza, efectividad y transparencia de la normatividad, en el mediano y largo plazo. Sin embargo, en la actualidad el marco jurídico sólo exige como obligatoria la

[25] OECD Reviews of Regulatory Reform. Guía Metodológica de Análisis de Impacto Normativo. 2016. Disponible en: https://www.oecd.org/gov/regulatory-policy/Colombia-2016-web.pdf
[26] Consejo Nacional de Política Económica y Social

aplicación de AIN para la expedición de Reglamentos Técnicos de acuerdo con lo dispuesto en el Decreto 1074 de 2015, modificado por el Decreto 1595 de 2015.

Pese a lo anterior, la CRC ha formalizado la aplicación de AIN dentro de sus procesos de diseño regulatorio desde el primer trimestre de 2017[27], como una buena práctica que contribuye a la estimación y cuantificación de los costos y beneficios de sus eventuales medidas, y a las alternativas que como regulador puede adoptar, junto con sus posibles efectos.

Ahora bien, como se mencionó anteriormente, las medidas y reglas implementadas por la CRC para la restricción de la operación de equipos terminales móviles reportados como hurtados o extraviados en las redes de telecomunicaciones móviles, fueron formuladas y desarrolladas desde el año 2011 como actividades conformantes de la estrategia del Gobierno Nacional contra el hurto de este tipo de bienes, por lo tanto, es claro que para la época la aplicación de metodologías de AIN no era parte del proceso de diseño regulatorio de la CRC. En esta medida, la normatividad expedida con ocasión de las líneas de acción que se plantearon desde el Gobierno Nacional surtió solo parcialmente el proceso de análisis costo – beneficio y la exploración de alternativas regulatorias que plantea el proceso de análisis AIN formalizado hoy en día en la CRC.

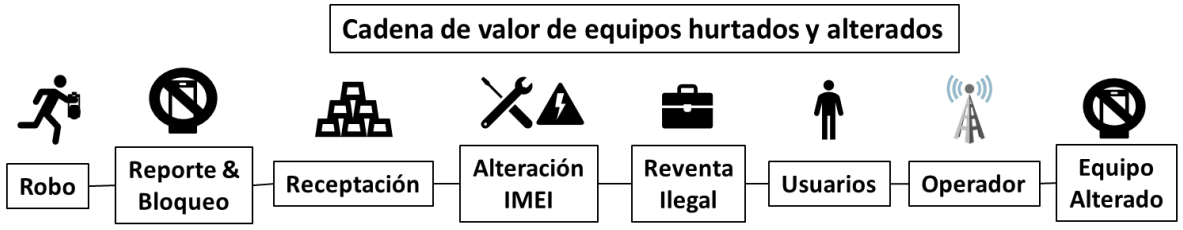
Esta situación, en efecto, pudo redundar en la eficiencia de las mencionadas medidas en el mediano y largo plazo, o en las alternativas con las que cuenta el regulador para evitar la complejidad y carga administrativa que reviste la implementación y mantenimiento en el tiempo de las obligaciones que trae consigo la regulación.

[27] En 2017 la CRC dio aplicación a metodologías de Análisis de Impacto Normativo (AIN) en el marco del proyecto de revisión al Reglamento para Redes Internas de Telecomunicaciones –RITEL- con mesas de trabajo conjuntas con la Dirección Nacional de Planeación y el Ministerio de Vivienda, Ciudad y Territorio.

3.3 Focalización de las medidas en condiciones técnicas de red y bases de datos

Consideremos ahora la forma en que la estrategia diseñada ha asignado esfuerzos en toda la cadena del hurto de terminales móviles. Para esto consideremos la cadena de hurto indicada en la Ilustración 3:

Ilustración 3 Cadena de valor de ETM hurtados y alterados



Fuente: Elaboración propia CRC

La cadena comienza con el delincuente que roba el teléfono al usuario. Dicha persona se comunica con los establecimientos dedicados a la comercialización de celulares, donde ofrece el teléfono usado a muy bajo costo, y allí vende el teléfono hurtado. Quien lo compra se encarga de restaurarlo (a través de los dispositivos de reprogramación), realiza la alteración del IMEI, restaura el equipo, borrando cualquier evidencia y de esta manera procede a comercializarlo como un celular aparentemente legal. Finalmente es vendido al usuario final, ya sea para el mercado interno o para exportación. A continuación, las diferentes etapas del ciclo del hurto:

1. **Robo y reporte al operador:** La cadena criminal tiene como punto de partida el robo del equipo al usuario, objetivo que se puede cumplir mediante las modalidades de hurto o atraco a mano armada o robo. Una vez materializado el hecho, la víctima realiza el reporte al operador móvil para el bloqueo del equipo y en la mayoría de los casos, hace el denuncio ante las autoridades competentes.

2. **Receptación y alteración del IMEI:** Sin importar la modalidad del hurto los celulares son llevados a un centro de acopio. El delincuente vende el dispositivo hurtado y el comprador se encarga de la restauración de fábrica del dispositivo, la reprogramación del IMEI y la sustitución de partes defectuosas, dejando el equipo en condiciones para su posterior comercialización.

3. **Tráfico y comercialización:** Los ETM que están listos para su comercialización en el mercado interno ilegal, son distribuidos y vendidos en diferentes zonas o municipios del país, ya sea por vía terrestre, aérea o fluvial, además existe un mercado en el exterior donde los equipos son exportados por diferentes vías y hacia distintos países de la región.

4. **Reactivación en la red móvil:** El equipo móvil que se comercializa dentro del territorio colombiano es vendido al usuario final. Este reactiva el equipo hurtado en la red móvil de un proveedor de redes y servicios, posteriormente la red detecta que el IMEI del equipo puede clasificar en una de las siguientes tipologías: inválido, sin formato, no homologado, duplicado o no registrado y procede con el bloqueo del equipo. Ahora bien, un porcentaje de equipos hurtados se exportan a países que no cuentan con las medidas de control para la detección de IMEI adulterados o donde existe una demanda de partes significativa.

Un análisis preliminar de las medidas adoptadas dentro de la estrategia del gobierno nacional para las diferentes etapas de la cadena de hurto indicaría una aparente concentración en los eslabones de reporte y reactivación, asociados a las medidas adoptadas desde el sector TIC, sin que pueda evidenciarse el mismo nivel de esfuerzo en el resto de los eslabones de la cadena.

Tabla 2 Eslabones de la cadena de hurto y medidas asociadas

Eslabón	Responsables	Medidas asociadas	Resultados
Robo	PONAL DIJIN DISEC FISCALIA	• Individualización • Acción diferencial y priorizada • Identificación de actores reincidentes	Según la información presentada en CTS de marzo de 2018, se han desarticulado 27 bandas dedicadas al hurto de celulares

Eslabón	Responsables	Medidas asociadas	Resultados
Reporte al operador	CIUDADANOS CRC MINTIC PRST	• Implementación de BD- • Reporte de Hurto • Reporte de extravíos • Bloqueo Hurtados • Condiciones para ingreso y retiro	Se han implementado todas las medidas asociadas, y se han bloqueado 13,3 millones de dispositivos bajo la tipología de *"hurto y extravió"*
Receptación y alteración del IMEI	PONAL DIJIN DISEC FISCALIA	• Incautaciones • Allanamientos a sitios de receptación • Incautaciones de equipos para manipulación de ETM • Intervención a oferta online de alteración de IMEI	Según la información presentada en CTS de marzo de 2018, se han realizado 607 capturas y 193 cierres de establecimientos
Tráfico y comercialización	POLFA DITRA DIAN MINCOMERCIO PONAL	• Controles en zonas fronterizas, puertos y aeropuertos • Controles aduaneros • Aplicación del CNP • Cierre de establecimientos	Según la información presentada en CTS de marzo de 2018, se han incautado cerca de 13.000 celulares y 600 dispositivos electrónicos.
Reactivación en la red móvil	CRC MINTIC PRST CIUDADANOS	• Detección de IMEI alterados • Registro de Terminales • Campañas de sensibilización a los usuarios. • Detección de IMEI duplicado	Se han implementado todas las medidas asociadas y se han realizado cerca de 4.5 millones de bloqueos bajo las modalidades de *"IMEI Alterado"* e *"IMEI duplicado"*

Fuente: Elaboración propia CRC

Así las cosas, se evidencia una importante concentración de los esfuerzos en los eslabones de la cadena de hurto apalancados en el control realizado por los PRST. Esta concentración puede redundar en una mayor complejidad del esquema de control a través de listas negras, sobre todo si se busca controlar toda la fenomenología desde los eslabones de reporte y reactivación en vez de fortalecer las medidas en toda la cadena de hurto.

4. CONSECUENCIAS DEL PROBLEMA

4.1 Posible reducción en la capacidad inversora de los operadores

El siguiente punto en el análisis es el de las potenciales consecuencias del problema identificado. En particular, como consecuencia del problema identificado podría presentarse una reducción en la capacidad de inversión de los operadores.

Con respecto a este punto, de acuerdo con los datos disponibles en la cuenta satélite TIC del DANE para los años 2014 a 2017, se encuentra que, el monto agregado reportado por las empresas del sector TIC para la actividad de inversión en infraestructura TIC corresponde a:

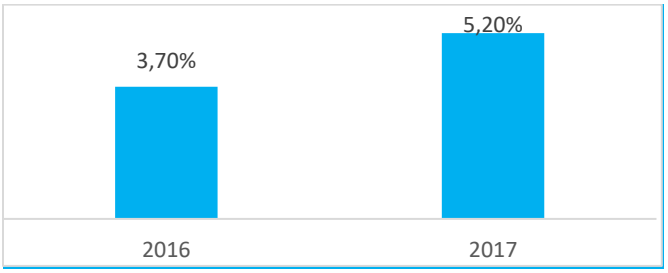
Tabla 3 Inversión en obras civiles de las actividades económicas de telecomunicaciones

2014	2015	2016	2017
$442.264.000.000	$447.761.000.000	$362.072.000.000	$370.842.000.000

Fuente: DANE - Cuenta Satélite TIC (Actualizado a diciembre de 2018)

Debe tenerse en cuenta que los valores reportados corresponden a la actividad que agrega los procesos productivos de construcción en obras de ingeniería civil TIC, como: líneas de transmisión de comunicaciones, líneas de larga distancia, líneas urbanas de transmisión de comunicaciones; entre otras. Adicionalmente el valor reportado incluye la inversión de todas las empresas del sector y no está limitada a la inversión realizada por los PRST, sin embargo, este valor tope puede usarse como referencia para evaluar el porcentaje de la capacidad de inversión en infraestructura sectorial agregada que representa la implementación de medidas de restricción de equipos terminales hurtados, para construir el porcentaje se utilizan los costos reportados por los operadores para los años 2016 y 2017.

Gráfica 4 Costos de implementación y operación de medidas para restringir la operación de ETM hurtados como porcentaje de inversión en infraestructura TIC [28]

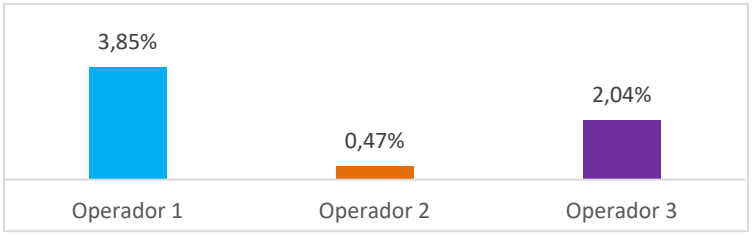


Fuente: Elaboración propia CRC con datos de cuenta Satélite TIC.

Como se evidencia en la Gráfica 4, el costo de la implementación medido como porcentaje de la inversión en infraestructura TIC se incrementó entre los años 2016 y 2017, por el efecto combinado de una reducción general en la inversión sectorial y un incremento en los costos de implementación y operación asociados a las medidas de control de ETM hurtados.

Antes de continuar con las potenciales consecuencias, se decidió verificar el potencial impacto de la implementación en la capacidad inversora de cada PRSTM. Así, se tomaron los valores reportados en la tabla 1.29 del modelo de separación contable, referente a la actividad inversora a nivel de activos y se compararon contra los costos de implementación y operación asociados a las medidas de control.

Gráfica 5 Costos de implementación y operación de medidas para restringir la operación de ETM hurtados como porcentaje de la capacidad de inversión de cada operador para el 2016[29]



Fuente: Elaboración propia CRC.

[28] Solo se tuvieron en cuenta los PRSTM, no todos los operadores reportaron los mismos años, se calculan solo 2016 y 2017, porque solo para estos dos años se tienen los costos agregados de los tres PRSTM.

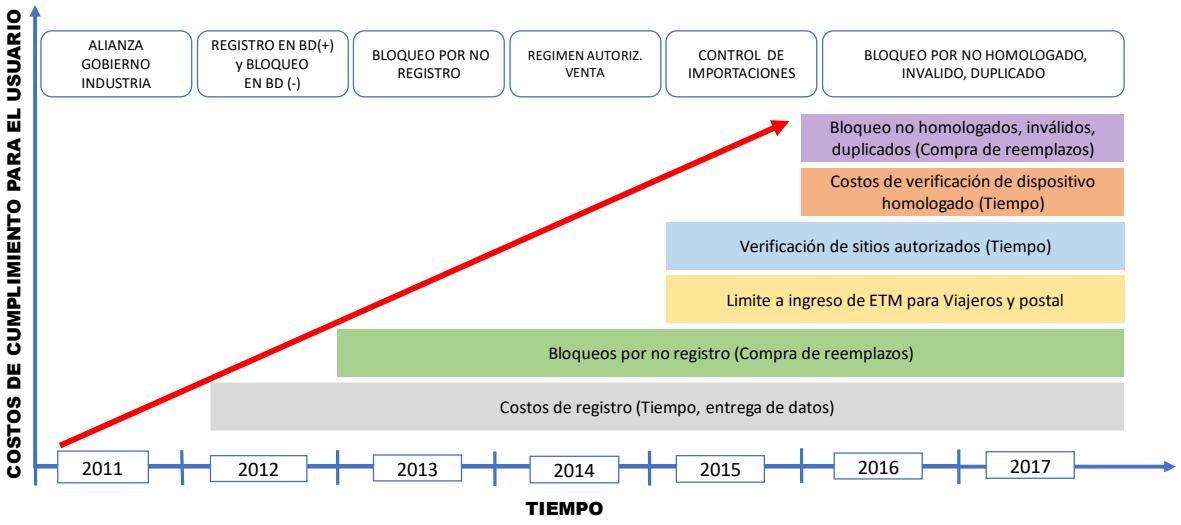
[29] Se realiza el ejercicio únicamente para el 2016. Los cambios metodológicos introducidos en el modelo de separación contable limitan la realización del ejercicio para otros años.

El resultado del análisis arroja resultados en la media de 2.2%, los cuales no distan de los impactos calculados a nivel agregado usando como referencia la cuenta satélite TIC. De cualquier forma, si bien no existe garantía alguna de que los operadores hubiesen destinado los recursos invertidos hasta ahora en otra infraestructura TIC, en un ambiente de contracción de los niveles de inversión es necesario evaluar mecanismos para incrementar la eficiencia de los controles y reducir el potencial impacto en el nivel de inversión sectorial.

4.2 Aumento gradual de los costos de cumplimiento en los ciudadanos

El siguiente aspecto en el análisis de las consecuencias identificadas es el de los costos de cumplimiento para los ciudadanos. Estos se refieren a los costos directos asociados al cumplimiento del marco regulatorio propuesto[30]. En muchos casos, el costo de cumplimiento para los ciudadanos es un costo de tiempo. Así, por ejemplo, el tiempo necesario para familiarizarse con las medidas resulta en costos de

Ilustración 4 Resumen de los costos acumulados de cumplimiento para los ciudadanos



Fuente: Elaboración propia CRC.

[30] Metodología de *Regulatory Burden Measure (RBM),* categorías de costo: https://rbm.obpr.gov.au/help.aspx?path=%2fUsing+the+Compliance+Cost+Calculator%2f2.About+cost+categories.txt

oportunidad directos para los ciudadanos. Otros costos de tiempo asociados a las medidas incluyen el tiempo requerido para realizar el registro del ETM, el tiempo requerido para verificar si un lugar se encuentra autorizado para la venta, y el tiempo requerido para verificar si un dispositivo se encuentra homologado. Sin embargo, en el caso del sistema de control para la restricción de la operación de equipos terminales móviles hurtados también deben considerarse los costos directos de reemplazo de dispositivos y tarjetas SIM, generados en los ciudadanos que adquieren de buena fe dispositivos robados que resultan bloqueados por el sistema de control.

En suma, una revisión de la eficiencia del sistema de control como la recomendada en este estudio, podría tener un impacto positivo no sólo en los costos para los PRSTM, sino también en los costos de cumplimiento para los ciudadanos.

4.3 Costos de entrada para nuevos operadores

Con respecto a los eventuales costos de entrada, algunas agencias de competencia han optado por revisar aquellos marcos regulatorios que pueden haber incrementado el costo para los agentes entrantes al mercado[31]. Aquellas agencias que han optado por este tipo de revisiones lo han hecho a través de la publicación de informes que estudian los efectos de la regulación sobre la competencia, y a la identificación de alternativas menos restrictivas.

En los sectores regulados, los procesos de concesión de licencias, las restricciones territoriales, las normas de seguridad y otros requisitos legales pueden disuadir o retrasar innecesariamente la entrada de nuevos agentes, teniendo en cuenta que las inversiones requeridas[32] para implementar el sistema de listas negras, blancas y los ciclos de validación de IMEI en la red propia y en otras redes, tendrían que ser realizadas por un operador entrante al mercado en un lapso de tiempo más corto que el lapso de tiempo de seis años que han tenido los operadores establecidos para realizar las adecuaciones. Resulta

[31] OECD (2005), Barriers to Entry, (Mejores prácticas), disponible en: www.oecd.org/daf/competition/documentation
[32] Los operadores manifestaron haber requerido adecuaciones en los sistemas de EIR, así como desarrollos de IT asociados a los sistemas de CRM, IVR, pagina web entre otros repositorios de datos.

pertinente revisar la eficiencia del sistema de control para llevar al mínimo los eventuales desincentivos de entrada en el mercado generados por la implementación del sistema de control.

5 AGENTES INTERESADOS

El problema identificado en el presente documento impacta a los siguientes grupos de actores:

Ilustración 6 Matriz de grupos de valor

Fuente: Elaboración propia CRC.

Tabla 4 Matriz de grupos de valor

Grupo de valor	Descripción	Interés en el Proyecto	Impacto en el proyecto
Presidencia de la República	La Presidencia de la República como primera Entidad del Estado, es la encargada de modelar la gestión pública orientada a la coordinación de temas de emprendimiento, productividad e innovación con la articulación de las entidades del gobierno y empresas del sector privado.	**Alto.** La Presidencia de la República diseña e implementa las políticas públicas de inclusión social y lidera la estrategia contra el hurto de ETM	**Alto.** Las medidas regulatorias identificadas pueden depender del apoyo directo de la Presidencia y la evolución del marco regulatorio puede depender de los objetivos de política publica planteados desde la Presidencia de la Republica.

Grupo de valor	Descripción	Interés en el Proyecto	Impacto en el proyecto
MinTIC	Ministerio de las Tecnologías de la Información y Comunicaciones: Institución gubernamental encargada del diseño, formulación, adopción y promoción de las políticas, planes, programas y proyectos del sector TIC	**Alto.** La CRC desarrolla la normativa regulatoria en coordinación con conjunto de políticas públicas lideradas por el ministerio	**Alto.** Las medidas regulatorias adoptadas pueden tener dependencias con la política pública sectorial liderada desde MINTIC
Proveedores de Redes y Servicios de Telecomunicaciones Móviles -PRSTM	Responsables de la operación de redes y/o de la provisión de servicios de telecomunicaciones a terceros.	**Alto.** Los PRSTM han manifestado ampliamente su interés en que la CRC realice una revisión integral de las medidas regulatorias con respecto a las restricciones de ETM. Las medidas regulatorias pueden generar ajustes o modificaciones en los procesos internos de sus empresas	**Alto.** Son parte fundamental para el desarrollo del proyecto, son los directamente responsables por la implementación de parte de la estrategia, son sobre quienes se evidencian muchos de los efectos del problema identificado, suministran información clave necesaria para el análisis y toma de decisiones.
Usuarios	Ciudadanos que contratan un servicio de telecomunicaciones	**Medio.** Los usuarios esperan procedimientos y trámites sencillos y efectivos	**Medio.** Las medidas regulatorias impactan directamente en los usuarios ya que son quienes deben de cumplir con las obligaciones establecidas en la normativa
Fabricantes, importadores y comercializadores de ETM	Persona jurídica que se dedica a la fabricación o a la comercialización de los ETM como producto final	**Medio.** Las medidas regulatorias pueden generar ajustes o modificaciones en los procesos internos de sus empresas	**Alto.** El proyecto debe analizar, considerar y contemplar los impactos que la regulación pudiera generar en las empresas fabricantes o comercializadoras de ETM algunas de las soluciones potenciales requieren de su cooperación directa.
MinComercio, Minjusticia, Mindefensa, DIAN, Fiscalía, Policía	Entidades gubernamentales encargadas del diseño, la orientación y evaluación de las políticas públicas.	**Medio.** Las medidas regulatorias son pieza fundamental para definir los mecanismos de acción en pro del cumplimiento de lo establecido en la normatividad y alcanzar los objetivos de política publica diseñada por estas entidades	**Medio.** Las recomendaciones, sugerencias y el juicio de expertos son de suma importancia para lograr alcanzar el cumplimiento de los objetivos establecidos
Administrador de base de datos	Proveedor de servicios de consultoría tecnológica y soluciones en materia de tecnología informática, tanto al sector público como al sector privado.	**Alto.** Las medidas regulatorias establecidas pudiesen generar modificaciones en la gestión integral del uso de las bases de datos	**Medio.** La Información sobre la gestión de la base de datos es insumo para la identificación de las medidas regulatorias

Grupo de valor	Descripción	Interés en el Proyecto	Impacto en el proyecto
GSMA	Organización de operadores móviles y compañías relacionadas, dedicada al apoyo de la normalización, la implementación y promoción del sistema de telefonía móvil GSM	**Medio.** La organización puede participar asesorando en la implementación de estándares técnicos definidos por GSMA y manteniendo la base de datos internacional	**Medio.** Las especificaciones, estándares y recomendaciones técnicas son base para la formulación de procedimientos dentro del proyecto, el componente de cooperación internacional depende del adecuado mantenimiento de la base de datos de IMEI de la GSMA.
Otros reguladores, REGULATEL, organismos internacionales CITEL, CAN	Entidades reguladoras y organismos internacionales que trabajan en políticas públicas y regulatorias de telecomunicaciones	**Medio.** Las entidades reguladoras de otros países pueden consultar y comparar la normatividad expedida en Colombia y servir de referente en el desarrollo del marco regulatorio local.	**Bajo.** Si bien son un referente importante, la implementación del proyecto no depende directamente de las decisiones de estos organismos. Sin embargo algunas organizaciones internacionales como la CAN pueden adoptar decisiones de carácter vinculante.
Gremios	ACIEM, Asomedios, Asomóvil, ANDI, Cámaras de Comercio, CCIT.	**Alto.** Demuestran alto interés en el proyecto en el aporte de recomendaciones o sugerencias durante el proyecto	**Medio.** Se involucran activamente en la participación y socialización de información con otros proveedores de red y grupos de valor
Sociedad civil	ONG y organizaciones privadas que trabajan para el adecuado desarrollo y cumplimiento de políticas públicas y regulatorias para los ciudadanos	**Medio.** Pueden tener interés enfocado en pro del beneficio del ciudadano realizando aportes, recomendaciones o sugerencias durante el proyecto	**Alto.** Pueden aportar información y recomendaciones en busca de maximizar el bienestar de los ciudadanos
Academia	Expertos y académicos interesados en el desarrollo de políticas públicas y regulatorias en el sector de las telecomunicaciones	**Bajo.** Aporte de conocimiento técnico de juicio de expertos durante el desarrollo del proyecto	**Medio.** Aportan fuentes de información confiables y opinión experta.

Fuente: Elaboración propia CRC.

Anexos

A.1 Resoluciones de carácter general expedidas por la CRC en el marco de la estrategia de Hurto.

NÚMERO	ACÁPITE	FECHA
3128 DE 2011	Por la cual se define el modelo técnico, los aspectos operativos y las reglas para la implementación, cargue y actualización de las bases de datos positiva y negativa para la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados y se modifican los artículos 10 y 93 de la Resolución CRC 3066 de 2011	7 de septiembre de 2011
3530 DE 2012	Por la cual se establecen las reglas asociadas a la autorización para la venta de equipos terminales móviles en el país, se modifican el artículo 4 y 10 de la Resolución CRC 3066 de 2011, así como los artículos 4, 6 y 14 de la Resolución CRC 3128 de 2011	10 de febrero de 2012
3584 DE 2012	Por la cual se adicionan los artículos 18a y 18b a la Resolución CRC 3128 de 2011, se modifica el artículo 2° de la Resolución CRC 1596 de 2006, y se dictan otras disposiciones.	12 de abril de 2012
3667 DE 2012	Por la cual se modifican en lo pertinente los artículos 3°, 4°, 6°, 7°, 12°, 13°, 14° y 17° de la Resolución CRC 3128 de 2011, se modifica el parágrafo del artículo 1° de la Resolución CRC 3066 de 2011 y se dictan otras disposiciones	24 de mayo de 2012
3854 DE 2012	Por la cual se modifica el artículo 18 de la Resolución CRC 3128 de 2011, en relación con el plazo para el inicio de detección y control de cambio SIM en el Equipo Terminal Móvil	31 de julio de 2012
3912 DE 2012	Por la cual se modifican los numerales 3.7, 3.8, 3.10 y 3.12 y se adiciona el numeral 3.28 al artículo 3° de la Resolución CRC 3128 de 2011, un parágrafo al artículo 17 de la Resolución CRC 3129 de 2011 y un parágrafo al artículo 64 de la Resolución CRC 3066 de 2011	11 de septiembre de 2012
3947 DE 2012	Por la cual se modifican algunas reglas asociadas al proceso de registro de equipos terminales móviles, se modifican los numerales 18.4 y 18.6 de la Resolución CRC 3530 de 2012, se adiciona un parágrafo al artículo 64 de la Resolución CRC 3066 de 2011 y se dictan otras disposiciones	1 de octubre de 2012
3985 DE 2012	Por la cual se modifica la Resolución CRC 3038 de 2011	23 de octubre de 2012
4017 DE 2012	Por la cual se modifican los numerales 3,20 y 3,21 de la Resolución CRC 3128 de 2011	10 de diciembre de 2012
4119 DE 2013	Por la cual se modifica en lo pertinente los artículos 3, 4, 7, 7a , 10 y 11 de la Resolución CRC 3128 de 2011	14 de marzo de 2013
4584 DE 2014	Por la cual se establece el Régimen de Autorizaciones para la Venta con fines comerciales de Equipos Terminales Móviles en Colombia	26 de agosto de 2014
4407 DE 2014	Por la cual se modifica en lo pertinente los artículos 3, 4, 7 y 17 de la Resolución CRC 3128 de 2011 y se dictan otras disposiciones	31 de enero de 2014
4813 DE 2015	Por la cual se establecen medidas de identificación de equipos terminales móviles dentro de la estrategia nacional contra el hurto de equipos terminales móviles, se modifica la Resolución CRC 3128 de 2011 y se dictan otras disposiciones	26 de octubre de 2015
4807 DE 2015	Por la cual se modifica la Resolución CRT 087 de 1997, la Resolución CRT 2028, la Resolución CRC 3067 de 2011, la Resolución CRC 3128 de 2011 y la Resolución CRC 3496 de 2011	6 de octubre de 2015
4868 DE 2016	Por la cual se adicionan condiciones para la identificación y depuración de IMEI en la Resolución CRC 3128 de 2011 y se modifica el artículo 13.1.2 del Capítulo I del Título XIII de la Resolución CRT 087 de 1997	1 de febrero de 2016
4948 DE 2016	Por la cual se suspenden los efectos de los numerales 3.7, 3.8 y 3.10 del artículo 3 de la Resolución CRC 3128 de 2011 y del parágrafo 4 del artículo 64 de la Resolución CRC 3066 de 2011	20 de mayo de 2016

NÚMERO	ACÁPITE	FECHA
5038 DE 2016	Por la cual se modifica el ciclo interred de la etapa de verificación de equipos terminales móviles y se suspenden los efectos de los numerales 10a.2, 10a.3 y 10a.5 del artículo 10a, el numeral 10b.2 del artículo 10b y el literal d) del artículo 10d la Resolución CRC 3128 de 2011	28 de octubre de 2016
5084 DE 2017	Por la cual se modifica el numeral 2.7.3.12.3.2 del artículo 2.7.3.12 del Capítulo 7 del Título II de la Resolución CRC 5050 de 2016	12 de enero de 2017
5132 DE 2017	Por la cual se modifica el numeral 2.7.3.12.3.2. del Artículo 2.7.3.12. del Capítulo 7 del Título II de la Resolución CRC 5050 de 2016	25 de abril de 2017
5164 DE 2017	Por la cual se modifica el artículo 2.7.3.8 del Capítulo 7 del Título II de la Resolución CRC 5050 de 2016	28 de junio de 2017
5178 DE 2017	Por la cual se modifican los numerales 2.7.3.11.3.7 y 2.7.3.12.4.1 del Capítulo 7 del Título II y el Anexo 2.6 del Título de Anexos de la Resolución CRC 5050 de 2016	31 de julio de 2017
5292 DE 2017	Por la cual se modifican el numeral 2.7.2.1.25 del artículo 2.7.2.1, el parágrafo 2 del artículo 2.7.3.2, el parágrafo 1 del artículo 2.7.3.3 y los numerales 2.7.3.12.2 y 2.7.3.12.3 del artículo 2.7.3.12 del Capítulo 7 del Título II de la Resolución CRC 5050 de 2016, y se hace una Fe de Erratas a la Resolución CRC 5050 de 2016	29 de diciembre de 2017
5427 DE 2018	Por la cual se deroga el numeral 2.7.2.2.17 del artículo 2.7.2.2 y se modifica el artículo 2.7.3.5 del Capítulo 7 del Título II de la Resolución CRC 5050 de 2016	15 de agosto de 2018

Fuente: Elaboración propia CRC

A.2 Normas contra el hurto de equipos terminales expedidas por otras entidades del estado.

NÚMERO	ACÁPITE
DECRETO 1630 DE 2011	Por medio del cual se adoptan medidas para restringir la operación de los equipos terminales hurtados que son utilizados para la prestación de servicio de telecomunicaciones móviles
LEY 1453, ART. 105 Y 106	Por medio de la cual se modifica 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
DECRETO 2365 DE 2012	Por el cual se adoptan medidas de control para las exportaciones de equipos terminales móviles
DECISION 786 DE LA CAN	Intercambio de información de equipos terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina
DECRETO 2025 DE 2015	Por el cual se establecen medidas para controlar la importación y exportación de teléfonos móviles inteligentes, teléfonos móviles celulares, y sus partes, clasificables en las subpartidas 8517.12.00.00 Y 8517.70.00.00 del Arancel de Aduanas, se adiciona el Decreto 2685 de 1999 y se deroga el Decreto 2365 de 2012
DECRETO 2142 DE 2016	Por el cual se modifica y adiciona el Decreto 2025 de 2015 y se modifica el artículo 121 del Decreto 2685 de 1999

Fuente: Elaboración propia CRC