PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

DISERTACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE MAGISTER EN TECONOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN CON MENCIÓN EN REDES DE COMUNICACIONES

“Estudio técnico y normativo en el ámbito de las telecomunicaciones respecto a la evolución de la cantidad de equipos móviles reportados como robados, perdidos o hurtados en el Ecuador durante los años 2014 a 2018”

Autor: Luis Vinueza

Quito – Ecuador

2021

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Luis Alfredo Vinueza Vinueza, bajo mi supervisión.

Ing. Juan Francisco Chafla Altamirano, MSc.
DIRECTOR DEL PROYECTO

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El presente proyecto de titulación efectúa un estudio desde el ámbito regulatorio y técnico del problema que ocurre en el país debido al robo, hurto y pérdida de los equipos móviles, realizando un análisis a la normativa vigente que ha sido generada en el país y a nivel internacional y las posibles propuestas que contribuirían a combatir esta situación.

En primera instancia se ejecuta una revisión de la regulación emitida en Ecuador en lo que respecta a telecomunicaciones tanto a nivel de leyes, reglamentos y normas y el efecto que han producido en el combate de este ilícito, considerando las cifras de robos entre los años 2014 y 2018. Esta actividad se complementa con el estudio de las disposiciones constantes en el Código Orgánico Integral Penal, dado que es fundamental evaluar las acciones tomadas por las instituciones del estado para contrarrestar este suceso.

Es imprescindible también analizar la experiencia y las normas generadas en otros países, con el objetivo de adoptar las mejores prácticas en función de la realidad del Ecuador, por ello se han revisado los instrumentos normativos expedidos por los países vecinos, su relación y similitud con aquellos aplicados localmente.

Por otro lado, se ha examinado el alcance y el fondo de las recomendaciones y resoluciones emitidas internacionalmente por organismos reconocidos a nivel mundial y continental, a fin de verificar si son aplicables en Ecuador y más que todo determinar la forma en que se está llevando su incidencia en otras latitudes.

Además, se ha identificado las herramientas y aplicaciones desarrolladas por los principales fabricantes y proveedores de equipos para controlar y bloquear el dispositivo, acción que puede ser efectuada por los mismos usuarios, como una alternativa tecnológica.

Con toda esta investigación se ha elaborado una propuesta que apoye al combate del robo de equipos celulares y contribuya a desincentivar este ilícito, considerando las diferentes aristas y las entidades que se encuentran inmersas en la supervisión y vigilancia nacional.

INTRODUCCIÓN

Los equipos celulares se han convertido en objetos muy relevantes para la población ecuatoriana por varias circunstancias, a más de facilitar la comunicación entre las personas, permiten que los usuarios accedan a Internet y por tanto a una serie de aplicaciones y servicios que ayudan a satisfacer sus necesidades en forma rápida y sencilla. A más de lo indicado, en Ecuador y los países de Sudamérica, este bien tiene un costo elevado, debido a que localmente no se fabrican este tipo de equipos, como si sucede en los países desarrollados y por otro lado por los aranceles que se imponen para su importación.

La penetración de la telefonía móvil o servicio móvil avanzado en el país supera el 90% de la población, lo que implica que casi todos los ecuatorianos utilizan este equipo y lo llevan consigo mientras realizan sus gestiones diarias.

Estos hechos han provocado que este equipo sea demasiado atractivo para los malhechores y las bandas delincuenciales, las cuales han desarrollado estrategias para robar y posteriormente comercializar estos terminales, reintroduciéndolos al mercado.

En el país la sustracción de equipos celulares se ha convertido en un problema que debe ser estudiado y considerado por el estado ecuatoriano, con el objetivo de buscar soluciones y acciones que ayuden a combatirlo. Las cifras actuales revelan que este hecho se ha mantenido con una incidencia alta durante los últimos cinco años y se prevé un incremento en los próximos años sino se toman medidas oportunas y se realizan nuevas actividades de control.

Es preciso indicar que este ilícito afecta notoriamente a toda la población y provoca incluso daños físicos en la ciudadanía.

En el presente documento se realiza un estudio desde el ámbito de las telecomunicaciones respecto a las acciones que se han tomado a nivel nacional para contrarrestar este ilícito y se plantean posibles actividades que contribuyan a su disminución.

De acuerdo a las cifras publicadas por la institución de regulación y control de las telecomunicaciones la cantidad de terminales móviles reportados por robo, hurto y pérdida bordea la cifra de 622.521 equipos en los años 2017 y 2018. Este ilícito afecta notoriamente a la población.

Por tanto, se hace necesario realizar un estudio sobre la evolución de este problema en los últimos años y las normas que se han aplicado. Es importante también analizar la experiencia y las normas generadas en otros países, a fin de adoptar las mejores prácticas, considerando la realidad del Ecuador. Es fundamental, evaluar las acciones tomadas por las instituciones del estado con miras a generar nuevas formas de control que permitan adoptar medidas para combatir este suceso. Con todo este análisis se podrá generar alternativas regulatorias y técnicas que apoyen el combate al robo de equipos celulares desde el ámbito de las telecomunicaciones y plantear propuestas que contribuyan a desincentivar este ilícito.

Para el presente proyecto se utilizarán fuentes secundarias, los datos que se analizarán se tomarán de una institución del estado denominada la Agencia de Regulación y Control de las Telecomunicaciones, que es la autoridad de telecomunicaciones del país. Por otro lado, la normativa a estudiar será tomada de Internet, de los portales web de las instituciones gubernamentales de Ecuador y de los países de Sudamérica que hayan emitido regulación al respecto, especialmente de los que colindan con el Ecuador.

En el primer capítulo se revisará en forma detallada la normativa en telecomunicaciones para realizar el control de los equipos móviles robados, perdidos o hurtados que ha sido emitida en el país, relacionándola con los equipos móviles que han sido reportados entre el año 2014 y el 2018.

El segundo capítulo tendrá como objetivo principal comparar la regulación que ha sido expedida en los países colindantes con Ecuador, así como aquella destacada en otros países y sus semejanzas o diferencias.

La problemática social inherente a este fenómeno será abordada en el tercer capítulo, en donde adicionalmente se revisará el papel de los fabricantes de dispositivos para apoyar el combate de este problema.

Finalmente, en función de todos los análisis realizados, se delineará una propuesta que apoye y trate de enfrentar este inconveniente social, desde el ámbito de las telecomunicaciones.

JUSTIFICACIÓN

De acuerdo a las cifras publicadas por la Agencia de Regulación y Control de las Telecomunicaciones la cantidad de equipos reportados por robo, hurto y pérdida bordea la cifra de 622.521 terminales en los años 2017 y 2018 (ARCOTEL, 2019), lo que equivale a un promedio de 853 equipos sustraídos diariamente en el Ecuador y a una cantidad aproximada de $ 62’252.100 USD que ha sido sustraída a la ciudadanía en los dos últimos años (si se estima un valor de 100 USD por cada equipo), cifras realmente alarmantes y preocupantes para el país. Este ilícito afecta notoriamente a la población y provoca a más de la sustracción del equipo, agresiones físicas, intimidación y en algunos casos el deceso de personas.

Por tanto, se hace necesario realizar un estudio sobre la evolución de este problema en los últimos años y efectuar una revisión de las medidas y disposiciones que se han generado en el Ecuador en el ámbito técnico y regulatorio de las telecomunicaciones. Es importante también analizar la experiencia y las normas generadas en otros países, a fin de adoptar las mejores prácticas, considerando la realidad del Ecuador. Es fundamental, evaluar las acciones tomadas por las instituciones del estado con miras a generar nuevas formas de control que permitan adoptar medidas para combatir este suceso. Con todo este análisis se podrá generar alternativas regulatorias y técnicas que apoyen el combate al robo de equipos celulares desde el ámbito de las telecomunicaciones y plantear propuestas que contribuyan a desincentivar este ilícito.

La vida de las personas es algo que no tiene valor y cualquier acción que se realice para proteger y preservarla, es de trascendental relevancia para el bienestar de la ciudadanía en general.

ANTECEDENTES

El problema del robo de equipos móviles afecta prácticamente a toda Sudamérica, principalmente debido a que este tipo de dispositivos tienen un tamaño reducido, están ampliamente masificados en la población y su costo especialmente para los smartphones es alto.

Cuando la telefonía celular inició y dio sus primeros pasos en el país, la penetración de equipos móviles fue baja y su utilización no fue alta, debido a que se trataba de una tecnología poco conocida y no se sabía si iba a tener una acogida considerable. Esto ocurrió durante la época de los noventas e inicios de la década siguiente, no obstante con el surgimiento de la tecnología GSM y las ventajas que implica su uso, tales como la movilidad y el uso de sim card o chip inteligente que permite mantener los datos principales del usuario y poderlos cambiar a otro equipo, la penetración del servicio móvil avanzado en el país fue creciendo de manera acelerada, de forma que de acuerdo a las cifras que mantiene la Agencia de Regulación y Control de las Telecomunicaciones, la densidad nacional de líneas activas del servicio móvil avanzado es del 91,47%, a noviembre de 2019.

Todos estos factores han contribuido a que la cantidad de equipo móviles robados, perdidos o hurtados en el país presente una cifra alta. Cabe señalar que el problema del robo de equipos móviles afecta prácticamente a toda Sudamérica, en donde se observa cifras elevadas en varios países de la región. De acuerdo con un estudio realizado por Telecommunications Management Group, Inc[1] en el año 2018, en Colombia durante el año 2017 se hurtaron más de 1.3 millones de equipos, en Perú la cantidad diaria de equipos robados superó la cifra de 6.000 diarios en el año 2016, en tanto que en Argentina dicha cantidad fue superior a 4.700 en forma diaria.

En el Ecuador conforme cifras proporcionadas por la ARCOTEL[2], este problema no está muy distante respecto a los otros países:

---

[1] Telecommunications Management Group. (2018). *Device Theft in Latin America*. Arlington, Estados Unidos, Recuperado de https://www.tmgtelecom.com/publications/latam_device_theft/.

[2] Agencia de Regulación y Control de las Telecomunicaciones

Tabla 1. Equipos reportados como robados/perdidos/hurtados en Ecuador por año (ARCOTEL, 2019)

Año	Cantidad de terminales reportados como robados/perdidos/hurtados
2015	542.484
2016	354.034
2017	304.376
2018	318.145
2019	212.258 (jun-19)

Estas cifras han provocado que las autoridades nacionales de regulación de los países expidan normativa que apoye el control de este fenómeno desde el ámbito de las telecomunicaciones. Las listas negativas contienen todos los equipos móviles que han sido reportados como robados, perdidos o hurtados y que por tanto se encuentran impedidos o bloqueados para operar a nivel nacional. Las listas positivas contienen todos los equipos móviles que se encuentra aptos para ser utilizados en el país y pueden ser activados puesto que han cumplido con la reglamentación emitida por la autoridad.

En el Ecuador la normativa ha sido expedida por el ex-Consejo Nacional de Telecomunicaciones desde el año 2009 a través de varias resoluciones, las cuales se citan a continuación:

- Resolución 006-01-CONATEL-2009 de 15 de enero de 2009
- Resolución 191-07-CONATEL-2009 de 25 de mayo de 2009.
- Resolución TEL-214-05-CONATEL-2011 de 24 de marzo de 2011.
- Resolución TEL-535-18-CONATEL-2012 de 9 de agosto de 2012.
- Resolución TEL-752-25-CONATEL-2012 de 25 de agosto de 2012.
- Resolución TEL-878-30-CONATEL-2012 de 18 de diciembre de 2012.

La primera resolución corresponde a un procedimiento para el registro de equipos por robo, hurto y pérdida, en tanto que las resoluciones siguientes conciernen a una norma con más articulado y disposiciones adicionales.

Acorde a lo establecido en la citada norma, la ARCOTEL es la institución que tiene la función de implementar y manejar la base de datos de equipos reportados como robados, perdidos y hurtados a nivel nacional.

Posteriormente a la legislación mencionada, en cierta parte de la Ley Orgánica de Telecomunicaciones y su Reglamento General, se hace referencia en forma muy breve y específica a equipos robados.

OBJETIVOS

OBJETIVO GENERAL

Como objetivo general de este trabajo de titulación se ha planteado realizar un estudio técnico y normativo en el ámbito de las telecomunicaciones respecto al robo de equipos celulares, para generar propuestas o alternativas que ayuden a combatir este problema.

OBJETIVOS ESPECÍFICOS

- Analizar la normativa y los cambios regulatorios efectuados en Ecuador con los períodos en los cuales se ha detectado la mayor cantidad de equipos del servicio móvil avanzado reportados como robados, perdidos o hurtados.
- Estudiar la regulación en el ámbito de las telecomunicaciones de los países sudamericanos colindantes y evaluar las coincidencias y diferencias de dichas regulaciones con la que ha sido emitida en el Ecuador.
- Analizar alternativas regulatorias y técnicas en telecomunicaciones que apoyen el control del robo, pérdida o hurto de equipos celulares.
- Desarrollar una propuesta que contribuya a contrarrestar el robo de equipos celulares.

CAPÍTULO I

1. NORMATIVA ECUATORIANA RESPECTO AL ROBO, HURTO Y PÉRDIDA DE EQUIPOS MÓVILES Y SU RELACIÓN CON LA CANTIDAD DE EQUIPOS ROBADOS, PERDIDOS Y HURTADOS EN EL PAÍS

1.1. NORMATIVA EXPEDIDA EN EL ECUADOR

Hace más de una década que el ex–Consejo Nacional de Telecomunicaciones CONATEL emitió su primera resolución que contiene normativa respecto al robo, hurto y pérdida de equipos móviles. El 15 de enero de 2009 dicha entidad expidió la Resolución No. 006-01-CONATEL-2009 que contiene un procedimiento inicial para el registro de equipos robados y normativa para el empadronamiento de abonados, consignando en un solo instrumento dos aspectos esenciales para el control de la telefonía móvil. En este año se da comienzo a la regulación generada por una autoridad nacional de telecomunicaciones para dar apoyo al combate del robo de equipos móviles, esta iniciativa surge en conjunto con el empadronamiento de abonados, debido a que en aquella época no se mantenía como obligación el registro de los nombres de los abonados que han activado líneas telefónicas del servicio móvil avanzado en el país, situación que no permitía conocer a ciencia cierta la identidad de las personas que utilizaban el servicio especialmente en la modalidad prepago, por lo que si se realizaban comunicaciones con fines sospechosos o fraudulentos se tornaba muy difícil obtener los datos de identificación de estas personas.

En la resolución citada se establecen las siguientes obligaciones para los prestadores del SMA, respecto al robo, hurto y pérdida de equipos móviles.

> **"*ARTÍCULO CINCO***. *Las operadoras del Servicio Móvil Avanzado (SMA), implementarán dentro del término de quince (15) días, contados a partir de la fecha de notificación de esta resolución, un sistema para recepción y registro de reporte de los abonados, por robo o pérdida de equipos terminales de telefonía móvil, que permita al operador suspender de forma inmediata el servicio y a su vez bloquear el terminal y el chip reportado. Este procedimiento deberá realizarse sin perjuicio de que el usuario presente la correspondiente denuncia ante las*

autoridades competentes (Policía o Fiscalía, según corresponda), para los efectos de carácter judicial que podrían derivarse. La información específica respecto de un terminal reportado a las operadoras como perdido, robado o hurtado, podrá ser requerida por la Policía Nacional o autoridad competente, previo el cumplimiento de los requisitos y procedimientos de ley.

Se prohíbe expresamente a las operadoras del Servicio Móvil Avanzado (SMA), la activación de equipos terminales y/o sim cards que consten en la base de datos anteriormente mencionada.

En todos los casos, cuando la operadora reciba un reporte de pérdida, robo o hurto de equipos terminales de telefonía móvil, notificará al usuario o abonado, de su obligación de presentar la denuncia ante las autoridades correspondientes, para los efectos de carácter judicial que podrían derivarse del uso delictivo del terminal y/o sim card reportado.

***ARTÍCULO SEIS**. Las operadoras del Servicio Móvil Avanzado (SMA), mantendrán actualizadas diariamente las listas de teléfonos reportados como perdidos, robados o hurtados. Esta base de datos será intercambiada entre éstas (…).*" (CONATEL, 2009, p.5)

En esta primera resolución el ex-CONATEL define un procedimiento que el usuario debe seguir al momento que desee reportar un equipo como robado, hurtado o perdido, así como que las operadoras del SMA deben implementar un sistema que reciba estos reportes y proceda a bloquear el equipo en su red. Sobre este procedimiento es necesario puntualizar lo siguiente:

a) No se establece una obligación a las operadoras respecto a la captura automática del IMEI del equipo. Este aspecto es fundamental puesto que los abonados no conocen el IMEI del equipo, a menos que lo puedan observar en la caja del equipo o en la factura correspondiente, sin embargo, en muchos casos estos elementos fueron perdidos por el usuario, lo que dificulta determinar la identificación del equipo.
b) Si bien se define que el equipo debe ser bloqueado en forma inmediata, no se establece el tiempo de bloqueo exacto que disponen las operadoras para efectivizar esta acción.

c) En el artículo seis se menciona que las operadoras deben mantener actualizadas sus bases de equipos reportados como robados, perdidos o hurtados y deben intercambiar esta información. No obstante, no se señala la periodicidad de este intercambio ni la forma o el medio a través del cual debe realizarse.

Es importante destacar que en esta primera resolución se logra dar un paso sustancial para evitar que se usen equipos robados y principalmente que el usuario disponga de un mecanismo a través del cual pueda realizar sus reportes de bloqueo de equipo y de chip.

Por otro lado, existe otro hecho que enfatizar, esto es que se instituye como obligación de las operadoras notificar al usuario que debe presentar la denuncia ante las autoridades correspondientes, para los fines judiciales pertinentes.

Durante ese mismo año, el 25 de mayo de 2009, el ex-CONATEL expide la Resolución No. 191-07-CONATEL-2009, mediante la cual se emite una normativa que abarca el procedimiento para el empadronamiento de abonados y el registro de los dispositivos robados, es decir, del procedimiento que se generó unos meses atrás, con esta nueva resolución se define ya una norma que lo regula en todo su contexto.

La norma se divide en dos grandes secciones, la primera contiene disposiciones relativas al empadronamiento en el servicio móvil avanzado y la segunda se refiere al registro de terminales perdidos, robados o hurtados. Adicionalmente incluye dos disposiciones transitorias, dos disposiciones generales y una disposición final que deroga la Resolución No. 006-01-CONATEL-2009.

En la Norma se destaca la inclusión de los siguientes artículos para el registro de teléfonos robados, perdidos o hurtados que no estaban contemplados en la anterior resolución.

> ***"ARTÍCULO NUEVE. Comparación de información.*** *Previo al registro de terminales perdidos, robados o hurtados, el concesionario deberá comparar la información que tiene de dicho terminal en su base de datos, con la información que proporcione el abonado al momento del reporte.*
>
> *Una vez realizado el registro de los terminales reportados como robados, perdidos o hurtados por parte del concesionario, este emitirá, a pedido del interesado, una comunicación específica para uso o constancia del abonado que realizó el reporte,*

en la que indique claramente la información del terminal reportado y la fecha y hora de registro, así como la causa (robo, hurto o pérdida) del reporte realizado. Es obligación del abonado presentar la correspondiente denuncia o acción en el ámbito pertinente.

ARTÍCULO DIEZ. Base de datos de terminales reportados como robados, perdidos o hurtados. *Es obligación de los concesionarios del SMA mantener vigente una base de datos con la información de los equipos terminales de telefonía móvil reportados.*

(…)

La actualización en línea, permitirá ingresar los siguientes datos:

a) Fecha de reporte del Abonado

b) IMEI o número serial de equipo

c) Tipo de transacción (robo, hurto, pérdida o liberado por el Abonado)

Los concesionarios del SMA, no activarán los equipos terminales o sim cards que consten en las bases de datos anteriormente mencionadas, excepto en los casos en que estos ya se encuentren liberados por los respectivos Abonados, mediante comunicación escrita o el mecanismo que para el efecto implemente el Concesionario." (CONATEL, 2009, p.4-5)

En los artículos citados, la Norma establece nuevas obligaciones para las operadoras del SMA, tales como:

a) Las operadoras del SMA deben contrastar la información que tienen en sus registros internos con la que entregue el cliente/usuario durante el reporte. Esta contrastación permite que la operadora valide la información del equipo que el usuario va a reportar.
b) A pedido del interesado, la operadora debe entregar una constancia del reporte de robo realizado por el usuario, situación que constituye un respaldo para al abonado que realiza el reporte.
c) Define que los datos que reposan en la base de datos de equipos reportados como robados, perdidos o hurtados es confidencial y puede ser requerida únicamente por autoridad competente.

d) La ex-Superintendencia de Telecomunicaciones tendrá la facultad de realizar los controles e inspecciones que considere pertinentes a la base de datos que poseen las operadoras.
e) A pesar de que no se define un procedimiento específico, por primera vez se hace referencia a un concepto importante requerido por los usuarios en los casos que encuentren su equipo o lo recuperen luego de un robo. Este aspecto constituye la liberación del terminal.

Los aspectos señalados se convierten en avances importantes con relación a la resolución emitida a inicios del año 2009.

El 24 de marzo de 2011, aproximadamente dos años después de haber sido emitida la Resolución No. 191-07-CONATEL-2009, el ex-CONATEL resolvió modificar el referido cuerpo normativo en varios aspectos, para lo cual emitió la Resolución No. 214-05-CONATEL-2011 que contiene 10 artículos, 6 disposiciones transitorias y un glosario de términos. Dicha resolución realiza una modificación en más del cincuenta por ciento del articulado de la norma, destacándose los siguientes cambios en lo que respecta al registro de equipos reportados como robados, perdidos o hurtados:

- Se incluye como obligación de los prestadores del servicio móvil avanzado el bloqueo de equipos móviles que hayan sido reportados en otros países, con lo cual se garantiza que se puedan bloquear en un país vecino los equipos que han sido reportados en otro y contrarresta en cierta forma la distribución de equipos fuera de las fronteras locales. En otras palabras, lo que se busca es controlar el tráfico ilícito de terminales robados entre países y evitar que un terminal robado pueda ser comercializado libremente en otro país vecino, afectando a usuarios que adquirieron el equipo en forma legal.

  En este sentido, actualmente se mantiene un convenio interinstitucional para el intercambio de equipos sustraídos, hurtados, perdidos y recuperados con la República del Perú, en tanto que con Colombia el intercambio se lo realiza a través de la conexión a una plataforma internacional. De esta manera se trata de impedir el comercio de este tipo de dispositivos entre naciones limítrofes.

  El Ministerio de las Telecomunicaciones y de la Sociedad de la Información (MINTEL), institución que tiene la representación del país en temas

internacionales, es el encargado de suscribir acuerdos o convenios binacionales que faculten el bloqueo de equipos robados entre países de la región.

- Se especifica que el abonado que fue víctima de un robo debe reportar dicho evento en la operadora en la cual estaba registrado el teléfono, es decir, no puede reportar en otra operadora, sino únicamente en la cual contaba con el servicio previo al robo del terminal. Con este aspecto, se aclara al usuario que su reporte no puede ser efectuado indistintamente en cualquier operadora, sino solo en aquella en la tenía el servicio, situación que es conveniente puesto que dicha operadora es la única que tiene la información en su red sobre el equipo que utilizaba el usuario.
- Se agrega como condición que exclusivamente los abonados que reportaron el robo, hurto o pérdida de sus equipos son los que pueden solicitar la liberación del mismo. Aspecto que es fundamental para efectuar un debido control de estos eventos, dado que solo los usuarios que reportaron el suceso, pueden requerir su liberación. De esta manera se evita que usuarios o personas que adquirieron el equipo en forma ilícita liberen el equipo, sin ningún tipo de verificación previa.
- Se recalca que la información correspondiente a los terminales reportados como robados, perdidos o hurtados debe ser intercambiada entre las operadoras y la ex-SUPERTEL y los formatos, esquemas y procedimientos serán establecidos por la ex-Superintendencia de Telecomunicaciones. Esta situación constituye un gran avance puesto que se dispone que una institución del estado determine el procedimiento a seguir para transmitir y recibir este tipo de información, con lo que se logra utilizar un proceso uniforme que debe ser cumplido por las tres operadoras, evitando que se produzcan acciones desiguales entre ellas o condiciones que no sean acatadas en forma idéntica entre todas las operadoras.
- Se define claramente que las operadoras del servicio móvil avanzado deben realizar en forma obligatoria la captura automática del IMEI del equipo, acción que favorece tremendamente al usuario, ya que en la mayoría de casos desconoce el IMEI del equipo, ya sea por complejidad (15 dígitos numéricos) o por falta de interés en anotarlo y tenerlo presente ante cualquier eventualidad.

- Por primera vez en todo el historial de la norma se define el concepto de lista blanca y adicionalmente se establece un plazo para que la ex-SENATEL, operadoras del SMA y la ex-SUPERTEL realicen un informe de factibilidad respecto de la utilización de las listas blancas. Este hecho es de vital importancia, dado que las listas negativas permiten el bloqueo de los equipos robados, no obstante, debido a la problemática de la adulteración de equipos y la dinámica que presentan las bandas delictivas se hace necesario efectuar un control a través de las listas blancas, lo que aportará al control de este tipo de incidentes.

Meses después de generada esta normativa, el MINTEL expide el Acuerdo No. 005-2012, mediante el cual, emite varios compromisos o disposiciones a ser consideradas por la ex-SENATEL, el ex-CONATEL y la ex-SUPERTEL, con el fin de abordar en forma más concreta el problema del robo de celulares. Los acuerdos que forman parte de este documento se resumen a continuación:

- Creación de las listas positivas cuya administración debe ser asumida por la ex-Superintendencia de Telecomunicaciones.
- La lista positiva estará conformada por:
    - Equipos terminales en modalidad prepago y pospago que estén asociados a los abonados empadronados.
    - Equipos importados por los prestadores del SMA o importadores autorizados.
    - Equipos terminales que se encuentren en los puntos de venta o centros de expendio.
    - Equipos terminales ensamblados en el país.
    - Equipos terminales ingresados de manera individual desde el extranjero a través de fronteras y arribos internacionales, y aquellos que son producto de un regalo o cesión.
    - Equipos terminales nuevos o de medio uso, adquiridos a través del intercambio (regalo o cesión).
    - Equipos terminales recuperados de las listas negativas. (MINTEL, 2012)

- La comercialización a la ciudadanía de equipos celulares sean estos nuevos o usados se realizará únicamente a través de:
    - Los prestadores del SMA.
    - Locales de venta que tengan una autorización de las operadoras del servicio móvil avanzado.
    - Locales de venta autorizados por la ex-Secretaría Nacional de Telecomunicaciones. (MINTEL, 2012)
- Los locales de venta entregarán la siguiente documentación:
    - Certificación de que el equipo no se encuentra en listas negativas y que está homologado.
    - Factura emitida por la empresa en donde el usuario adquirió el dispositivo, en donde debe constar el IMEI.
    - Garantía de operación del equipo. (MINTEL, 2012)
- El MINTEL realizará las coordinaciones y acciones pertinentes para penalizar la clonación, adulteración o manipulación ilícita de terminales móviles. (MINTEL, 2012)

Conforme consta en el Acuerdo Ministerial señalado, la parte medular del mismo se enfoca en la creación de las listas blancas, que estarán conformadas por varias fuentes como son los importadores, ensambladores, intercambio de equipos, entre otros. Este hecho es trascendental para el manejo de las listas positivas, dado que en este acuerdo ya se define la conformación de las listas y además se establece que la ex-SUPERTEL manejará la base centralizada de listas positivas, con lo que se garantiza que el estado ecuatoriano administrará dicha base y por tanto podrá efectuar los controles necesarios para asegurar que las operadoras cumplan con la normativa expedida.

A más de estas acciones se delinean obligaciones para los puntos de venta, como son la emisión de facturas, certificados y garantías de equipos, con lo que se busca beneficiar al usuario al momento que realice las compras de los equipos.

Con fecha 9 de agosto de 2012 el ex-CONATEL, considerando los lineamientos emitidos por el MINTEL, expidió la Resolución TEL-535-18-CONATEL-2012, que básicamente

contiene las reformas delineadas por el MINTEL y algunos temas adicionales. Es preciso señalar que a pesar de que dicho Ministerio delineó que la ex-SUPERTEL debe ser la institución que administre y maneje la base de datos centralizada, en la resolución emitida por el ex-CONATEL se establece que el administrador debe ser externo y contratado por las operadoras, en los siguientes términos:

> *"La creación, coordinación y operatividad de la base de datos de listas positivas y negativas será centralizada, y se implementará y operará por medio de un Administrador de Base de Datos de Listas Positivas y Negativas (ABD), el cual será seleccionado y contratado por los prestadores del SMA. Las bases de datos de listas positivas y negativas bajo gestión del ABD, deben permitir identificar casos de duplicidad de IMEI dentro de estos listados, así como la constancia de un identificador de IMEI en los 2 tipos de listas (positivas y negativas) para los fines de control y supervisión que correspondan. Además, se debe respetar la normativa de homologación vigente.*
>
> *(…) Se crea el Comité Técnico para la selección y contratación del Administrador de Base de Datos de Listas Positivas y Negativas, el mismo que estará constituido por el Secretario Nacional de Telecomunicaciones o su delegado, quien lo presidirá y los representantes, o sus delegados de los prestadores del Servicio Móvil Avanzado.*
>
> *El Presidente del CBD designará un Secretario del CBD, el mismo que será seleccionado de entre los funcionarios de la Secretaría Nacional de Telecomunicaciones.*
>
> *El CBD, entre otras, tendrá las siguientes atribuciones:*
>
> a. *Elaborar los lineamientos o términos de referencia y sustanciar el proceso, según corresponda, para la selección del ABD.*
> b. *Coordinar y supervisar la creación y operatividad de la Base de Datos de Listas Positivas y Negativas.*
>
> *Los acuerdos que alcance el CBD deberán ser adoptados por unanimidad de ser posible. En caso de no alcanzar unanimidad, se resolverá por mayoría simple, el Presidente tendrá voto dirimente en los casos que corresponda. Los acuerdos a*

> *los que llegue el CBD deberán ser comunicados también a la Superintendencia de Telecomunicaciones.*
>
> *(…)"* (CONATEL, 2012, p.4-5)

En la Resolución referida se establece que las operadoras deben contratar un administrador de base de datos y además que para este efecto se debe designar un Comité Técnico para la selección de dicho administrador. En este sentido, la ex-SUPERTEL ya no se encarga de esta acción y únicamente ejecutará la vigilancia y supervisión de las tareas del ABD. Por tanto, todo el control que tenía la ex-SUPERTEL al ser administradora se ve disminuido y se fijan obligaciones más concretas para dicha institución.

Cabe resaltar que en esta resolución se establece el intercambio internacional de la información de equipos robados, perdidos o hurtados y además la conexión con la base de datos de la GSMA, en los siguientes términos:

> *"Los prestadores del SMA, deberán realizar el intercambio internacional de información de terminales móviles robados, perdidos o hurtados a través de las diferentes plataformas existentes y operativas para las diferentes tecnologías de acceso.*
>
> *Para el caso de la tecnología GSM, los prestadores del SMA deberán conectarse a la base de datos de GSMA IMEI DB, en los términos que se establezcan para el efecto por parte de dicha Asociación. La SENATEL previa coordinación con el MINTEL, determinará los países con los que existe mayor comercio de equipos terminales móviles, a fin de que los prestadores del SMA incluyan la información de dichos IMEI en sus listas negativas y los bloqueen."* (CONATEL, 2012, p.7)

La GSMA (GSM Association) constituye una asociación que agrupa a la mayor cantidad de operadoras de telefonía móvil a nivel mundial, e incluye a empresas que se encargan del desarrollo de software, fabricantes y ensambladores de terminales, proveedores de servicios de Internet y organismos afines al sector de las telecomunicaciones.

Uno de los servicios principales que ofrece esta asociación es una base mundial de equipos reportados como robados, perdidos o hurtados, que se alimenta de los reportes que suben las operadoras que se encuentran asociadas y que han aceptado cargar esta

información a la plataforma de la GSMA, a fin de que pueda ser consultada a nivel internacional. En el país las operadoras del servicio móvil avanzado:

- Corporación Nacional de Telecomunicaciones CNT EP
- Consorcio Ecuatoriano de Telecomunicaciones S.A. CONECEL
- OTECEL S.A.

Todas se encuentran conectadas a la plataforma citada y suben la información en forma diaria de los equipos reportados en Ecuador.

Es necesario señalar que el acceso a dicha base de datos es exclusivamente para las operadoras y no para terceros como por ejemplo las instituciones estatales que se encargan de la regulación y control. Dichas autoridades de los países únicamente pueden solicitar un servicio de consulta individual de IMEIs, para lo cual deben efectuar una solicitud formal a dicha entidad, a fin de que se pueda obtener una autorización para este servicio.

Durante ese mismo año, el ex-Consejo Nacional de Telecomunicaciones expidió la Resolución TEL-752-25-CONATEL-2012 de 1 de enero de 2012, mediante la cual, se otorgaron dos plazos referentes a una de las disposiciones transitorias de la Resolución 535-18-CONATEL-2012:

1. 30 días laborables para que el Comité Técnico contrate al Administrador de la base de datos de listas positivas y negativas.
2. 60 días calendario para operativizar las listas positivas y negativas. (CONATEL, 2012)

Los plazos citados se establecieron considerando el informe presentado por el CBD, que contiene las acciones realizadas y un cronograma tentativo para el proceso contractual del ABD, dado que se debe establecer un proceso adecuado y conveniente para el cumplimiento de lo citado en la Resolución 535-18-CONATEL-2012, especialmente en lo que concierne a la selección para la administración de la base de datos de listas positivas y negativas y el tiempo que se requerirá para la implementación del esquema de listas positivas y negativas.

No obstante a lo dispuesto, considerando el avance del proceso mencionado, el ex-CONATEL emitió la disposición 34-28-CONATEL-2012, en la cual se establece que la ex-

SUPERTEL debe presentar al ex-CONATEL una propuesta para la implementación del esquema de listas positivas y negativas.

La ex-SUPERTEL mediante oficio STL-2012-00666 de 12 de diciembre de 2012 remitió al CONATEL la propuesta requerida.

Considerando los antecedentes expuestos, el ex-Consejo Nacional de Telecomunicaciones expidió la Resolución TEL-878-30-CONATEL-2012 de 18 de diciembre de 2012, en la cual se reforma la normativa emitida hasta la fecha, especialmente en lo que se refiere a la selección del administrador de la base de datos de listas positivas y negativas, estableciendo:

a) La derogación parcial de la Resolución 535-18-CONATEL-2012, en todo lo que corresponde a la selección del ABD y las funciones del CBD.

b) La finalización de las funciones encomendadas al CBD comité técnico para la selección y contratación del ABD.

c) Derogación del artículo dos de la Resolución TEL-752-25-CONATEL-2012.

d) Designar a la ex-Superintendencia de Telecomunicaciones que efectúe la implementación de las listas positivas y negativas, en un plazo de 90 días, acorde a la normativa vigente y siguiendo los lineamientos que el MINTEL defina para este fin. (CONATEL, 2012)

La resolución citada estableció que la ex-Superintendencia de Telecomunicaciones realice la implementación del esquema de listas positivas y negativas, con lo cual se entregó a dicha institución toda la potestad para diseñar y desarrollar este esquema, lo que facilita que las acciones de control se ejecuten de manera adecuada y que se pueda dar un seguimiento conveniente a la puesta en producción por parte de las operadoras del servicio móvil avanzado.

Esta es la última resolución que emitió el ex-CONATEL respecto a la regulación referente al registro de equipos robados, perdidos y hurtados. Posteriormente en la Ley Orgánica de Telecomunicaciones (LOT) y su Reglamento General (RLOT) se hace una breve mención al registro de teléfonos robados, perdidos o hurtados, conforme se indica a continuación.

LOT: El artículo 118 de dicha ley establece como infracción de segunda clase la activación de equipos reportados como robados (ASAMBLEA NACIONAL, 2015)

RLOT: El artículo 114 define lo siguiente:

> ***"Art. 114**.- Control previo y posterior de terminales.- La ARCOTEL establecerá los procedimientos de control, manuales o automáticos, para asegurar que los terminales cumplan con el procedimiento de homologación y obtención de la certificación respectiva. Para el efecto, tendrá la facultad de implementar mecanismos de forma individual o de forma conjunta con instituciones públicas y privadas, nacionales e internacionales para evitar que se usen u operen terminales duplicados, adulterados, no homologados, robados y los demás que la ARCOTEL defina para el cumplimiento del presente artículo.*" (Presidencia de la República del Ecuador, 2016, p.33)

Un paso importante para destacar en la Ley Orgánica de Telecomunicaciones es que establece en forma específica que la activación de equipos robados constituye una infracción atribuible a las personas naturales y jurídicas que posean un título habilitante, es decir para las operadoras del servicio móvil avanzado del país. En este contexto, se convierte en una situación de especial atención para las operadoras del país, verificar en forma continua que los equipos que estén operando en su red no estén reportados como robados, perdidos o hurtados y por tanto implementar las medidas respectivas a nivel de su plataforma para impedir que se activen equipos que estén reportados como robados. Es preciso señalar que para este fin las operadoras del servicio móvil avanzado han instalado en su red un dispositivo denominado EIR (Equipment Identity Register) Registro de la Identidad de Equipos, que básicamente contiene información del estado de un equipo en la red del prestador y que generalmente dispone de tres tipos de listas: negras, grises y blancas.

Por otro lado, el artículo 114 del Reglamento General a la Ley Orgánica de Telecomunicaciones, permite que la ARCOTEL pueda desarrollar mecanismos que eviten el uso u operación de equipos duplicados, adulterados, no homologados, robados y los demás que la ARCOTEL defina. Esta normativa es de vital importancia puesto que permite añadir al control de equipos robados otras categorías adicionales que van a

permitir fortalecer la supervisión de este ilícito, debido a que se ha detectado que los equipos robados son adulterados para volverlos a lanzar al mercado.

1.2. EQUIPOS DEL SERVICIO MÓVIL AVANZADO QUE HAN SIDO REPORTADOS COMO ROBADOS, HURTADOS Y PERDIDOS EN EL ECUADOR.

En función del análisis efectuado a la normativa emitida respecto al robo, hurto y pérdida de equipos móviles, se desprende que el control y combate de este ilícito en el ámbito de las telecomunicaciones se remonta en el Ecuador al año 2009, donde se expidió la primera regulación a manera de un procedimiento, posterior al cual se fueron dando pasos avanzados hasta convertirlo en una norma que regula el registro de equipos robados, perdidos y hurtados. La ex-Superintendencia de Telecomunicaciones fue la encargada de desarrollar las listas positivas y negativas a partir del año 2012 y fue la institución que implementó el esquema operacional del intercambio de información entre las operadoras de Ecuador.

La siguiente gráfica expone las cantidades de equipos reportados como robados, perdidos y hurtados en el transcurso de los últimos años y permite contextualizar el comportamiento que ha tenido este problema.

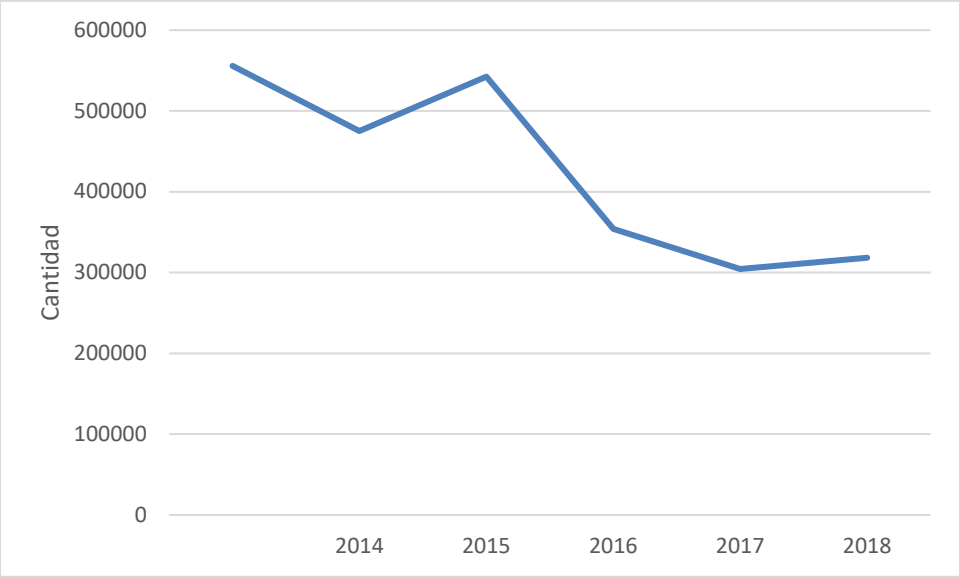

Figura 1. Equipos reportados como robados, perdidos o hurtados (ARCOTEL, 2019, p.13)

Como se observa en la Figura 1, a partir de que la ex–Superintendencia de Telecomunicaciones realizó el esquema de intercambio de la información entre dicha institución y las operadoras, y se hizo cargo de la operatividad y desarrollo de las listas positivas y negativas, acatando lo dispuesto en la resolución TEL-878-30-CONATEL-2012, la cantidad de equipos como robados, perdidos o hurtados tuvo una baja considerable hasta el año 2014. No obstante, durante el año 2015 se observa un incremento cuyo valor se acerca a las cifras mantenidas en años anteriores. Para los años 2016 y 2017 también existió un decremento de la información y para el año 2018 se observa una nueva subida de las cifras.

Es preciso destacar que las personas que se dedican a este ilícito constantemente están innovando en sus mecanismos y tácticas de robo, por lo que la normativa también debe actualizarse e ir incorporando cambios sustanciales que permitan apoyar el combate de esta actividad, de forma que desde el ámbito de las telecomunicaciones se pueda contribuir a contrarrestar con dinamismo estas acciones que afectan notoriamente a la ciudadanía ecuatoriana. En la gráfica mostrada se visualiza que este fenómeno en el año 2018 tiene un ligero incremento, situación que debe ser analizada y se debe colocar alarmas puesto que las cifras podrían incrementarse en el siguiente año y la tendencia se puede revertir generándose incrementos considerables.

En la siguiente gráfica consta la cantidad mensual de equipos reportados como robados, perdidos o hurtados durante el primer semestre del año 2018.

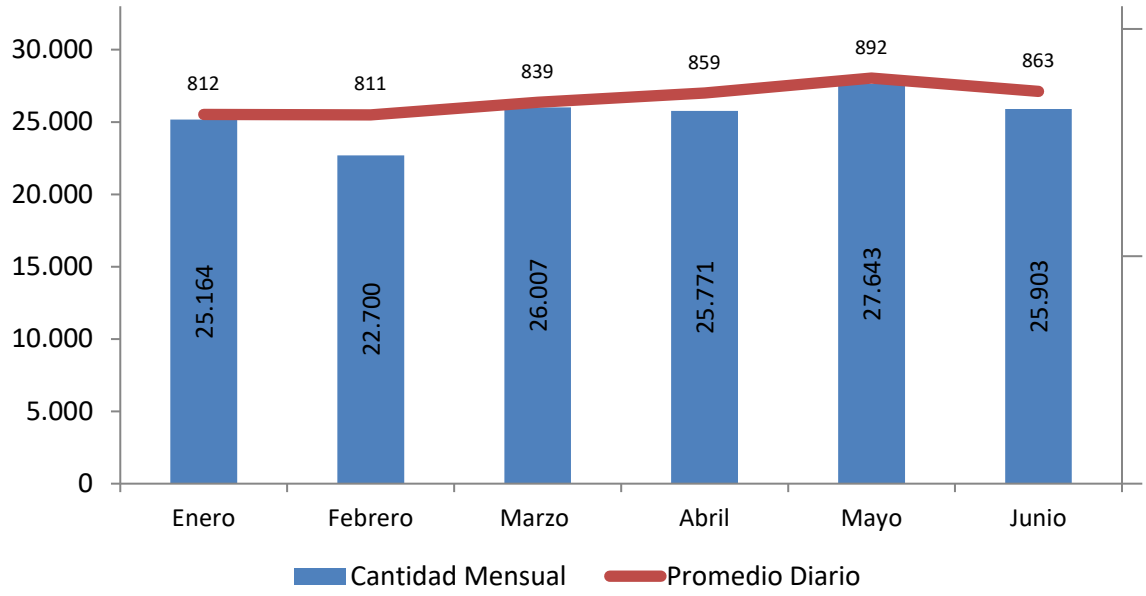

Figura 2. Equipos reportados como robados, perdidos o hurtados durante el primer semestre del año 2018. (ARCOTEL, 2018)

En la misma se puede observar que la tendencia se mantiene con un incremento no muy considerable en cada mes.

Si las cifras mostradas en la Figura 1 se trasladan a un promedio diario de robos, hurtos y pérdidas, se obtienen los siguientes resultados:

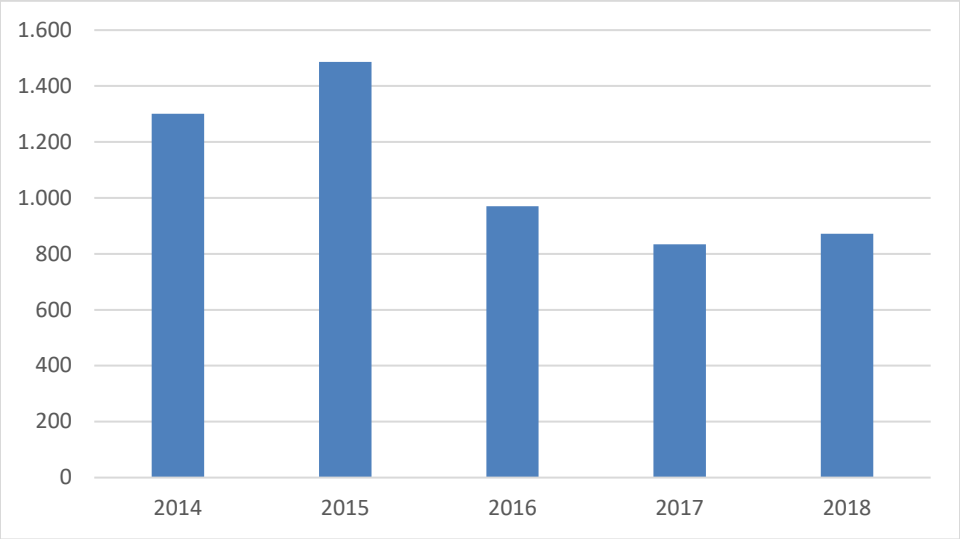

Figura 3. Promedio diario de equipos reportados como robados, perdidos o hurtados (ARCOTEL, 2019, p.13). Cálculos propios.

En la figura se observa que el promedio diario de equipos reportados como robados, perdidos y hurtados bajó del 2014 al 2018 un 33%, estableciéndose en el último año en 872, cifra que está próxima a los 1.000 equipos diarios, que constituye un valor alto para el país, puesto que, si se hace una proyección de este valor en dinero, considerando que en promedio un equipo móvil puede costar $100 USD, se obtiene que el perjuicio anual a la ciudadanía ecuatoriana es de alrededor de 31’828.000 USD.

CAPÍTULO II

2. NORMATIVA SUDAMERICANA RESPECTO AL ROBO, HURTO Y PÉRDIDA DE EQUIPOS MÓVILES COMPARADA CON LA EMITIDA EN ECUADOR

En el presente capítulo se revisará la normativa que ha sido emitida en varios países, específicamente en los que son colindantes con el Ecuador, cuya legislación referente a listas negativas pueda afectar directa o indirectamente al control que se realiza en el país.

2.1. REVISIÓN DE LA NORMATIVA EMITIDA POR PERÚ

2.1.1. DECRETO LEGISLATIVO No. 1338

Mediante Decreto Legislativo No. 1338 publicado el 6 de enero de 2017 la máxima autoridad de Perú creó el registro nacional de equipos terminales móviles para la seguridad, con el fin de luchar contra la problemática del robo de terminales móviles y apoyar a la ciudadanía en el combate de este tema, considerando que este delito tiene un alto índice en el Perú.

Dicho Decreto encarga al Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL) todo el desarrollo del RENTESEG[3]. Además, OSIPTEL tiene la función de supervisar el cumplimiento de la normativa, así como sancionar a las empresas operadoras que incumplan este decreto y su reglamento respectivo. Dicho Registro está compuesto por dos tipos de listas: Blanca y Negra. En la Lista Blanca se señala que constan todos los equipos móviles que han sido importados legalmente al país, en tanto que en la Lista Negra se especifica que se encuentran todos los equipos móviles que han sido perdidos, sustraídos o que se están inoperativos.

[3] Registro Nacional de Equipos Terminales Móviles para la Seguridad

Algo a destacar en la normativa peruana es la inclusión de la Identidad Internacional del Abonado Móvil (IMSI[4]) como un parámetro adicional. Por otro lado, se menciona que no se podrá brindar el servicio móvil avanzado en equipos que tengan un mismo IMEI. En el reglamento respectivo se definirán las condiciones y el procedimiento a seguir en estos casos.

Otro aspecto para destacar en este decreto es que los equipos exportados deben registrarse, algo adicional que no se venía ejecutando anteriormente, con lo que se pretende controlar el flujo de equipos que salgan del país como exportaciones, evitando que se puedan enviar al extranjero equipos que no cumplan con la normativa.

En el decreto se definen obligaciones para las operadoras peruanas de servicios móviles, entre las cuales se destacan las siguientes: identificar al usuario a través de la huella dactilar, mecanismo que permite que exista un mayor grado de seguridad sobre la persona que adquiere la línea telefónica del servicio móvil avanzado y que contribuye a evitar los fraudes o suplantaciones de identidades. Otras obligaciones son deshabilitar en la red del prestador del servicio móvil avanzado los equipos que hayan sido reportados como perdidos y sustraídos, así como suspender el servicio a dicho equipo terminal. De igual manera deben liberar los equipos que hayan sido recuperados, es decir volverlos a habilitar en su red. Es importante destacar que también se suspende el servicio asociado al equipo que ha sido detectado como duplicado, adulterado o que no conste en listas blancas.

En casos de que se requiera emitir mensajes a los usuarios que posean un equipo adulterado o duplicado, los prestadores del servicio móvil avanzado deben ejecutar esta acción.

Otra medida importante que se le establece al prestador del servicio móvil avanzado es que debe efectuar un adecuado tratamiento a los equipos que hayan dejado de funcionar o se encuentren en mal estado, para lo cual debe presentar un plan para operar este tipo de materiales.

---

[4] International Mobile Subscriber Identity por sus siglas en inglés

Como ya se indicó anteriormente, OSIPTEL tiene la potestad sancionadora y de tipificar las infracciones que ocurran cuando se vulnere las disposiciones expedidas. En el Decreto se señala puntualmente que la inobservancia de las obligaciones por parte de los prestadores del servicio constituye una infracción.

Adicionalmente en el Decreto se fijan los siguientes plazos:

- 30 días hábiles para la aprobación del Reglamento.
- 120 días hábiles para que OSIPTEL implemente el RENTESEG.

Es preciso señalar que el Decreto también establece que las instituciones de seguridad y vigilancia, entre las cuales consta el Ministerio del Interior pueden dictar las normas suplementarias que permitan la ejecución de lo dispuesto en el Decreto, situación importante que viabiliza el desarrollo de normas adicionales que ayuden a fortalecer el combate de este ilícito, no solo desde el ámbito de las telecomunicaciones sino también desde otros frentes de seguridad del estado peruano.

2.1.2. DECRETO SUPREMO No. 009-2017-IN

Tres meses después, con Decreto Supremo No. 009-2017-IN publicado el 30 de marzo de 2017 se expidió un reglamento, cuyo objetivo fue regular las disposiciones constantes en el decreto emitido en el mes de enero del mismo año.

El reglamento inicia detallando la composición de las listas que se denominan blancas y negras, la primera está estructurada de la siguiente manera:

- Registro de abonados
- Equipos importados
- Equipos recuperados

Para esta clasificación se destaca que a más del IMEI del equipo, se ha incluido el IMSI de la línea el servicio móvil avanzado y además información personal del abonado como son nombres completos y documento de identificación. Es decir, la lista no solo contiene datos de equipos sino también información personal del usuario, situación que permitirá identificar y asociar terminales con personas, aspecto que se considera importante para

tener un control más adecuado de la adulteración de equipos. Por otro lado, es preciso señalar que de esta lista se suprimen los equipos que han sido detectados como adulterados y exportados.

En la lista negra adicional a los equipos declarados como robados localmente y aquellos que se han reportado en otros países con los cuales tiene convenio Perú, se ha agregado las siguientes categorías:

- Terminales que no han cumplido con el intercambio seguro.
- Terminales no registrados en listas blancas
- Terminales con código de IMEI adulterado.

El reporte en listas negativas debe ser realizado por un abonado o usuario en la operadora del servicio móvil avanzado, no obstante, en el Decreto se fija que también los importadores y distribuidores de equipos pueden reportar ante la operadora del servicio móvil avanzado, lo que es razonable puesto que los equipos pueden ser sustraídos antes de que sean comercializados.

Para la liberación se establecen varias condiciones, sin embargo, la más importante es que la operadora debe verificar la identidad del usuario o abonado haciendo uso del sistema biométrico de huella dactilar, lo cual es importante para evitar suplantación de identidad o algún tipo de fraude que se pudiera realizar.

En el Decreto se determina como obligación que las operadoras del servicio móvil avanzado deben entregar información de los CDRs (registro detallado de llamada). Este aspecto se considera necesario y fundamental para ejecutar el control de los equipos adulterados y no registrados en listas blancas, puesto que de los CDRs se puede extraer el código IMEI de los terminales que han generado tráfico en cada prestador del servicio y demás otra información relevante como es el IMSI y el código de la celda de la llamada.

En lo que respecta al control de equipos adulterados y no registrados en listas blancas, el Decreto fija dos medidas:

1) Bloqueo del equipo; y,

2) Suspensión de la línea, si el usuario no proporciona el dispositivo a la operadora del servicio.

Para el caso de equipos duplicados se establece como sanción la suspensión la línea del servicio móvil avanzado.

Estas medidas constituyen un avance sustancial en el combate del robo, hurto y pérdida de equipos puesto que uno de los destinos de este ilícito es volver a introducir al mercado equipos robados, pero con el IMEI adulterado, es decir, a pesar de que se bloquea el equipo, al cambiarse el IMEI se convierte en otro equipo con una nueva identidad que puede ser vendido a un menor precio, en el mercado negro. Adicionalmente, otra medida que se observa en el Decreto es que las operadoras deberán enviar a la Policía Nacional los equipos que les hayan sido entregados por los usuarios.

Un aspecto fundamental para mencionar es que la normativa instaura la obligación de realizar el intercambio seguro de equipos, en consecuencia, un abonado o usuario que quiera cambiar su equipo por el de otro usuario, debe primero realizar una desvinculación del IMEI del equipo que está registrado en la operadora, de forma que se pueda asociar a otro usuario. Esta situación es importante puesto que se puede controlar equipos duplicados si se verifica que el mismo IMEI está asociado a varios IMSIs, una vez que se haya validado que no corresponden a personas que por descuido o desconocimiento no realizaron el intercambio seguro.

Como ya se había referido, la Policía Nacional es mencionada en el Decreto y tiene obligaciones específicas, que se citan a continuación:

- Bosquejar planos respecto al cometimiento de este delito para desplegar planes de combate.
- Elaborar procedimientos para contrarrestar el comercio ilícito de equipos móviles en la nación.
- Desarrollar un sistema que permita la realización de denuncias en forma ágil y eficiente. (Presidencia de la República de Perú, 2017)

Constituye un gran avance normativo que se establezcan acciones específicas para la Policía Nacional, a fin de combatir este fenómeno, estas acciones en beneficio de la ciudadanía son de mucha importancia y reflejan un gran avance. La Policía puede trabajar coordinadamente y en conjunto con otras instituciones del estado para diagramar acciones de control y desarrollar operativos que busquen contrarrestar este ilícito, no solamente desde el ámbito de las telecomunicaciones.

En el Decreto también se ratifica a OSIPTEL como el organismo encargado de ejecutar las sanciones e infracciones y adicionalmente se determina un plazo de 60 días laborables, a fin de que dicho organismo emita el régimen respectivo.

Por otro lado, a las operadoras se les otorga un plazo de diez meses para que implementen el proceso señalado en el artículo 35 del Decreto, relacionado con la contratación del servicio público móvil y la utilización del sistema biométrico para identificar a los abonados. Cabe señalar que para este último mecanismo se fija un plazo de cuatro meses para que las operadoras lo pongan en operación.

2.1.3. DECRETO SUPREMO No. 007-2019-IN

En el Decreto expresa que dada la aplicación del Decreto Supremo No. 009-2017-IN, se ha visto necesario emitir nuevas disposiciones para un mejor funcionamiento del RENTESEG, por lo que se expide un nuevo Reglamento del Decreto Legislativo No. 1338 y se deroga el citado Decreto Supremo No. 009-2017-IN.

El Decreto establece nuevas disposiciones, cambios e implementaciones adicionales con relación al Decreto No. 009-2017-IN. En lo que respecta a la conformación de la lista blanca se incluye una nueva categoría denominada equipos terminales móviles susceptibles de ser activados por las operadoras, que incluye a importadores (estaba considerado en el anterior Reglamento), ensambladores y equipos adquiridos en el exterior, los cuales deben cumplir con ciertos requisitos para que puedan ser inscritos. En lo concerniente al registro de abonados se asocia el IMEI del equipo con el correspondiente IMSI y/o MSISDN[5].

La lista negra contiene además el registro de equipos reportados por autoridad competente y también los equipos no registrados en la Lista de Excepción (equipos duplicados o clonados), es decir se agregan dos tipos de reportes adicionales que no constaban en el Decreto anterior. Con el último tipo de registro se agrega una clase de adulteración importante para combatir este problema, puesto que la duplicación es uno de los casos detectados en el mercado que son aplicados por los delincuentes para

[5] Mobile Station Integrated Services Digital Network.

reintroducir los equipos robados. Precisamente en el artículo 16 se detalla la forma de detección de duplicados a través de CDRs, utilizando principalmente dos métodos: simultaneidad de llamadas y conflicto distancia-tiempo, adicionalmente se menciona que la información que entregarán las operadoras correspondientes a sus CDRs, no corresponderá a:

a) Nombres de los usuarios que efectúan y reciben las llamadas.
b) Contenidos de:
    i. Llamadas de voz.
    ii. Mensajes de texto.
    iii. Mensajes de datos/voz (Presidencia de la República del Perú, 2019)

Es importante que se coloque esta aclaración en la normativa, a fin de que no exista dudas en la ciudadanía respecto a la información que se entrega a la autoridad de regulación y no se piense que se vulnera la confidencialidad de las comunicaciones.

Sobre las consultas públicas se indica que el RENTESEG implementará un módulo de consulta para entidades del estado, lo cual es realmente importante ya que el combate del robo de equipos tiene que ser una tarea coordinada y ejecutada en conjunto por varias instituciones del estado. El problema no debe ser visto desde una sola perspectiva, por ejemplo las telecomunicaciones, puesto que cada institución debe contribuir desde sus competencias para atacar más firmemente esta problemática desde la mayor cantidad de aristas posibles.

Un cambio sustancial señalado en este nuevo Decreto se relaciona con la detección de IMEIs alterados, equipos no registrados en listas blancas y aquellos que no han cumplido con el intercambio seguro, puesto que anteriormente se había definido que el Ministerio del Interior y el OSIPTEL detectan este tipo de terminales, no obstante, en el presente Decreto se especifica que esta tarea les corresponde a las operadoras.

En lo que respecta al intercambio seguro y la desvinculación del terminal, las disposiciones establecidas se mantienen con respecto a la anterior normativa derogada.

Es preciso señalar que se ha incluido, a más de los importadores y exportadores de equipos celulares, a los ensambladores y fabricantes de equipos, con lo cual se completa más tipos de equipos que pueden ser registrados en listas blancas.

Entre las obligaciones importantes para cumplimiento de las operadoras se encuentran las siguientes: registrar la identidad de las personas que contratan el servicio móvil a través del sistema biométrico de huella dactilar. Se considera que este control es fundamental para evitar fraudes y que se usen líneas del SMA indiscriminadamente en actividades ilícitas o contrarias a la normativa. Otra obligación sustancial señalada en el Decreto es la suspensión del servicio móvil asociado al equipo terminal que fue detectado con IMEI alterado o duplicado, algo necesario puesto que en el caso de duplicados existen varios equipos con el mismo IMEI y uno de ellos puede ser el original, por lo que la suspensión del servicio es lo más adecuado en este tipo de casos. Además, se ha considerado la entrega de CDRs al OSIPTEL o a la institución que esta escoja.

Es preciso indicar que las operadoras son las responsables del proceso de contratación del servicio móvil, esto incluye validar la identidad del usuario a través del sistema de verificación biométrica y no pueden comercializar chips previamente activados sin validar los datos del usuario.

Otro control destacable es impedir la habilitación de nuevas líneas en equipos no registrados en listas blancas, para este efecto la operadora debe ejecutar una consulta en línea a las listas blancas y negras.

Adicionalmente se establece que los usuarios que resultaren perjudicados por la adquisición de un equipo con IMEI alterado pueden presentar su denuncia ante el INDECOPI, institución con competencia para receptar los reclamos y verificar las infracciones cometidas a las disposiciones constantes en el Código de Protección y Defensa del Consumidor. Este hecho constituye un logro realmente destacable, puesto que el abonado conoce de antemano que puede acudir ante una autoridad del estado para tramitar e investigar sus denuncias en el caso de comprar un terminal adulterado o irregular.

Las campañas de difusión de los temas referentes a este Decreto deben ser divulgadas por varias entidades tanto estatales como privadas, entre las cuales se destaca OSIPTEL, INDECOPI y varios ministerios por parte del estado peruano, en tanto que las operadoras, importadores de equipos móviles y las casas comercializadoras de equipos para la parte privada.

Es importante destacar que se establece una disposición transitoria que permite al OSIPTEL emitir disposiciones adicionales en caso de que se desarrollen nuevas soluciones que posibiliten realizar un bloqueo de equipos más eficiente, aspecto que es de mucha relevancia puesto que permitirá adoptar mecanismos que presenten mayores prestaciones a futuro.

Por otro lado, en caso de que se recuperen los equipos, se designa al Ministerio del Interior o la Policía Nacional como las instituciones encargadas de realizar la devolución de los equipos a los titulares de estos.

En lo que concierne al intercambio seguro, existe una disposición transitoria que otorga un plazo de 150 días hábiles para que OSIPTEL implemente el procedimiento necesario para su seguimiento, además se menciona que los equipos que se encuentren en funcionamiento a la fecha de vigencia del decreto se vincularán al usuario en el que esté el servicio móvil activo.

En lo que respecta a la conformación de las listas blancas, así como el bloqueo de equipos, se emiten varias disposiciones transitorias que contienen varias acciones. A continuación, se destacan las principales:

- Fijación de un cronograma por parte del OSIPTEL y del Ministerio del Interior para el bloqueo de equipos móviles, a ser expedido en un plazo de diez días. Concluido este cronograma se debe comenzar de manera permanente el bloqueo de IMEIs inválidos.
- Incorporación a las listas blancas de todos los equipos que fueron importados previo a la entrada en vigencia de este Decreto, por parte de los importadores y las operadoras, siempre y cuando cumplan con los requisitos técnicos que se establecen en dicho cuerpo legal.
- Habilitación de IMEIs pregrabados por el fabricante que correspondan a IMEIs inválidos por un plazo de hasta 1 año, cuyo IMEI físico y lógico coincida. En este escenario, los abonados deben proceder a homologar sus equipos en este mismo plazo, caso contrario sus equipos serán bloqueados.
- Para el caso de equipos no homologados pero que sus IMEIs no sean alterados, se otorga el plazo de 1 año para que los abonados procedan a su homologación, de no ejecutar esta actividad las operadoras ejecutarán el bloqueo de estos.

2.2. REVISIÓN DE LA NORMATIVA EMITIDA POR COLOMBIA

La Ley 1453 expedida en Colombia en el año 2011, estableció en sus artículos 105 y 106 los plazos para desarrollar las listas positivas y negativas, así como que la Comisión de Regulación de las Comunicaciones es la entidad delegada para definir su implantación, modelo técnico y actualización de las bases, entre otros aspectos.

En función de la regulación citada y del Decreto 1630 de 2011, la Comisión de Regulación de las Comunicaciones emitió la Resolución No. 3128 de 7 de septiembre de 2011, la cual estableció el marco regulatorio para la restricción de operación de terminales móviles que han sido denominados como hurtados y perdidos en las redes de las operadoras del servicio móvil avanzado.

La Resolución citada ha tenido varias actualizaciones parciales desde que fue emitida, en las cuales se han modificado varios artículos y se han añadido acciones para combatir el robo, hurto y pérdida de teléfonos celulares (CRC, 2019).

2.2.1. RESOLUCIÓN No. 3128

Se establece inicialmente que la base de datos debe ser administrada por un ABD (Administrador de Base de Datos) cuya contratación debe ser realizada por los operadores de servicios móviles, quienes también deben asumir los costos de su implementación, funcionamiento y mantenimiento. Adicionalmente se define otra base de datos denominada BDO que constituye la Base de Datos Operativa administrada por el operador móvil. Estas bases de datos se deben interconectar entre si para fines de consulta y actualización respectiva.

Además, se especifica lo siguiente:

- Los operadores móviles deben activar únicamente equipos que hayan sido homologados en Colombia.
- Para el reporte de robo, hurto y pérdida de los equipos, así como para su liberación se definen las obligaciones que dichos operadores deben cumplir para ejecutar el

proceso. Es preciso destacar que para la liberación la CRC (2015) ha establecido tres métodos de validación que pueden ser usados, estos son:

a) Clave proporcionada al usuario el momento de efectuar su reporte de robo, hurto y pérdida.

b) Presentación física del equipo.

c) Validar la identidad del abonado a través de la central de riesgos, sistemas biométricos o preguntas de seguridad.

Los Operadores Móviles Virtuales también deberán receptar los reportes de robo, hurto y pérdida de sus usuarios, para lo cual deberán considerar los mecanismos definidos en la resolución.

Un aspecto importante para considerar es que se establece como obligación que los PRSTM[6] deben tener implementado un proceso que les permita identificar IMEIs duplicados, inválidos, sin formato, no homologados y no registrados en listas positivas. Además, para el caso de IMEIs duplicados la Comisión de Regulación de Telecomunicaciones ha dispuesto que los PRSTM implementen una funcionalidad que les permita verificar la dupleta IMEI-IMSI en el EIR.

La principal obligación del Administrador de la Base de Datos Administrativa constituye el dimensionamiento, monitoreo, mantenimiento, provisión de la infraestructura de hardware y de software correspondientes a dicha base. Otras obligaciones definidas por la CRC (2016) para destacar son las siguientes:

- Intercambiar información entre la BDA y la BDO.
- Mantener políticas de respaldo de la información.
- Garantizar la privacidad de la información personal contenida en la base de datos.
- Proveer un mecanismo de consulta para las instituciones estatales de telecomunicaciones.

[6] PRSTM: Proveedor de Redes y Servicios de Telecomunicaciones Móviles

- Proporcionar una consulta registro a registro a la ciudadanía a través de un portal web.
- Entregar reportes periódicamente a la CRC sobre la operación de la base de datos.
- Intercambiar los reportes de hurto, extravío y liberación con otros países con los cuales Colombia mantenga acuerdos internacionales.
- Mantener operativa la BDA las 24 horas y los 7 días a la semana.
- Excluir de las listas negativas los IMEIs de terminales que han culminado el tiempo de permanencia establecido en la Resolución CRC 3128.

La conformación de la BDA positiva es la siguiente:

- IMEIs de equipos importados legalmente a Colombia desde el 1 de diciembre de 2015.
- IMEIs de los usuarios que efectuaron el registro de propiedad del equipo.
- IMEIs que se cargaron por los PRSTM hasta el 30 de noviembre de 2015. (CRC, 2016)

En tanto que la BDA negativa se compone de:

- IMEIs de equipos reportados por hurto y pérdida en Colombia.
- IMEIs de equipos reportados por hurto y pérdida en países con los que Colombia tiene acuerdo internacional.
- IMEIs de equipos reportados por no registro en las listas positivas.
- IMEIs de equipos duplicados, inválidos y no homologados.
- IMEIs de equipos reportados por los operadores como reincidente.
- IMEIs de equipos reportados por fraude en la suscripción del servicio, pérdidas en inventarios o que aún no han sido vendidos. (CRC, 2016)

En lo que respecta a la BDO positiva, su composición se da únicamente por la información de IMEI-IMSI-MSISDN de los equipos registrados (CRC, 2016). La BDO negativa se compone de:

- IMEIs de equipos reportados por hurto y pérdida en Colombia.
- IMEIs de equipos reportados por hurto y pérdida en países con los que Colombia tiene acuerdo internacional.
- IMEIs de equipos reportados por no registro en las listas positivas.
- IMEIs de equipos duplicados, inválidos y no homologados.
- IMEIs de equipos reportados por hurto o extravío descargados de la GSMA que provengan de otros países.
- IMEIs de equipos reportados por los operadores como reincidente.
- IMEIs de equipos reportados por fraude en la suscripción del servicio, pérdidas en inventarios o que aún no han sido vendidos. (CRC, 2016)

Es preciso señalar que, para el caso de hurto y extravío, la CRC (2016) ha establecido que los PRSTM deben recabar los siguientes datos:

- ✓ IMEI del equipo.
- ✓ Tecnología del equipo.
- ✓ Nombre del PRSTM.
- ✓ Datos del usuario que efectuó el reporte.
- ✓ Fecha, hora y ubicación del sitio en que se produjo el suceso.

Adicionalmente, en caso de hurto, a partir del 29 de febrero de 2016, el PRSTM debe solicitar información relativa a:

- ✓ Si la víctima es menor de edad.
- ✓ Si el suceso fue con violencia.
- ✓ Si se usó armas blancas, de fuego, etc.
- ✓ Correo electrónico del usuario que realiza el reporte.

Es importante destacar que en Colombia se establece un ingreso temporal en la base de datos de listas negativas, tanto para bloqueos realizados a nivel nacional como para aquellos efectuados a nivel internacional. Se define un tiempo de 3 años para IMEIs reportados en Colombia y 1 año para IMEIs de otros países.

El ABD es el encargado de remitir cada 6 meses a los PRSTM la totalidad histórica de los IMEIs que han sido retirados de la base de datos negativa por tiempo mínimo de permanencia. Los PRSTM deben verificar si dichos IMEIs cursan tráfico en su red, en caso afirmativo deberán bloquear los equipos que hayan sido detectados y serán denominados bajo la denominación de reincidentes.

Los PRSTM son los encargados de realizar el registro del IMEI para planes pospago, para lo cual deben asociar los datos del propietario o usuario del equipo. Para prepago el registro lo deben efectuar los usuarios en los PRSTM de forma virtual, presencial o mediante atención telefónica.

Previo a realizar el registro del IMEI, sea pospago o prepago el PRSTM debe validar los datos del usuario en al menos una de las bases de datos de las siguientes instituciones: Registraduría Nacional del Estado Civil, Centrales de Riesgo crediticio o datos históricos del usuario en el PRSTM.

Para el registro en prepago, la CRC (2016) ha precisado los siguientes pasos:

a) Activación del equipo con la sim card

b) Verificación de la tenencia del equipo

c) Identificar el IMEI

d) Confirmar y actualizar los datos presentados por el abonado

e) Verificar los datos proporcionados

f) Confirmar el registro por parte del operador móvil

Si el equipo ha sido adquirido en el exterior el usuario debe presentar ante el operador móvil en el cual tiene su servicio, la factura de compra del equipo en el extranjero, comprobante de pago a su nombre o la Declaración de único responsable del uso y propietario de equipos terminales móviles (Anexo 1 de la Resolución No. 3128).

El PRSTM es el encargado de notificar al ABD todo cambio en los datos de identificación de un usuario que ya se encuentra incluido en la BDA y se debe asociar a los datos de otro usuario. El ABD debe actualizar este cambio en la BDA.

Para el caso del registro de los IMEIs de los equipos importados la Resolución No. 3128 señala que el proceso iniciará a través del ABD, el cual será reemplazado una vez que

se adecúe el sistema informático de la DIAN. Para ensambladores, equipos de prueba y garantías el ABD será quien adelante el proceso de carga.

Cabe resaltar que el MINTIC, la Superintendencia de Industria y Comercio, la CRC, autoridades policiales y judiciales tienen un acceso en línea a la BDA. (CRC, 2016)

Para incluir un IMEI en la base de datos de lista negativas se debe considerar lo siguiente:

a) Para el caso de IMEIs hurtados y extraviados en Colombia, el bloqueo en todas las redes de los PRSTM, que incluye el intercambio entre BDA y BDOs, debe realizarse en 25 minutos.
b) Los IMEIs que han sido reportados en otros países tienen que ser cargados por los PRSTM diariamente en un plazo de 48 horas siguientes a que hayan sido puestos en el aplicativo de la GSMA. Se consideran dos casos, los países con los cuales se ha establecido el intercambio de bases de datos negativas por medio de la GSMA y aquellos con los que se realice un intercambio de IMEIs con otros países utilizando otro medio.
c) Los IMEIs que han sido bloqueados por procesos de depuración deberán ser compartidos con la BDA en un plazo de hasta 48 horas luego del bloqueo, en tanto que la BDA los intercambiará hacia los otros PRSTM hasta el siguiente día calendario.

En la Resolución No. 3128 se ha establecido una etapa de verificación que consiste en la detección de IMEIs (CRC, 2016):

- Sin registro en la BDA positiva.- Equipos que no constan en la BDA positiva.
- Inválidos.- Equipo que no tiene TAC en la GSMA o en la lista de TACs que corresponden a marcas y modelos homologados.
- No homologados.- Equipos que no constan en el listado de TACs que corresponden a marcas y modelos homologados.
- Sin formato.- IMEIs que tengan una longitud diferente a 14 dígitos o que tengan caracteres alfabéticos.
- Duplicados.- IMEIs repetidos cuya detección se realiza utilizando:

- Simultaneidad de llamadas: IMSIs distintos que están asociados a un mismo IMEI, cuyas llamadas se superponen en el tiempo.
- Conflicto tiempo distancia: IMSIs distintos emparejados con un mismo IMEI que efectúan llamadas en un tiempo menor o igual a T a una distancia D o más.
- Criterio de consistencia entre el IMEI y su tipo de conexión a la red: el PRSTM puede hacer uso de otros campos del CDR como: Mobile Station Classmark.

Para lo cual se deben utilizar los CDRs de voz y datos, considerando varias etapas y para el caso de IMEIs duplicados en función de dos ciclos:

- Intrared.- Los PRSTM identificarán en su propia red los IMEIs que detecten como sin registro en la BDA positiva, duplicados, inválidos, no homologados y sin formato.
- Intered.- Los PRSTM identifican entre sus redes los IMEIs que detecten como sin registro en la BDA positiva, duplicados, inválidos, no homologados y sin formato.

Para el caso de IMEIs repetidos en dos o más redes se ha determinado la entrega de la siguiente información de CDRs:

- Hora de inicio y fin de cada llamada.
- IMEI
- IMSI
- Códigos del sector de inicio y fin de llamada (CI: identidad de la celda) y (LAC: código de localización de área).

Para la detección intra-red se ha contemplado la entrega periódica de las siguientes cantidades totales(CRC, 2016):

- IMEIs únicos en la red
- IMEIs inválidos
- IMEIs sin formato

- IMEIs duplicados
- IMEIs no homologados
- IMEIs no registrados en la BDA positiva
- IMEIs válidos

Para la detección inter-red se ha contemplado que los PRSTM deben tener habilitado un acceso para el MINTIC y la CRC sobre la siguiente información total mensual (CRC, 2016):

- IMEIs recibidos discriminados por prestador
- IMEs únicos entre todos los prestadores
- IMEIs repetidos entre redes
- IMEIs detectados duplicados
- IMEIs detectados duplicados por simultaneidad de llamadas
- IMEIs detectados duplicados por conflictos de distancia y tiempo

Para el caso de IMEIs duplicados los usuarios que han sido notificados por este tipo de causal deben presentar su documento de identificación, de ser posible respaldos de la compra del equipo y el Anexo 2 de la Resolución CRC 3128. Luego del plazo establecido, el PRSTM procederá a incluir en su EIR el IMEI duplicado y su IMSI asociado, los otros PRSTM deberán ingresar el IMEI en su EIR sin el IMSI. Adicionalmente el PRSTM deberá notificar a las autoridades los casos de IMEI duplicado entregando la información presentada por el usuario, el Anexo 2 de la Resolución CRC 3128 y demás documentación relacionada al caso.

Para todos los casos que corresponden a la detección de IMEIs a través de CDRs se le notifica al usuario a través de mensajes cortos (SMS) y mecanismos adicionales como son mensajes flash, mensajes USSD, enrutamiento a IVR, entre otros, que su equipo tiene una irregularidad y debe proceder a regularizarlo. Se le otorga un plazo para que realice esta acción, caso contrario el PRSTM ejecuta el bloqueo del equipo y no puede operar en su red.

Se contemplan varias metodologías para la liberación de los equipos que hayan sido bloqueados en este escenario, en todas ellas el equipo debe haber cumplido con las validaciones establecidas, previo a que pueda efectuarse el retiro de las listas negativas.

Un aspecto importante para destacar en la mencionada resolución es la creación del Comité Técnico de Seguimiento (CTS), el cual está conformado por los operadores móviles encargados de la implementación de la base de datos de listas positivas y negativas, que estarán representados por su representante legal o su apoderado. No obstante, se establece que dicho comité estará presidido por un representante de la CRC, quien podrá estar acompañado de un delegado del MINTIC.

Las propuestas definidas por el CTS se deben consignar en actas y tienen que ser aprobadas por el voto mayoritario de sus representantes.

Finalmente se delega el control del cumplimiento de la resolución CRC 3128 al MINTIC.

2.3. COMPARACIÓN DE LA NORMATIVA EMITIDA EN ECUADOR CON LA EXPEDIDA EN COLOMBIA Y PERÚ

Las normativas actuales de los países colindantes con Ecuador han sido expedidas en los últimos años, en el caso de Colombia su regulación ha sido actualizada constantemente desde que fue generada en el año 2011, con varias modificaciones elaboradas en cada año lo que supone una ventaja con la de Ecuador en donde la última reforma de la normativa de equipos robados, perdidos y hurtados fue emitida en el año 2012, en tanto que en Perú el Reglamento del Decreto Legislativo No. 1338 fue expedido el 4 abril de 2019, es decir recientemente. En este sentido, se nota una clara desventaja con la normativa de ambos países, puesto que el robo de celulares tiene una dinámica que evoluciona y varía en el tiempo, razón por la cual es necesario que la normativa y los controles que se realizan en cada país estén en constante actualización, a fin de combatir este ilícito con más herramientas. El ex-Consejo Nacional de Telecomunicaciones en su momento y la Agencia de Regulación y Control de las Telecomunicaciones no han expedido desde el año 2012 una actualización a la norma vigente, en lo que concierne a listas positivas y negativas. A época actual se hace imperante una reforma que contemple

formas de combatir a los nuevos escenarios y las metodologías que han surgido en el robo de celulares.

2.3.1. PRINCIPALES SEMEJANZAS Y DIFERENCIAS NORMATIVAS

Existen varias diferencias entre las normativas examinadas, a continuación, se expondrán las principales:

- La Resolución CRC No. 3128 describe la generación de dos bases de datos:
    - La base de datos administrativa (ABD); y,
    - La base de datos operativa (BDO).

  Es decir, hay una base que es administrada por una empresa externa y otra que la tiene a cargo cada operador móvil. Cada una a su vez se subdivide en la base de datos de listas negativas y base de datos de listas positivas. En Ecuador y en Perú, estas bases de datos son únicas y son gestionadas a través de una sola institución estatal. Es este aspecto, cada país ha definido la forma en que controlará las bases de datos, sin embargo, se ven claras diferencias concretamente con el modelo colombiano. Una empresa externa como administradora de la base de datos puede generar ciertos beneficios como son que el estado no tiene que invertir en su mantenimiento y gestión y la responsabilidad de su manejo cae en el lado de las operadoras, en el modelo con base de datos estatal se puede tener una supervisión más directa y los reportes y cambios que se requieran se pueden obtener de manera flexible y en el momento que se requiera.

- La composición de la base de datos de listas positivas varía en algunos aspectos entre cada país, conforme se puede demostrar a continuación:

Tabla 2. Comparativa de la composición de las Listas Positivas de Colombia, Perú y Ecuador

Fuente: Colombia (Comisión de Regulación de Comunicaciones), Perú (Decreto Presidencial), Ecuador (ExCONATEL)

COLOMBIA	PERÚ	ECUADOR
Tiene dos listas: • BDA (Administrador) • BDO (Operadoras)	Tiene una sola lista, cuya composición es:	Tiene una sola lista, cuya composición es:
a) BDA 1. IMEIs de equipos importados legalmente a Colombia desde el 1 de diciembre de 2015 2. IMEIs de los usuarios que efectuaron el registro de propiedad del equipo. 3. IMEIs que se cargaron directamente por los PRSTM hasta el 30 de noviembre de 2015.	1. IMEI correspondiente a los equipos terminales móviles asociados al IMSI y/o MSISDN de las líneas activadas por las operadoras del país. 2. Terminales susceptibles de ser activados: -Equipos importados -Equipos ensamblados -Equipos adquiridos en el exterior 3. Equipos recuperados de la lista negra. 4. Otros equipos terminales autorizados por el OSIPTEL	1. Equipos terminales en modalidad prepago y pospago que estén asociados a los abonados empadronados 2. Equipos importados por los prestadores del SMA o importadores autorizados. 3. Equipos terminales que se encuentren en los puntos de venta o centros de expendio 4. Equipos terminales ensamblados en el país 5. Equipos terminales ingresados de manera individual desde el extranjero a través de fronteras y arribos internacionales, y aquellos que son producto de un regalo o cesión 6. Equipos terminales nuevos o de medio uso, adquiridos a través del intercambio (regalo o cesión) 7. Equipos terminales recuperados de las listas negativas
b) BDO 1. IMEI-IMSI-MSISDN de los equipos registrados		

En Colombia se manejan dos bases de datos, una centralizada y otra para cada prestador del SMA, en tanto que Ecuador y Perú tienen una sola base de datos centralizada. En el único componente que coinciden las tres bases de datos es en el registro de los equipos importados. En otro aspecto que tienen cierta concordancia es en lo que respecta al registro de los equipos asociados a las líneas activadas en los prestadores del SMA.

- En lo que concierne a las listas negativas en Colombia se registra una categoría adicional denominada “equipos reincidentes” que corresponden a aquellos que salieron de la base de datos negativa por tiempo de permanencia, sin embargo, fueron nuevamente detectados en operación posteriormente, por lo que deben ser ingresados en listas negativas. En el caso de Perú, se registra adicionalmente los equipos inoperativos, que constituyen aquellos que han perdido una funcionalidad que no les faculta tener un desempeño adecuado en las redes de los prestadores del servicio móvil avanzado.
- En la norma ecuatoriana únicamente se cita como parte de las listas negativas los terminales reportados como robados, hurtados y perdidos, situación que difiere de las normas peruana y colombiana, en donde además de esta categoría se ha incluido a los equipos: duplicados, alterados, no homologados, no registrados, entre otros, lo que constituye una significativa desventaja para combatir el problema del robo de equipos, puesto que se ha evidenciado que los equipos sustraídos son adulterados y cambiados su identidad, situándolos en alguna de las categorías citadas arriba. Este hecho se debe principalmente a que la norma ecuatoriana no ha sido actualizada hace más de 7 años.
- La normativa colombiana establece en detalle los criterios para la detección de equipos con irregularidades: sin formato, inválidos, no homologados, duplicados y no registrados, mediante el uso de CDRs de voz y datos y establece los procesos puntuales que deben seguir los PRSTM y los usuarios en cada caso. La normativa peruana menciona la detección de IMEIs adulterados, así como el bloqueo de dichos equipos, no obstante, en el documento no se define el proceso completo que deberán seguir los PRSTM, dicho proceso se indica que se detallará en otros documentos. Al respecto, la norma ecuatoriana referente a listas positivas y

negativas no menciona este tipo de equipos irregulares ni describe proceso alguno para la detección y control de estos, únicamente en el en el artículo 114 del Reglamento General de la Ley Orgánica de Telecomunicaciones se manifiesta que se podrán definir procesos para evitar que se usen equipos duplicados, adulterados, no homologados, robados y los demás que la ARCOTEL defina.

- En Perú y Colombia se realiza el control de equipos duplicados a través de los criterios de simultaneidad de llamadas y conflicto distancia-tiempo, en tanto que en la normativa de Ecuador no se define los criterios a utilizar para realizar este tipo de control.
- Otra diferencia marcada es que Colombia y Perú registran los equipos que exportan, en cambio que en Ecuador no se realiza este proceso.
- Es importante señalar que únicamente en Perú se valida la identidad de sus abonados a través del uso de un esquema de verificación de la huella dactilar, aspecto que permite realizar un control más efectivo de la identidad de los usuarios que se suscriben para utilizar el servicio móvil avanzado. Esta validación es muy importante, a más de que simplifica los procesos de control, puesto que permite la ejecución de un procedimiento que brinda mejores garantías de seguridad.
- Una semejanza importante en los tres países es que todos permiten el ingreso de equipos robados, perdidos y hurtados que hayan sido reportados en otros países con los cuales se tenga acuerdo o exista una legislación que soporte su compartición. Este control es fundamental para combatir el traslado de equipos robados de un país a otro, evitando el comercio ilegal de estos equipos en países vecinos.

Se evidencia que actualmente el control de equipos irregulares no se debe enfocar únicamente en bloquear los reportes de robo, sino que es necesario efectuar la detección de equipos duplicados y alterados, puesto que Colombia y Perú están bloqueando este tipo de terminales, los cuales pueden ingresar y ser activados en Ecuador debido a que existe una frontera común con ellos. Es por esta razón que es imperante que en Ecuador se realice un control de equipos duplicados y adulterados e incluso se podría pensar en intercambiar este tipo de reportes con los vecinos Colombia y Perú, a fin de que se pueda

tener un control más efectivo a nivel regional y de ser necesario se lo podría realizar incluso con otros países.

CAPÍTULO III

3. ALTERNATIVAS REGULATORIAS Y TÉCNICAS EN TELECOMUNICACIONES QUE APOYEN EL CONTROL DEL ROBO, PÉRDIDA Y HURTO DE EQUIPOS CELULARES.

En el presente capítulo se analizarán varias alternativas que han sido recomendadas por organismos internacionales para contrarrestar el robo de equipos celulares, así como aplicaciones que brindan apoyo para combatir este ilícito.

3.1. RECOMENDACIÓN UIT-T Q.5050.

La Unión Internacional de las Telecomunicaciones entidad designada por las Naciones Unidas para regular las telecomunicaciones a nivel internacional, ha expedido la Recomendación UIT-T Q.5050 que define una solución marco para contrarrestar la falsificación de dispositivos TIC, dentro de la lucha contra este ilícito y el robo de dispositivos TIC. El objetivo de esta recomendación es establecer un marco de referencia que precise los requisitos y ponga de manifiesto las dificultades que se deben observar al momento de generar soluciones para combatir el uso de equipos TIC falsificados.

Una recomendación general que efectúa la UIT para los países que deseen optar por desplegar este tipo de soluciones es que deben intervenir múltiples instituciones y organismos del estado y también implementaciones tecnológicas que hayan sido puestas en operación en otros países que ya han tratado este tema, con el objetivo de conseguir guías y ejemplos que ya han dado resultados. Las entidades del estado principalmente involucradas en este tema, a más de las instituciones de telecomunicaciones son la policía y las aduanas, las cuales deben recibir colaboración de la industria.

3.1.1. Consideraciones previas.

La UIT (2019) establece varios aspectos que se deben considerar previo a emitir cualquier solución. A continuación, se analizan los principales:

a) Detección de equipos TIC falsificados. – Las personas que se dedican a este ilícito principalmente alteran el identificador único del dispositivo de manera que a través de este mecanismo se pueda vulnerar los controles de las entidades estatales.
b) Eliminación de dispositivos TIC falsificados. – La UIT recomienda tres medidas:
    a. Validación física o remota de equipos de las características del producto original.
    b. Cese de su uso.
    c. Incautación del equipo.

    Sin embargo, estas acciones para que sean eficaces requieren varios desafíos como la verificación física de un equipo, la cual solo puede realizarse mediante una reparación de este, algún evento de vigilancia o si una entidad judicial lo requiere. Esta verificación podría realizarse validando los identificadores únicos del equipo (IMEI), no obstante, se necesita una conexión externa a Internet y realizar una comparación con una base de datos central.

    Por otro lado, el cese de su uso solo podría afectar al usuario que adquirió el equipo en forma lícita sin notar que fue falsificado o adulterado, por lo que el usuario va a sentir que se han vulnerado sus derechos, más aún si se le llegaré a incautar el dispositivo, hecho que requiere además de la presencia de autoridades policiales.
c) La UIT recomienda restringir las importaciones, circulación y venta de equipos falsificados, sin embargo, esta medida implicaría la incorporación de controles en aduanas con personal del SENAE y para la venta de equipos se requeriría de efectivos policiales que tomen medidas en los locales o centros de expendio de equipos. Es preciso mencionar que en lo referente a telecomunicaciones también se podrían tomar medidas en estos locales, no obstante, se debería verificar si la efectividad es igual o inferior ya que la infracción caería únicamente en el ámbito de las telecomunicaciones.
d) En lo que respecta al usuario, la UIT establece que se debe efectuar las debidas publicidades que hagan caer en cuenta a la ciudadanía las ventajas que tienen al adquirir dispositivos genuinos, no robados ni adulterados. Adicionalmente, tal como se analizó en el literal b), se debe considerar los efectos que se tengan en el usuario ya que el equipo lo puede estar utilizando para una actividad esencial, además de que

se debe tratar de buscar los métodos ideales de contacto en caso de que no se traten de terminales que solo usen datos.

e) Se menciona también la eliminación de obstáculos para la importación de equipos genuinos, situación importante pero que también recaería en otras instituciones del estado como son el SENAE y el COMEX.

3.1.2. Requisitos marco.

Como requisitos marco que cita la UIT (2019) para atacar el problema se destacan los siguientes:

a) **Mantener una estrecha comunicación entre operadores, industria y asociaciones de consumidores. –** Aspecto importante para llegar a consensos y considerar la posición y opinión de los involucrados en el problema, con el objetivo de sacar los mejores compromisos y acciones a ejecutar.

b) **Identificadores únicos confiables. –** La UIT recomienda que la industria adopte identificadores que no puedan ser modificados y que integren medidas para detectar un cambio en cuyo caso se deberá inhabilitar el dispositivo. En este sentido en el caso de los IMEIs de los equipos móviles del servicio móvil avanzado, se ha observado que pueden ser fácilmente cambiados y detectar esa alteración no ha sido factible por los fabricantes de dispositivos.

   En una investigación realizada por Kumar y Kaur (2015) se menciona que existen 2 técnicas para modificar el IMEI de un equipo móvil:

   - Basadas en hardware. - consiste en substituir en el terminal el chip RX12 (equipos antiguos).
   - Basadas en software. – para cambiar el IMEI se utilizan varias herramientas y flashes de hardware en el mercado negro.

     En la siguiente tabla tomada de la publicación se muestran varias de estas herramientas de tipo gratuito y pagadas.

Tabla 3. Fabricantes de chipset y herramientas para modificar el IMEI (Kumar y Kaur, 2015, p. 531)

FABRICANTE DE CHIPSET	FABRICANTES DE EQUIPOS QUE USAN EL CHIPSET	HERRAMIENTAS PARA MODIFICAR EL IMEI
MediaTek (MTK)	LG, Motorola, Micromax, Lava, Lenovo, Panasonic, Samsung, HTC, entre otros.	SP_flash_tool, MTK Droid Root and Tools, Mobile Uncletool, SigmaKey.
QualComm Snapdragon	Samsung, NOKIA, HTC, LG, Lenovo, Xiaomi, Micromax etc.	NV-items Reader Writer tool Sigmakey.
Broadcom	Lava, Samsung, Karbonn, Micromax, entre otros.	Sigmakey, Repair 3G tool, Brcm Flash Tool, MultiFun Tool Setup.
Apple A4, A5, A6.	Apple iPhone, iPad	Ziphone

Conforme se muestra en el cuadro, es evidente que la modificación del IMEI es un problema latente que complica el control de los equipos robados, puesto que el bloqueo del equipo a través del EIR, no es suficiente si los individuos que realizan este tipo de atracos cambian el IMEI y lo reintroducen al mercado, de forma que evaden los controles implementados. A pesar de que los teléfonos actuales vienen con más seguridades y en la mayoría de los equipos la carcasa viene integrada en el dispositivo y no es extraíble fácilmente, los delincuentes han buscado formas de reprogramar la identidad de los equipos.

Esta alteración ha provocado que se encuentren en el mercado diferentes tipos de casos, como son:

IMEI sin formato. – IMEI que no cumple con el estándar de 15 dígitos numéricos y por tanto puede contener letras, menor cantidad de dígitos o incumplir con el algoritmo de Luhn (método diseñado para validar la serie de dígitos).

IMEI no asignado. – IMEI cuya estructura cumple con el formato, pero no ha sido asignado internacionalmente a una marca y modelo de dispositivo del mercado.

IMEI duplicado. – IMEI que ha sido copiado idénticamente de otro dispositivo que cumple con los estándares de la industria, y ha sido

replicado en una o más ocasiones, por tanto, en controles simples basados en IMEI no puede ser detectado y se requiere de técnicas más avanzadas para su detección.

IMEI adulterado con formato. – IMEI válido que corresponde a un equipo distinto al original colocado por el fabricante. Este caso es el más complicado de detectar, puesto que requiere de verificaciones físicas y comprobaciones adicionales para determinar que fue alterado.

Todos estos casos convierten los controles para contrarrestar el robo de celulares en una tarea complicada y que requiere el apoyo de varios organismos del estado, caso contrario, los controles tienen menos o poca eficacia.

c) **Base de datos centralizada. -** La UIT recomienda la utilización de una base de datos centralizada que contenga identificadores únicos y que sirva de consulta para los diversos organismos del estado como son las aduanas, la policía nacional, organismos de control y regulación, etc.

d) **Colaboración continua entre autoridades aduaneras y organismos del estado competentes. –** Tal como se ha citado en varias partes de este estudio, la colaboración entre las diferentes instituciones del estado es fundamental para combatir este problema, este aspecto lo reitera la UIT en todo su documento.
En este aspecto es preciso mencionar que a través de la Resolución No. 111 de 17 de septiembre de 2013, el COMEX[7] estableció en Ecuador que los IMEIs de todos los equipos que se importen deben ser incluidos en las declaraciones aduaneras, así como también que los IMEIs de dichos equipos deben constar en las listas positivas de la ex-Superintendencia de Telecomunicaciones, actualmente ARCOTEL.

Al respecto, se observa que se ha aplicado este concepto fundamental de colaboración entre las autoridades aduaneras y de telecomunicaciones del país, no obstante, esta medida se ha hecho extensiva únicamente a las importaciones a consumo o masivas, sin embargo, para las importaciones unitarias que ingresan

[7] Comité de Comercio Exterior

por tráfico postal, fronteras terrestres, aéreas, puertos marítimos o courier no se ha dispuesto una medida similar que obligue a registrar los IMEIs en la autoridad aduanera de la nación.

Es preciso mencionar que el COMEX con Resolución No. 049 de 29 de diciembre de 2015, define cuotas globales para la importación de teléfonos celulares, así como que la persona natural que importe un teléfono celular nuevo por tráfico postal, fronteras terrestres, aéreas, puertos marítimos o Courier podrá poner a cargo de su cédula de identidad el teléfono celular que importe.

Revisando normativa a nivel internacional, se observa que el modelo de control de equipos móviles hurtados implementado por Turquía combina una colaboración entre las aduanas y la autoridad de telecomunicaciones de dicho país, realizando un registro de todos los equipos importados y un monitoreo de los eventos de tráfico generados en las redes de los prestadores del servicio móvil avanzado. De acuerdo a una publicación realizada por la Comisión de Regulación de las Comunicaciones de Colombia (CRC, 2015), durante los tres primeros años de su realización produjo una disminución del 90% en el problema del hurto de celulares. El modelo turco se muestra en la siguiente gráfica:

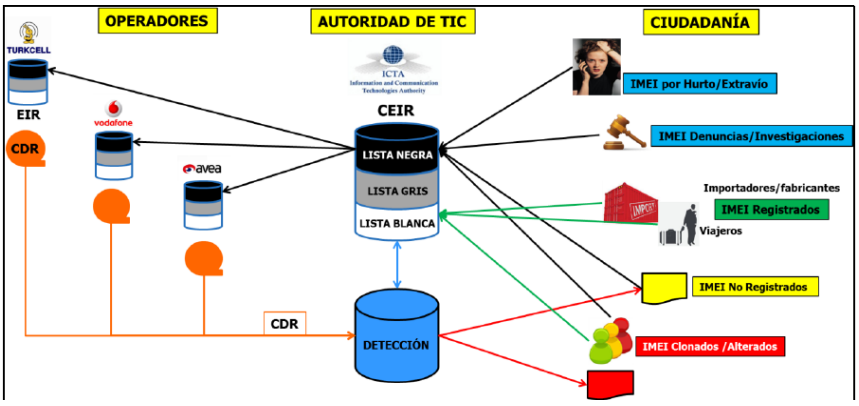

Figura 4. Modelo de Turquía para combatir el robo de celulares. (CRC, 2015)
Fuente: Comisión de Regulación de las Comunicaciones

En la figura se observa que el modelo turco se basa en una base centralizada a la que se conectan los prestadores del servicio móvil avanzado. Dicha base contiene tres partes: lista negra, lista gris y lista blanca.

Por otro lado, todos los prestadores del servicio móvil avanzado entregan sus registros de llamadas a la autoridad de telecomunicaciones de Turquía para que efectúe la detección de equipos no registrados, clonados y adulterados.

A dicha base de datos se conectan los importadores y las autoridades aduaneras, puesto que se registran los IMEIs de los equipos importados y también los IMEIs de los viajeros. Adicionalmente tienen conexión las entidades de justicia y la policía, con lo cual se observa que el modelo turco tiene una interacción entre varios organismos del estado, es decir cumple con la solución planteada por la UIT que establece que debe existir una estrecha relación entre las instituciones del estado para ayudar a contrarrestar este ilícito desde varios ámbitos, fortaleciendo el control. Es importante destacar esta colaboración interna que ha ayudado a disminuir notablemente este fenómeno.

e) **Información al usuario previo a tomar una acción correctiva. –** Se debe comunicar al usuario las acciones que se adoptarán al momento de detectar un dispositivo alterado, en cualquiera de los casos señalados: IMEI sin formato, IMEI no asignado e IMEI duplicado, IMEI adulterado con formato, así como adquirir este tipo de dispositivos en lugares de dudosa procedencia, sin factura o en la calle provoca que la delincuencia siga lucrando de esta actividad, así como que un equipo robado pudo haber provocado afectación a una persona o incluso la muerte.

   En ese sentido, es necesario efectuar una campaña previa, que muestre todas las implicaciones que surgen al adquirir un equipo robado. De igual forma se debe poner a disposición de la ciudadanía una aplicación que le permita consultar el estado del terminal que está yendo a comprar.

f) **Fortalecimiento de los marcos jurídicos y reglamentarios. –** Es necesario que las instituciones del estado fortalezcan su reglamentación, específicamente aquellas que tengan un rol de control e intervengan en este problema.

   Sobre este aspecto, el Código Orgánico Integral Penal del Ecuador en su Sección Novena, del artículo 191 al 194, establece varios delitos asociados contra la adulteración de terminales, como son la reprogramación, el reemplazo de sus etiquetas, el intercambio y la comercialización ilícita de los mismos.

El artículo 191 de dicho código sobre la reprogramación de terminales menciona que la persona que realice esta actividad tendrá una pena de 1 a 3 años de cárcel. (Asamblea Nacional, 2014). Para el resto de delitos señalados en los otros artículos se establece la misma pena.

Si bien este delito está penalizado, no se observa que los robos han disminuido, Ecuador dio un paso importante al colocar este tipo de ilícito en el Código Penal, sin embargo, es necesario adoptar acciones adicionales que mejoren esta situación, la estrecha colaboración entre la Fiscalía General del Estado (FGE) y la Policía Nacional, incluyendo también a las autoridades de regulación de las telecomunicaciones es fundamental para combatir este hecho. Se hace necesario acciones puntuales en conjunto para ejecutar pasos en firme que beneficien a la ciudadanía en general.

En un estudio realizado por Velásquez, Tovar, Vargas (2016) para la localidad de Florencia Caquetá (Colombia), se observaron varias estadísticas importantes relacionadas con el robo de celulares, la cuales se muestran a continuación:

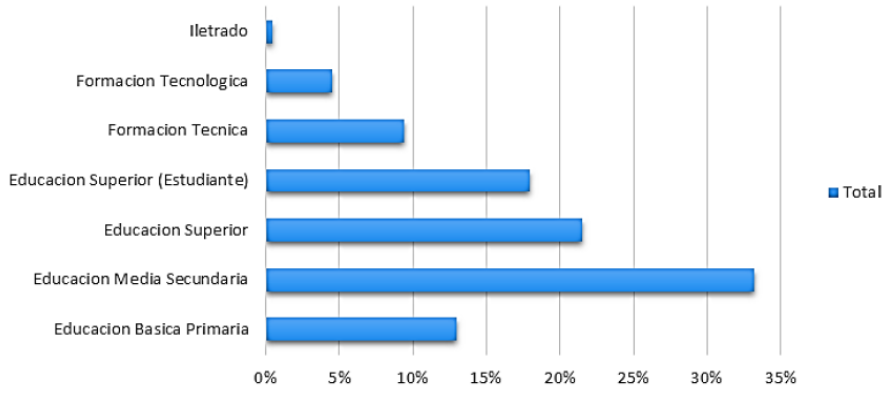

Figura 5. Nivel de educación de las víctimas de robo. (Velásquez, et al., 2016)

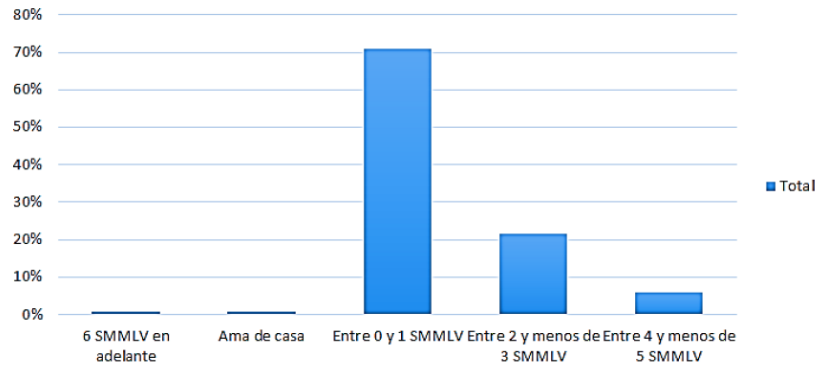

Figura 6. Ingresos mensuales de las víctimas de robo. (Velásquez, et al., 2016)

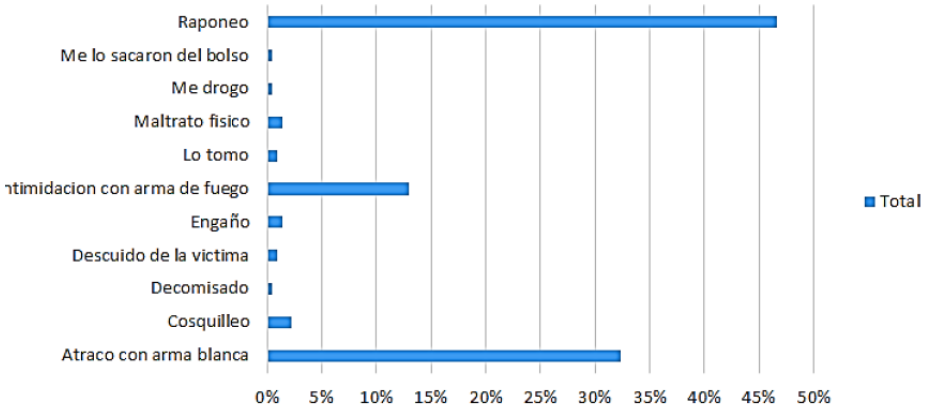

Figura 7. Forma en que se efectuó el robo. (Velásquez, et al., 2016)

En las figuras citadas se muestran datos importantes sobre este ilícito, se destaca que el grupo más afectado por robos en dicha localidad son los estudiantes secundarios, seguido de cerca por estudiantes universitarios, lo que revela que los ladrones lo que buscan es encontrar víctimas jóvenes que sean vulnerables y a los que les puedan quitar sus pertenencias.

Se observa también que las personas que tienen un rango de ingresos de hasta 1 salario mínimo mensual legal vigente (las de menor recursos económicos) son las más asaltadas por los malhechores, lo que evidencia que existe cierta preferencia para realizar este tipo de incidentes.

Por otro lado, se ha detectado que el raponazo es la modalidad preferida para el robo de equipos celulares, que consiste en arranchar los dispositivos y salir

corriendo del lugar. En tanto que en segundo lugar se encuentra el atraco con arma blanca.

De los hechos citados se determina que hay conductas que emplean las personas que ejecutan este tipo de daños, por lo que esta clase de estudios deberían ser utilizados y realizados por las autoridades de seguridad y vigilancia para tomar cartas en el asunto.

g) **Consideraciones previas. –** Se debe prever que al momento que se dispongan las medidas de control existen terminales inválidos que se encuentran operando en el mercado, por lo que una acción de control afectará considerablemente a las personas que cuenten con estos equipos y se deberá analizar alternativas transitorias que minimicen el impacto inicial.

3.1.3. Soluciones generales según la UIT.

La UIT (2019) establece tres aspectos principales para combatir el problema de equipos falsificados:

A. **Prohibir el uso de identificadores de dispositivos que no son válidos. –** Es necesario realizar el bloqueo de:
   - Equipos con identificadores inválidos.
     i. En este aspecto es fundamental bloquear los equipos que hayan sido reportados como robados.
   - Equipos no homologados.
   - Equipos que no hayan sido importados legalmente y controlar la venta ilícita de los mismos.

     Para esta tarea es fundamental que se cuente con una de datos centralizada.

B. **Vigilar el mercado y certificar los equipos. –** Contempla las medidas necesarias para restringir el uso o circulación de equipos que con cumplan los requisitos definidos en la normativa vigente, que incluye la prohibición, retiro y recuperación de los equipos. Es imprescindible la certificación de los equipos, puesto que este

proceso garantiza que se usen equipos que cumplan con los parámetros técnicos definidos a nivel nacional. En este aspecto cabe citar que el Reglamento de Homologación y Certificación de Equipos define a la homologación como un proceso técnico para evaluar y determinar si un terminal móvil es apto para funcionar en una red de telecomunicaciones del Ecuador (ARCOTEL, 2017), en consecuencia, constituye un proceso netamente técnico.

C. En el mismo documento normativo se precisa a los terminales del servicio móvil avanzado como una de las clases de equipos de telecomunicaciones que requieren homologación, es decir todo equipo que posea un IMEI y se conecte a las redes de los prestadores del SMA.

   Por otro lado, la Ley Orgánica de Telecomunicaciones establece algunas prohibiciones vinculadas con la homologación y comercialización de equipos que se citan a continuación:

   Prohibiciones:

   - Comercializar equipos que causen interferencias o interrupciones a las redes de telecomunicaciones del país, afecten la prestación de otros servicios de telecomunicaciones o puedan provocar afectación a usuarios. En cualquiera de los casos mencionados los terminales deben ocupar el espectro radioeléctrico.
   - Comercializar equipos que no estén debidamente homologados y usen el espectro radioeléctrico.
   - Comercializar equipos que no presenten compatibilidad con el Plan Nacional de Frecuencias.
   - Comercializar terminales que estén bloqueados y se encuentren impedidos de operar en las redes de telecomunicaciones móviles del país. (Asamblea Nacional, 2015)

   En este sentido se observa que la legislación ecuatoriana si ha expedido las normas relativas a la homologación de terminales que incluye una reglamentación propia con obligatoriedades, definiciones, prohibiciones, entre otros, que permiten efectuar una certificación de equipos y vigilar el mercado.

D. **Gestionar el ciclo de vida de los terminales. –** Se basa en el uso de identificadores únicos para los equipos con los cuales se pueda gestionar el ciclo de vida de los mismos, es decir la UIT recomienda que se debe controlar todas las etapas como son: origen, transporte y venta.

En resumen, la Unión Internacional de Telecomunicaciones (UIT, 2019) describe su modelo de referencia mediante el siguiente gráfico:

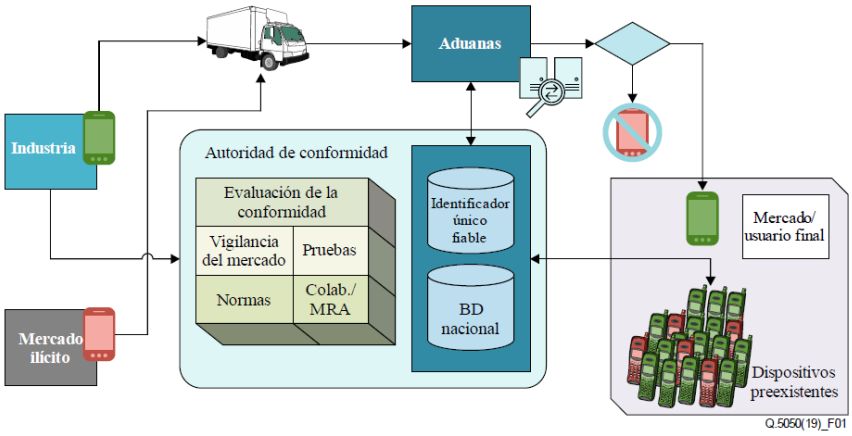

Figura 8.- Modelo de referencia expuesto por la Unión Internacional de Telecomunicaciones (UIT, 2019)

En el esquema mostrado convergen actores, actividades y las diferentes instituciones que intervienen en el control de este problema.

El mercado ilícito y los dispositivos preexistentes forman parte del ciclo de control.

3.1.4. Soluciones específicas para equipos móviles según la UIT.

En lo que respecta específicamente a equipos móviles la UIT describe soluciones que se basan en el IMEI de los equipos y menciona que las mismas tienen por objetivo bloquear equipos con números de IMEI que no son válidos (para este fin se puede tomar como referencia el TAC del terminal en función del listado de la GSMA), esto es: IMEIs con caracteres inválidos, IMEIs duplicados, IMEIs sin formato, etc, así mismo,

complementariamente indica que los países deben tomar medidas legislativas y actividades de sensibilización hacia el usuario.

La UIT (2019) cita 4 consideraciones específicas para equipos móviles:

1) **Base de datos única. –** Debe existir información completa, central, y constantemente actualizada que disponga de tres tipos de listas:
   - ❖ Lista blanca. – Base de equipos autorizados para operar en el país.
   - ❖ Lista gris. – Base de equipos que requieren de alguna regularización para pasar a formar parte de las listas positivas.
   - ❖ Lista negra. – Base de equipos rechazados y que no pueden operar en el país.

   En Ecuador la normativa establece dos tipos de listas: listas negativas y listas positivas. Por listas negativas se entiende todos los terminales robados, perdidos y hurtados, en tanto que las listas positivas comprenden una clasificación de equipos que están autorizados para realizar y recibir llamadas. En tal sentido, dentro de las soluciones que referencia la UIT, el Ecuador cuenta con una base centralizada cuya creación fue dispuesta a la ex-Superintendencia de Telecomunicaciones por el ex-CONATEL mediante Resolución TEL-878-30-CONATEL-2012. Es preciso señalar que dicha base no cuenta con listas grises, tal como lo señala la UIT, sin embargo, se definen claramente las listas positivas y negativas. Para las listas positivas, acorde a lo referido en la resolución citada, la base de datos contempla lo señalado por la UIT esto es, equipos importados y ensamblados en el país.

2) **Integrar la red del prestador del servicio móvil avanzado. –** Se debe tener un intercambio efectivo entre la base de datos de listas negativas y los registros que mantenga el prestador del servicio móvil avanzado en su plataforma, específicamente con su equipo EIR (Equipment Identity Register), a fin de que se pueda compartir la información entre ambos y se pueda mantener actualizadas las bse de datos de ambos actores.

   La UIT pone de manifiesto que cuando se conecta un teléfono por primera ocasión, el prestador del SMA debe capturar el IMEI y compararlo con la base de datos, a fin de verificar si está inscrito o no en listas blancas, caso contrario pasará

a listas grises y se le dará un plazo al usuario para que lo inscriba. Por otro lado, la UIT manifiesta que la base de datos debe compartirse con todos los actores, incluso con la población del país.

Al respecto, la normativa ecuatoriana señala que cuando un usuario reporte un equipo como robado, perdido o hurtado, el prestador del SMA debe suspender el servicio y bloquear el terminal y el sim card en un plazo de 30 minutos (ExConsejo Nacional de Telecomunicaciones, 2012). No se define el dispositivo de la red del prestador que efectúa el bloqueo, no obstante, esta tarea en el servicio móvil avanzado lo realiza el EIR.

La normativa de Ecuador define que los prestadores del SMA deben intercambiar en forma diaria con la ex-Superintendencia de Telecomunicaciones y entre ellos la información de sus listas negativas, en base a un esquema concreto instaurado por dicha entidad (Ex-Consejo Nacional de Telecomunicaciones, 2011). Sin embargo, no se precisa un mecanismo para la verificación referente a equipos que se conectan por primera ocasión en la red del prestador del servicio móvil avanzado.

La ARCOTEL ha puesto a consideración de la ciudadanía en general la página web: www.tucelularlegal.arcotel.gob.ec, en la cual se puede consultar en forma individual si un equipo se encuentra reportado como robado, perdido y hurtado, así como si está homologado. Adicionalmente se puede revisar información adicional como videos y preguntas frecuentes.

En las dos ilustraciones siguientes se visualiza las consultas en dicha página web:

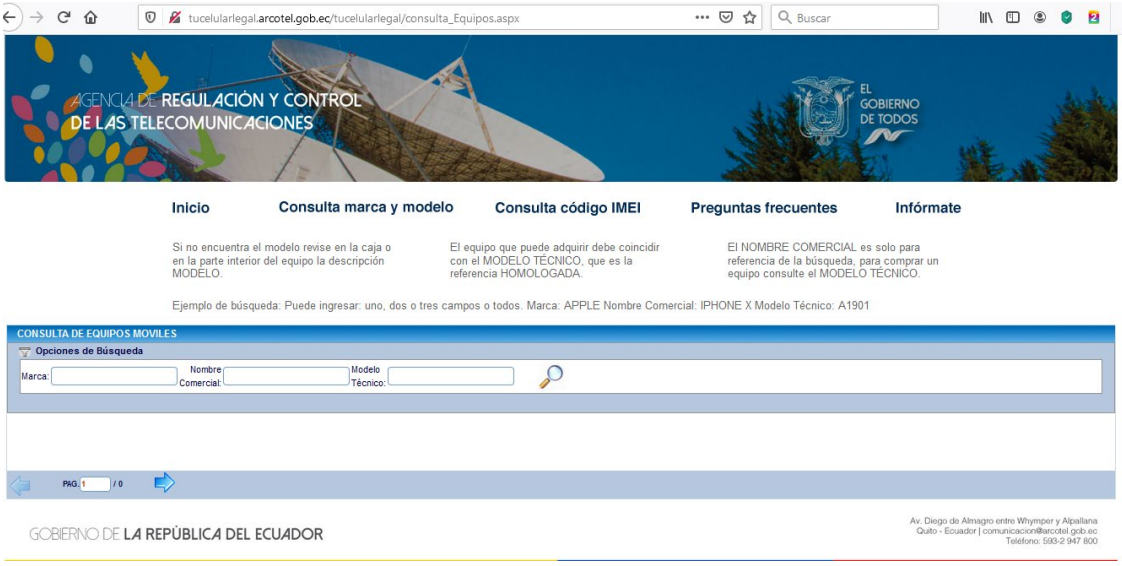

Figura 9. TUCELULARLEGAL Consulta por Marca y Modelo (ARCOTEL, 2020)

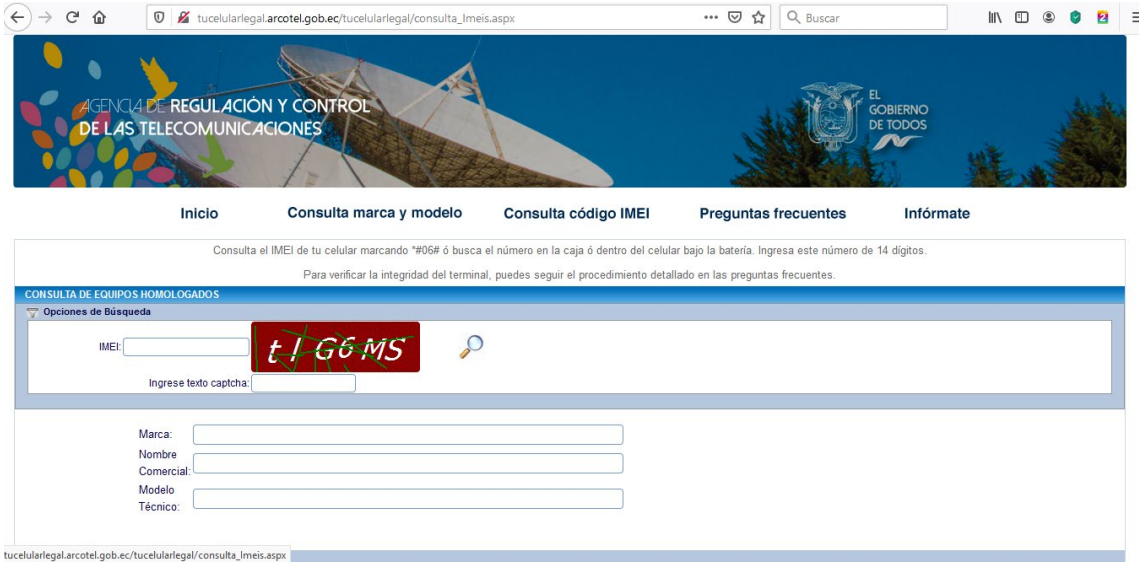

Figura 10. TUCELULARLEGAL Consulta por IMEI (ARCOTEL, 2020)

La página citada es un portal oficial de un autoridad nacional de telecomunicaciones del país y está disponible para consulta de toda la ciudadanía,

se pueden efectuar dos tipos de consultas e incluso se puede imprimir el resultado para los fines que tenga el usuario.

3) **IMEIs duplicados. –** Se indica que se debe crear una base con información adicional sobre el equipo que permita identificar otras propiedades del mismo.

   En la normativa ecuatoriana se expresa únicamente que se debe contemplar la identificación de duplicidad de IMEIs (ExConsejo Nacional de Telecomunicaciones, 2012), pero no se define la manera ni como se deben tratar estos casos.

4) **Otras consideraciones. –** También se recomienda lo siguiente:

   - ❖ Bloquear la importación de terminales que no cumpla la normativa nacional.
   - ❖ Colocar los terminales robados en la lista negra.
   - ❖ Bloquear los equipos no homologados.

   Sobre estos aspectos, como ya se analizó anteriormente la legislación ecuatoriana contempla las listas negras en la normativa de equipos robados, perdidos y hurtados y el control de equipos no homologados se encuentra señalado en la Ley Especial de Telecomunicaciones y su reglamento general y en forma específica en el Reglamento para Homologación de Equipos. Con relación a la importación de terminales en la normativa se cita el registro de terminales que ingresan al país, no obstante, no se menciona acciones contra los equipos que no hayan cumplido con este requisito.

Finalmente, la UIT menciona otras alternativas que contribuyen a mejorar este problema, entre las cuales se citan las siguientes:

- Base de datos de la GSMA
- DIRBS (Sistema de identificación, registro y bloqueo de equipos)
- Grupo Trusted Computing
- Plataforma Global
- JTC1/SC27 de la ISO/CEI

- Foro OTTF (Open Group Trusted Technology Forum)
- Instituto de Ingenieros Eléctricos y Electrónicos

3.2. RESOLUCIÓN 2935 (CITEL)

La Comisión Interamericana de las Telecomunicaciones (CITEL), organismo creado por la OEA[8] emitió la Resolución 2935 de 23 de julio de 2020 denominada “ESFUERZOS HEMISFÉRICOS PARA COMBATIR EL USO DE EQUIPOS TERMINALES MÓVILES HURTADOS, EXTRAVIADOS O ADULTERADOS”, la cual cita varios aspectos, destacándose (CITEL, 2020) los siguientes:

- Intercambio de equipos robados, perdidos y hurtados entre los estados miembros.
- Intercambio de experiencias exitosas en el combate del robo, hurto y pérdida de equipos entre los países miembros.
- Bloquear localmente los equipos duplicados y alterados.
- Fortalecer los marcos regulatorios y normativos para incrementar las sanciones y las acciones policiales contra el robo, hurto, pérdida, duplicación y adulteración de equipos del servicio móvil avanzado.

Se observa que el problema del robo y la alteración de los equipos es una práctica común en los países que son parte de esta entidad, lo que ha conllevado a la adopción de una resolución que contiene puntos importantes para tratar este ilícito.

Al igual que en el caso de la UIT, el documento expone que se debe fortalecer los marcos legislativos de cada país para condenar la adulteración de los equipos. Se declara la importancia del intercambio de equipos robados, perdidos y hurtados entre los países miembros con el objetivo de que al ser llevados a otras jurisdicciones no puedan ser activados y se contrarreste de alguna manera la salida de estos equipos hacia otros destinos.

[8] Organización de Estados Americanos

Con respecto al primer punto es necesario precisar que la CAN[9] emitió la Decisión 786 de 24 de abril de 2013 que establece la obligatoriedad de efectuar un intercambio de información entre todos sus países miembros respecto a los reportes de equipos que han sido denominados como robados, hurtados, perdidos y recuperados en la Comunidad Andina, lo cual incluye a Ecuador. Por lo que se evidencia que al momento existe una normativa internacional que obliga a los países de la CAN a realizar la transferencia de los IMEIs de los equipos que han sido reportados en sus respectivos países.

La Decisión de la CAN (2013) define los lineamientos bajo los cuales se debe realizar el intercambio de los reportes de robo, hurto y pérdida entre los países miembros de la CAN, bajo los siguientes principios:

- Los prestadores del servicio móvil avanzado de cada país miembro deben conectarse a la GSMA IMEI DB, que constituye una plataforma diseñada por la GSMA (Asociación GSM) para la carga y descarga de la información correspondiente a los equipos reportados como robados, perdidos y hurtados. La GSMA está conformada mayoritariamente por los concesionarios de servicios móviles de diferentes países y también por fabricantes, proveedores, compañías de software, entre otros.
- Los operadores móviles que se encuentran asociados a esta entidad son los que pueden realizar la carga y descarga de los reportes de robo, hurto y pérdida de sus abonados y usuarios, para lo cual deben establecer una conexión con la plataforma de dicha entidad.
- Con periodicidad diaria y en un plazo de 48 horas siguientes a la recepción del reporte de robo, hurto y pérdida los prestadores del servicio avanzado deben subir a la plataforma de la GSMA y bloquear en su red el IMEI del equipo reportado.
- En un plazo de hasta 48 horas posterior a que un IMEI haya sido puesto en la plataforma de la GSMA IMEI DB, el prestador del servicio móvil avanzado debe descargar esta información y proceder al bloquear el equipo en su red.
- Únicamente el prestador del servicio móvil avanzado que reportó un equipo como robado, perdido y hurtado es el que puede liberar el mismo. Dicha liberación se

[9] Comunidad Andina de Naciones

podrá efectuar hasta en un plazo de 48 horas desde que el IMEI fue colocado en la GSMA IMEI DB.

- Los formatos para la carga y descarga de la información son los que ha definido la GSMA. Los prestadores del servicio móvil avanzado deben cumplir con estos formatos.
- Se establece como datos a cargar en la plataforma los siguientes: IMEI, fecha de procesamiento, prestador del servicio móvil avanzado, tipo de reporte y tipo de acción.
- Los prestadores del servicio móvil avanzado deben instalar en su red el equipo EIR, dispositivo que permite realizar el bloqueo de los IMEIs de los terminales.

Con relación al bloqueo de equipos duplicados y adulterados tanto Colombia como Perú han adoptado en sus normativas el tratamiento de este tipo de equipos. El numeral 3.32 de la Resolución CRC 3128 establece que los prestadores del servicio móvil avanzado deben tener implementado un proceso de verificación para la detección de una diversidad de equipos irregulares entre los cuales se destacan IMEIs duplicados e IMEIs sin formato e inválidos. Para el caso de Perú, los artículos trece y veintiuno del Decreto Supremo No. 007-2019-IN definen acciones a efectuar para el caso de detectarse en operación IMEIs de equipos duplicados y alterados.

En lo que concierne a Ecuador la normativa menciona que la base de datos de listas positivas y negativas debe reconocer IMEIs duplicados, no obstante, no expresa el tratamiento que se debe dar a este tipo de casos. El Reglamento General a la LOT[10] en su artículo ciento catorce enuncia que la ARCOTEL tiene la facultad para implementar procedimientos para evitar que se usen equipos duplicados, adulterados, no homologados, entre otros. De lo que se desprende que con la expedición del mencionado reglamento la autoridad de telecomunicaciones de Ecuador tiene la potestad para emitir los procedimientos necesarios para controlar el problema de la duplicidad y la adulteración de terminales.

Es preciso recalcar que la resolución de la CITEL establece que se deben fortalecer los marcos regulatorios de los países, en ese sentido, tal como se ha analizado en párrafos

[10] Ley Orgánica de Telecomunicaciones

anteriores se observa que los vecinos Perú y Colombia han efectuado varias modificaciones a sus respectivos marcos regulatorios de listas positivas y negativas, en tanto que para Ecuador la última reforma puntual sobre este tema se dio en el año 2012 y con la emisión del Reglamento General a la LOT, específicamente el artículo ciento catorce se otorgaron en forma general facultades a la ARCOTEL para controlar equipos irregulares.

3.3. APLICACIONES INFORMÁTICAS CONTRA EL ROBO DE CELULARES

3.3.1. KILL SWITCH

La aplicación informática Kill Switch surgió como una alternativa moderna al robo de celulares, cuya intención es que el usuario que perdió su equipo o se ha visto afectado por la sustracción del mismo debido a la delincuencia común, pueda efectuar el bloqueo del dispositivo desde cualquier ubicación.

Al ser concebida como una solución tecnológica, este aplicativo tiene una finalidad bastante útil, puesto que el usuario únicamente debe usar la herramienta instalada en su dispositivo el momento que lo considere adecuado y emplearla para salvaguardar la información almacenada en su terminal.

Los fabricantes y desarrolladores de aplicaciones han dado un importante paso con el desarrollo de esta herramienta, considerada para mejorar los niveles de seguridad del usuario. Desde luego requiere que el usuario tome conocimiento del uso de la misma y la configure de manera que pueda ser utilizada en el momento adecuado.

La aplicación teóricamente debe permitir:

- Borrado remoto de los datos.
- Impedir el uso del dispositivo para usuarios no autorizados.
- Revertir el bloqueo en caso de que el usuario recupere el equipo.

En Estados Unidos en el año 2015 los estados de California y Minnesota adoptaron el Kill Switch como una alternativa para combatir el robo de los equipos móviles. De acuerdo al portal CNET, la normativa aprobada establecía que todos los equipos que sean

comercializados en California deben tener precargado una herramienta antirrobo que permita bloquear el equipo remotamente y de esta manera se pueda disuadir a los malhechores a no cometer este delito. En Minnesota en el mismo año también se aprobó una normativa similar con la diferencia que no era obligatorio que el software venga precargado en el sistema (CNET, 2015).

Previo a esta iniciativa, la instalación de este tipo de software trajo beneficios puesto que en Estados Unidos existió una reducción del robo de equipos de 3,1 millones a 2,1 millones del año 2013 al 2014 (Consumer Reports, 2015).

En el mismo reporte se indica que desde que APPLE instaló su aplicación Find My Iphone en el año 2013 y luego Activation Lock, se redujeron los índices de robo de dispositivos de esta marca.

En el año 2020 el Senado colombiano a través de la senadora Soledad Tamayo impulsó un proyecto de ley que permita al usuario que reportó el robo de su terminal, borrar remotamente la información del mismo y bloquearlo. Esta aplicación puede ser utilizada únicamente en los teléfonos inteligentes. Dicho proyecto de ley cita que todos los equipos que sean importados al país deben contar con la aplicación preinstalada por el fabricante, a fin de que el usuario pueda utilizarla para su beneficio (Congreso de la República de Colombia, 2020).

En Inglaterra el alcalde de Londres, tomó en cuenta lo sucedido en EEUU y solicitó a los fabricantes la instalación del Kill Switch en sus terminales (CRC, 2015).

En el Ecuador no se han verificado este tipo de iniciativas y se ha considerado únicamente el bloqueo de los terminales robados en la red del prestador del servicio móvil avanzado.

A pesar de este esfuerzo realizado por la industria, la aplicación presenta desventajas, por ejemplo, no puede ser utilizada si el celular está apagado o si ha sido configurado como modo avión.

Los principales fabricantes de teléfonos móviles han desarrollado aplicativos que han sido instalados en sus dispositivos, a fin de sumarse a esta iniciativa. Desde el año 2013 APPLE añadió a sus dispositivos el aplicativo FIND MY IPHONE que usa el Apple ID y la contraseña de usuario para el borrado y el reseteo del equipo.

SAMSUNG a su vez creó el aplicativo LOCALIZAR MI MÓVIL, el cual se encuentra instalado en sus terminales y permite ubicar y controlar el teléfono de forma remota, para lo cual el usuario debe acceder a su cuenta SAMSUNG y realizar tareas de control a distancia a través de la página web https://findmymobile.samsung.com.

3.3.2. OTRAS APLICACIONES.

Adicionalmente existe una cantidad de aplicaciones gratuitas y pagadas en las tiendas APPLE STORE y GOOGLE PLAY que permiten efectuar tareas de seguridad para el dispositivo. Por ejemplo, las siguientes aplicaciones encuentran disponibles para su descarga en forma gratuita en la tienda Google (GOOGLE PLAY, 2021):

- LOCKWARCH.- Es un software que toma una fotografía de manera secreta cuando una persona pretende desbloquear el equipo con un código inválido y luego la envía por correo electrónico incluyendo la ubicación GPS sin que el individuo que efectuó esta acción se entere.

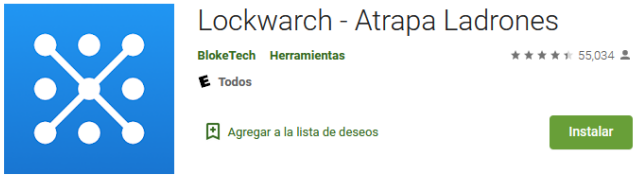

Figura 11.- Aplicación Lockwarch (GOOGLE PLAY, 2021)

- ENCONTRAR MI DISPOSITIVO DE GOOGLE.- Permite observar la ubicación del teléfono en un mapa, además que permite borrar y bloquear el dispositivo con un mensaje personalizado y un número de contacto.
- ENCONTRAR TELÉFONO PERDIDO: PROTECCIÓN ANTIRROBO.- aplicativo que tiene opciones interesantes como son:
    - Localizar teléfono aplaudiendo
    - Localizar teléfono perdido
    - No tocar el dispositivo

Figura 12.- Encontrar teléfono perdido: protección antirrobo (GOOGLE PLAY, 2021)

- CROOKCATCHER - SEGURIDAD.- Toma una foto secreta cuando alguien intenta desbloquear el teléfono sin acertar el patrón de seguridad del equipo. Estas fotos pueden ser almacenadas en el dispositivo o pueden ser enviadas por correo incluyendo la localización del equipo.

Figura 13.- CrookCatcher – Seguridad (GOOGLE PLAY, 2021)

- ALARMA ANTIRROBO.- Genera alarmas y sonidos, así como tiene una variedad de patrones de seguridad, incluyendo alarma cuando se desenchufa el cargador.
- SELFIE AL INTRUSO.- Toma una foto de la persona que ha intentado desbloquear el equipo sin autorización del dueño.

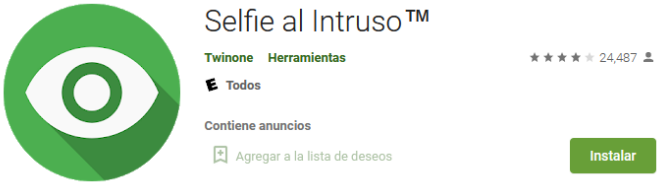

Figura 14.- Selfie al Intruso (GOOGLE PLAY, 2021)

Las aplicaciones citadas brindan al usuario una alternativa al momento de requerir tomar una acción frente al robo de su equipo celular.

CAPÍTULO IV

4. DESARROLLO DE UNA PROPUESTA QUE CONTRIBUYA A COMBATIR EL ROBO Y HURTO DE EQUIPOS CELULARES.

Como se ha mencionado en capítulos anteriores, el robo y hurto de equipos móviles es un problema que se da a nivel mundial y especialmente en América Latina, lo que ha conllevado a que cada país emita su respectiva legislación para tratar de combatir este ilícito. La Unión Internacional de Telecomunicaciones también ha expedido recomendaciones para su análisis y uso a nivel global.

En concordancia con la normativa analizada y lo emitido por la UIT, a continuación, se citan varias acciones que podrían contribuir y apoyar a contrarrestar el robo y hurto de equipos celulares.

4.1. Colaboración entre la Autoridad Aduanera y la Autoridad de Telecomunicaciones.

Uno de los requisitos marco que establece la Unión Internacional de Telecomunicaciones en la Recomendación UIT-T Rec.Q.5050 es la estrecha colaboración entre las autoridades aduaneras y los organismos nacionales competentes (UIT, 2019). En tal sentido, es fundamental que las instituciones del estado ecuatoriano coordinen acciones en bien de la ciudadanía y más aún para combatir el robo y hurto de equipos móviles.

Considerando que una de las vías principales de acceso al país de los equipos móviles constituye el ingreso por aeropuertos y fronteras terrestres, es necesario definir controles que permitan determinar si los equipos que llegan tienen alguna irregularidad, de manera que este tipo de acción se convierta en un control previo esencial desarrollado para impedir la utilización de estos equipos. Esta validación inicial tiene que efectuarse en coordinación entre la autoridad aduanera y la autoridad de telecomunicaciones del país, de forma que se pueda realizar una verificación preferentemente en línea de los equipos que ingresan por fronteras terrestres y aeropuertos contra la base de datos centralizada que mantiene la Agencia de Regulación y Control de las Telecomunicaciones.

Es preciso citar la siguiente normativa que apoya las actividades coordinadas entre instituciones del estado:

- El artículo 226 de la Constitución de la República menciona que las administraciones públicas pueden realizar sus acciones en forma coordinada con el objetivo de cumplir sus funciones en beneficio de la ciudadanía. (Asamblea Constituyente, 2008)

Los artículos 25 y 28 del COA[11] disponen:

- Las instituciones del estado ejecutarán sus competencias y atribuciones observando el bienestar común en beneficio de la ciudadanía.
- Las instituciones del estado podrán realizar sus acciones colaborando entre ellas de manera coordinada buscando ejecutar sus actividades de manera eficiente y ordenada.
- La forma en que las instituciones del estado efectivizarán sus mecanismos de colaboración será a través de procedimientos, convenios o instrumentos que celebren entre ellas. (Asamblea Nacional, 2017)

Por otro lado, la normativa expedida en lo que se refiere a telecomunicaciones también establece que los organismos del estado pueden ejecutar acciones coordinadas:

El artículo 114 del Reglamento General a la LOT define lo siguiente:

> ***"Art. 114**.- Control previo y posterior de terminales.- La ARCOTEL establecerá los procedimientos de control, manuales o automáticos, para asegurar que los terminales cumplan con el procedimiento de homologación y obtención de la certificación respectiva. Para el efecto, tendrá la facultad de implementar mecanismos de forma individual o de forma conjunta con instituciones públicas y privadas, nacionales e internacionales para evitar que se usen u operen terminales duplicados, adulterados, no homologados, robados y los demás que la ARCOTEL defina para el cumplimiento del presente artículo."* (Presidencia de la República, 2015, p. 33)

[11] Código Orgánico Administrativo

En las partes subrayadas se resalta la regulación que faculta la coordinación de actividades entre las instituciones del estado en beneficio de la ciudadanía. Es por esto, que se hace necesario un apoyo entre las autoridades de telecomunicaciones y aduanas, considerando que es primordial efectuar un control previo de terminales.

De acuerdo a lo revisado se ha verificado que no existe un convenio o instrumento entre ambas instituciones que permita efectuar un registro coordinado de los equipos que ingresan por fronteras terrestres y aeropuertos como efectos personales del viajero. Sobre este aspecto, es preciso resaltar que la normativa emitida por la autoridad aduanera del país establece lo siguiente para efectos personales de viajeros:

- Acceso por aeropuertos internacionales: Todo pasajero que ingrese al país por esta vía podrá ingresar un equipo celular nuevo y un usado. En caso de grupos familiares también se puede ingresar una unidad nueva por el grupo y una usada por cada uno de sus miembros (SENAE, 2017).
- Acceso por frontera terrestre: Todo viajero puede ingresar únicamente un equipo celular usado (SENAE, 2019).

A más de lo indicado, el SENAE[12] también define que una persona natural puede importar hasta un teléfono celular por año fiscal y con cargo a su cédula de ciudadanía a través de tráfico postal o courier, pasos fronterizos terrestres, salas de arribo internacional y puertos marítimos, es decir, con el correspondiente pago de tributos (Comité de Comercio Exterior, 2015).

Considerando las vías de acceso señaladas, es necesario establecer un control de ingreso de este tipo de mercancía, el cual podría efectuarse colocando puestos de registro en:

- Puntos específicos fijados por la autoridad ecuatoriana de aduanas a nivel nacional.
- Lugares o establecimientos dispuestos por la autoridad de telecomunicaciones a nivel nacional.

[12] Servicio Nacional de Aduanas del Ecuador

También se puede analizar la opción de que esta tarea sea efectuada por un tercero, que efectúe el registro en los puntos específicos que señalen las autoridades nacionales. Con esto se lograría tener un control puntual para esta actividad.

De esta manera, todo equipo que ingrese por las vías de acceso legales al país será registrado en la base de datos centralizada que mantiene la autoridad de telecomunicaciones y con ello se tendrá una base sólida con información actualizada que permita hacer verificaciones.

En los puntos en donde se efectúe el registro se debe contar con una aplicación que tenga conexión directa con la base de datos centralizada que maneja la autoridad de telecomunicaciones, con el fin de validar que los equipos cumplan con las siguientes condiciones:

- El equipo se encuentre homologado.
- El equipo no conste en listas negativas.
- El IMEI cumpla con el algoritmo de Luhn.
- El equipo no se encuentre registrado previamente.

A más de las condiciones señaladas, también se debe cumplir con la normativa aduanera, esto es:

- Pago de tributos, en caso de que el importe de equipos no esté dentro del límite establecido como efectos personales del viajero.
- Importación de hasta un teléfono celular por año fiscal y con cargo a la cédula de ciudadanía del individuo que ingrese el terminal, a través de tráfico postal o courier, pasos fronterizos terrestres, salas de arribo internacional y puertos marítimos.
- Los demás que establezca el SENAE.

Únicamente cuando el terminal cumpla con todos los requisitos señalados, tanto a nivel de telecomunicaciones como a nivel de aduanas, podrá registrase en la base de datos centralizada.

Previo a realizar estas acciones, se considera esencial la celebración de un convenio entre las autoridades de telecomunicaciones y de aduanas del país o a su vez la expedición de normativas o instrumentos que permitan la ejecución de acciones conjuntas

entre ambas instituciones, en donde consten los mecanismos de registro de equipos que ingresan por tráfico postal o courier, pasos fronterizos terrestres, salas de arribo internacional y puertos marítimos.

La labor de registro de equipos es una actividad fundamental para el control de equipos adulterados y por otro lado, aporta con la supervisión y pago de tributos de los equipos que ingresan al país desde el exterior.

4.2. Colaboración entre las Autoridades de Seguridad y Vigilancia Nacional y la Autoridad Nacional de Telecomunicaciones.

El Código Orgánico Integral Penal del Ecuador define varios delitos asociados contra la adulteración de terminales entre los artículos 191 al 194, específicamente la reprogramación de terminales, el reemplazo de las etiquetas, el intercambio y la comercialización ilícita de terminales, en todos con una pena de uno a tres años para la persona que realice estas irregularidades (Asamblea Nacional, 2014).

No obstante, para que se puede configurar estos delitos, específicamente los dos primeros, es necesario demostrar que la persona aprehendida fue la que efectuó el ilícito o detenerla en flagrancia.

A pesar de que se ha dado un paso importante al penalizar este tipo de delitos, no se ha observado un decremento de los robos de celulares. Actualmente el reporte de robo, pérdida y hurto de equipos lo efectúan los usuarios notificando el hecho al prestador del servicio móvil avanzado en el cual tienen en uso su línea telefónica. Cabe señalar que en la normativa vigente de telecomunicaciones no se ha determinado como obligación realizar la denuncia ante la Fiscalía General del Estado, sino más bien como un hecho independiente y que no constituye un requisito para el bloqueo del terminal (Ex-Consejo Nacional de Telecomunicaciones, 2012). Es por esta razón que muchos de los robos de equipos se reportan al prestador de telecomunicaciones, pero no son denunciados ante la Fiscalía General del Estado.

La Policía Judicial de acuerdo a un reporte publicado en Diario El Comercio registró entre enero y octubre de 2018 un total de 3.712 denuncias por robo de teléfonos celulares, lo

que representa apenas un 1,2% con respecto al promedio de reportes de robo efectuados en el mismo lapso ante los prestadores del servicio móvil avanzado (El Comercio, 2018). Es decir, se evidencia que existe una notoria diferencia con la cantidad de reportes que mantiene la ARCOTEL en sus registros, lo que demuestra la baja concurrencia de los abonados afectados por el robo de su terminal ante las autoridades de supervisión y vigilancia.

Así mismo, se indica que las bandas delictivas dedicadas a este ilícito tienen una logística bien estructurada, conformada por un cabecilla, un responsable de escoger las víctimas, personal que efectúa el asalto con armas de distinto tipo y personas encargadas del escape y huida del sitio. Los lugares preferidos por los asaltantes son principalmente: paradas del transporte público, buses, alrededores de los centros de educación superior y discotecas. El horario en el cual se han producido la mayor cantidad de atracos es de 18:00 a 20:00 (El Comercio, 2018).

En la misma publicación se menciona que los celulares robados son llevados a talleres clandestinos en donde se resetea el equipo para posteriormente comercializarlo en otras provincias e incluso afuera del país. Adicionalmente el equipo puede ser desmantelado para vender sus partes como repuestos.

Según investigación de la Policía Judicial de Pichincha el desbloqueo de los equipos robados es realizado con “cámaras flashadoras”. Después cambian los IMEIs con códigos traídos de otros países (El Comercio, 2016). La Interpol ha señalado en sus informes que países como Bolivia, Perú, Colombia, Chile y Ecuador son mercados utilizados por estas mafias. Este ilícito mueve alrededor de 1,2 millones al día en la región (El Comercio, 2016).

En la ciudad capital en cinco sectores se han detectado que existen alrededor de 10 locales que ofrecen el desbloqueo de los celulares por un valor que oscila entre 40 y 120 dólares. Para realizar este trabajo se necesita de 24 horas (El Comercio, 2016).

En operativos realizados por la Policía Nacional en Quito se han detenido a sospechosos que tenían en su poder equipos reportados como robados en Ecuador, Colombia y Perú, y se procedió a la incautación de los celulares. El Ministerio del Interior citó que esta actividad de control se efectuó debido a denuncias de que en dichos sectores se comete el presunto delito de receptación (El Comercio, 2016).

En otra publicación de Diario El Comercio se señala que la adulteración de la identidad de los celulares se realiza especialmente en las ciudades de Quito, Guayaquil, Tulcán e Ibarra. Personal de la Policía Judicial menciona que en el país no solo existe gente que se ha capacitado en Internet para efectuar esta alteración, sino que también llegó personal de afuera para vender aplicaciones que cuestan alrededor de 600 USD (El Comercio, 2019).

En Colombia, Rojas (2016) menciona que la Policía de dicho país ha caracterizado este fenómeno y lo visualiza de la siguiente manera:

Figura 15.- Ciclo del hurto de celulares (Rojas, 2016)

Según Rojas (2016) el castigo a esta conducta criminal impone sanciones que van de 3 a 8 años de cárcel, sin embargo, si los detenidos admiten su culpa, el régimen sancionatorio de dicho país, les permite disminuir la pena incluso sin privación de la libertad. Por esta razón muchas de estas personas retoman sus actividades ilícitas pero ocultan o disminuyen su perfil con otras actividades, con el objetivo de que no sean capturados nuevamente, lo que complica en cierta manera, las actividades de las autoridades de vigilancia. (Rojas, 2016)

Por tal circunstancia, menciona que la extinción de dominio se ha constituido, junto con otras estrategias operativas, en una herramienta novedosa contra el combate al comercio de celulares robados, que ha impactado en la ciudad de Bogotá y que su aplicación constituye un elemento que aporta en la lucha contra este ilícito (Rojas, 2016).

Nicol, Garreton y Schodt (2018) citan que:

- En el 2013, el Fiscal General de California acusó a dos personas de tráfico de casi USD 4 millones en celulares a Hong Kong, un centro internacional para teléfonos robados, junto con Dubai y que se han encontrado teléfonos robados de Estados Unidos en todos los continentes excepto en la Antártida.
- Según la Interpol las organizaciones de robo de celulares que se mueven por América Latina gana un promedio de USD 550.000 por día. Muchos de estos traficantes están conectados a cárteles de la droga que invierten en el contrabando de celulares dado que lo consideran de bajo riesgo y alta recompensa en comparación con los narcóticos.

Considerando los aspectos analizados, en Ecuador urge una colaboración entre las autoridades de seguridad y de telecomunicaciones que contribuya a combatir este problema y que permita adoptar medidas en beneficio de la ciudadanía. Para este efecto se plantean las siguientes acciones:

- Crear unidades especializadas en la Policía y la Fiscalía General del Estado que se dediquen a procesar los reportes de robo de los equipos móviles y a su vez generen las respectivas tareas de control dentro de su ámbito, situación que permitirá focalizar, dar seguimiento y tratar de forma especializada este tipo de robos.
- Complementar la normativa señalada en el COIP o a su vez generar una reforma, en función de la experiencia que han recabado las entidades de seguridad y vigilancia en todos sus controles y operativos realizados hasta la fecha. Si bien el COIP contiene varias tipificaciones, al momento se han detectado aplicaciones que permiten la adulteración de equipos y que se encuentran en Internet, lo que complica los controles y operativos que efectúan las autoridades. Así mismo, el robo de terminales se va modernizando constantemente, por lo que es necesario ir a la par para contrarrestar su avance.

- Remitir a las instituciones de seguridad y vigilancia del país (Policía Nacional, Fiscalía General del Estado, Policía Judicial, entre otros) todos los reportes de robo, hurto y pérdida de equipos móviles que son centralizados en la base de datos que posee la ARCOTEL, con el fin de que dichas entidades cuenten con los insumos necesarios que les permita mejorar sus tareas de control. Este hecho es necesario, considerando principalmente que existe una cantidad baja de robos de celulares denunciados ante las autoridades de vigilancia y seguridad del país, lo que dificulta sus acciones.

  Esta acción puede ejecutarse en línea o en forma posterior, de acuerdo a la necesidad de las autoridades, no obstante, debe contener todos los datos que sean requeridos para tomar acciones concretas.

  De igual forma si este hecho requiere un cambio a la normativa de telecomunicaciones vigente, se debe ejecutar las reformas necesarias especialmente en la norma referente a listas positivas y negativas que es la que contiene la regulación específica al respecto.
- En la página web de la ARCOTEL www.tucelularlegal.arcotel.gob.ec se visualiza los campos IMEI, fecha del reporte de robo, prestador que realizó el reporte y si el equipo está homologado o no. Al respecto, se propone ampliar los campos y adicionar la ciudad o localidad donde se efectuó el robo, de forma que contribuyan a dar un tratamiento más extenso de estos casos y se pueda focalizar el control en las ciudades en las cuales se detecten la mayor cantidad de robos o hurtos.

4.3. Detección de terminales irregulares a través de CDRs y generación de procesos de regularización.

En la normativa nacional referente al robo, hurto y pérdida de equipos celulares, no se observan procesos y disposiciones puntuales en contra de los terminales irregulares denominados como inválidos, duplicados y no registrados. De lo revisado en las regulaciones emitidas por Perú y Colombia, ambas establecen medidas y acciones a efectuar para este tipo de equipos, situación que debe considerarse de manera especial, puesto que, al tener dos países limítrofes con medidas para combatir estas irregularidades, Ecuador podría convertirse en un lugar donde se envíen y se concentren

los terminales que han sido bloqueados en los países vecinos. Es por esta razón que urge la toma de acciones para contrarrestar este tipo de equipos.

De acuerdo al análisis realizado a las regulaciones internacionales y verificando la parte técnica, es factible la utilización de los CDRs[13] de voz y datos para verificar los equipos que cursan llamadas y determinar si estos corresponden a equipos irregulares, esto es: duplicados, no registrados e inválidos. Es importante considerar que este tipo de formato contiene información abundante tanto en cantidad como en campos, por lo que es necesario discernir únicamente los datos de valor.

Un CDR es un formato de recopilación sobre un evento tasable en la red de un prestador del servicio móvil, que contiene: hora de establecimiento de la llamada, cantidad de datos transferidos, IMEI, IMSI, entre otros, para su utilización en facturación y tarifación (Instituto Europeo de Normas de Telecomunicaciones [ETSI[14]] ,2019).

De toda esta información se considera necesario los siguientes campos:

Tabla 4. Campos del CDR

ÍTEM	CAMPO DEL CDR
1	Hora de establecimiento de la llamada
2	Fecha de establecimiento de la llamada
3	Hora de fin de la llamada
4	Fecha de fin de la llamada
5	IMEI
6	IMSI
7	Tipo de llamada: ❖ Origen

[13] CDR: Charging Data Records
[14] ETSI: European Telecommunications Standards Institute

ÍTEM	CAMPO DEL CDR
	❖ Terminación

Fuente: Creación propia, 2021

Es preciso indicar que los CDRs se generan tanto en llamadas de voz, mensajes de texto y llamadas de datos, por lo que se debe discriminar la información a obtener, así como escoger la que se utilizará para los fines de control.

La información a obtener debe ser periódica, al igual que los controles a efectuar, puesto que la detección de este tipo de terminales debe ser constante.

Por otro lado, tal como lo expone el principal organismo mundial de telecomunicaciones en su recomendación UIT Q.5050, es necesario que exista una adecuada información al usuario previo a cualquier acción correctiva o preventiva (UIT, 2019). El control a efectuar puede provocar el bloqueo del equipo, por lo que es necesario ejecutar campañas con la debida antelación a los usuarios, tanto por las autoridades locales como por los prestadores del servicio móvil avanzado. La campaña debe enfocarse en tres aspectos:

- Adquisición legal de los equipos por parte de los usuarios.
- Formas de regularizar su terminal en caso haya sido detectado como irregular por parte de la autoridad de telecomunicaciones.
- Acciones a efectuarse si el usuario no regulariza su terminal en los plazos otorgados por la autoridad de telecomunicaciones.

Es fundamental recalcarle al usuario que debe adquirir legalmente su equipo y debe ser consciente de las acciones que pueden ocurrir si utiliza un terminal irregular.

4.3.1. Control de equipos no registrados.

Los equipos no registrados son aquellos que no constan en las listas positivas de la autoridad de telecomunicaciones y constituyen los siguientes casos:

- Equipos ingresados por viajeros que no han sido debidamente registrados en las listas positivas.
- Equipos adulterados.
- Equipos ingresados por contrabando.

Para detectar este tipo de equipos se pueden utilizar los CDRs que disponen los prestadores del servicio móvil avanzado y realizar la comparación respectiva con la base de datos de listas positivas de la autoridad de telecomunicaciones.

Para esto se requiere que los CDRs cumplan con los siguientes requisitos:

Tabla 5. Información de CDRs para detección de equipos no registrados

ÍTEM	NOMBRE	DESCRIPCIÓN
1	Periodicidad	DIARIA o la que la autoridad de telecomunicación defina.
2	Información	Todos los registros CDRs de los prestadores del servicio móvil avanzado MOVISTAR, CLARO, CNT EP.
3	Tipo	Voz y datos

Fuente: Creación propia, 2021

Una vez que se realice esta tarea se requiere que:

- Los prestadores del servicio móvil avanzado notifiquen a través de mensajes a los usuarios que se encuentran utilizando un equipo que no está registrado en el país y por tanto deben acercarse a regularizar su terminal.
- El plazo para que el usuario efectúe esta actividad vendrá dado por disposición de la autoridad de telecomunicaciones del país.
- Además, el prestador del servicio móvil avanzado le debe comunicar al abonado que en caso de que no realice la regularización del equipo en el plazo señalado, se procederá a ingresar el terminal en listas negativas y se bloqueará el mismo.
- El usuario puede registrar su equipo durante el plazo brindado para realizar la regularización del mismo. También lo puede ejecutar en forma posterior, pero el equipo ya se encontrará bloqueado.
- El registro se podrá realizar para viajeros que hayan ingresado por frontera terrestre/sala de arribo/paso marítimo o a través de courier únicamente cuando se cumpla con las condiciones que se describen a continuación:
    - El equipo se encuentre homologado.
    - El IMEI del equipo cumpla con el algoritmo de Luhn.

- El equipo haya cumplido con todos los requisitos y normas aduaneras de internación lícita al país.

4.3.2. Control de equipos duplicados.

Los equipos duplicados son aquellos que tienen un IMEI repetido, debido a una adulteración provocada en le terminal por un agente externo.

Para detectar este tipo de equipos se deben utilizar los CDRs que disponen los prestadores del servicio móvil avanzado y realizar una revisión para detectar llamadas realizadas que:

a) Coincidan o se traslapen en tiempo (simultaneidad de llamadas); o,

b) Que se realicen a una distancia que no sea posible efectuar un cambio de sim card (conflicto distancia-tiempo).

Para esto se requiere que los CDRs cumplan con los siguientes requisitos:

Tabla 6. Información de CDRs para detección de equipos no registrados

ÍTEM	NOMBRE	DESCRIPCIÓN
1	Periodicidad	DIARIA o la que la autoridad de telecomunicación defina.
2	Información	Todos los registros CDRs de los prestadores del servicio móvil avanzado MOVISTAR, CLARO, CNT EP.
3	Tipo	Voz y datos

Fuente: Creación propia, 2021

En este tipo de detección es necesario manejar la dupleta IMEI-IMSI, por lo que se debe obtener el IMSI de manera obligatoria y adicionalmente para este caso particular se debe extraer de los CDRs la información referente a la identificación del sector de inicio y fin de la llamada, datos fundamentales para poder realizar una detección adecuada.

Ejecutada esta tarea se requiere que:

- Los prestadores del servicio móvil avanzado notifiquen a través de mensajes a los usuarios que se encuentran utilizando un equipo que ha sido detectado como duplicado y por tanto deben acercarse a regularizar su terminal.
- El plazo para que el usuario efectúe esta actividad vendrá dado por disposición de la autoridad de telecomunicaciones del país.
- Además, el prestador del servicio móvil avanzado le debe comunicar al cliente que en caso de que no realice la regularización del equipo en el plazo señalado, se procederá a ingresar el terminal en listas negativas y se bloqueará el mismo.
- El usuario puede regularizar su equipo durante el plazo brindado. También lo puede realizar en forma posterior, pero el equipo ya se encontrará bloqueado.

Finalmente, de todos los usuarios que han sido notificados como equipos duplicados, se debe verificar quien ha regularizado su terminal, a fin de colocar la dupleta IMEI-IMSI en las listas blancas del EIR del prestador del servicio móvil avanzado, y constituirá el equipo que podrá operar en la red, el resto de dupletas IMEI-IMSI serán ingresadas en listas negativas en el EIR de los otros prestadores del servicio móvil avanzado.

4.3.3. Control de equipos inválidos.

Los equipos inválidos son aquellos que tienen un IMEI con una cantidad de dígitos diferente a 15 o que contienen dígitos no numéricos en su estructura. Al igual que para los casos anteriores, se hace imprescindible el uso de CDRs para su detección y supervisión.

Para esto se requiere que los CDRs cumplan con los siguientes requisitos:

Tabla 7. Información de CDRs para detección de equipos no registrados

ÍTEM	NOMBRE	DESCRIPCIÓN
1	Periodicidad	DIARIA o la que la autoridad de telecomunicación defina.
2	Información	Todos los registros CDRs de los prestadores del servicio móvil avanzado MOVISTAR, CLARO, CNT EP.

3	Tipo	Voz y datos

Fuente: Creación propia, 2021

Ejecutada esta tarea se requiere que:

- Los prestadores del servicio móvil avanzado notifiquen a través de mensajes a los usuarios que se encuentran utilizando un equipo cuyo código de identificación (IMEI) no es válido y por tanto debe cambiar de terminal puesto que será bloqueado.
- El plazo para que el usuario efectúe esta actividad vendrá dado por disposición de la autoridad de telecomunicaciones del país.
- En caso de que el usuario solicite una explicación sobre el tipo de equipo que está usando se le deberá informar adecuadamente sobre las particularidades que posee su equipo.

Cumplido el plazo señalado, la autoridad nacional de telecomunicaciones deberá proceder a ingresar el equipo en listas negativas y los prestadores del servicio móvil avanzado deberán bloquearlo en su red.

4.4. Acciones adicionales.

A más de las acciones señaladas, se plantean varias que contribuirán a combatir el problema del robo de celulares:

4.4.1. Difusión de campañas para reportar el robo de equipos móviles.

La Unión Internacional de Telecomunicaciones recomienda una adecuada difusión a los usuarios previo a cualquier acción preventiva y correctiva a tomar por parte de las autoridades (UIT, 2019). Es por ello que se considera necesario ampliar la difusión a la ciudadanía sobre la forma de reportar un robo, hurto o pérdida de un equipo celular, principalmente porque este aspecto corresponde a un hecho que sucede recurrentemente y que puede pasarle a cualquier persona, por lo que es primordial que

los abonados conozcan de forma clara y precisa las acciones a efectuar el momento que les suceda el robo de su equipo.

En la página web de la ARCOTEL www.tucelularlegal.arcotel.gob.ec en la sección preguntas frecuentes[15] se encuentra cierta información sobre como reportar un equipo robado, perdido y hurtado. También se ha revisado que dicha institución ha realizado la difusión sobre el robo de equipos celulares en sus redes sociales, no obstante, se considera esencial incrementar la difusión hacia los usuarios, desde muchos otros ámbitos, como son:

- Campañas en medios de radio y televisión abierta.
- Colocar en las páginas web de los prestadores del servicio móvil avanzado el procedimiento detallado que cada usuario debe seguir para reportar el robo de su equipo y que contenga, entre otros aspectos:
    - Medios de reporte: call center, centro de atención al usuario, página web, etc.
    - Horarios de reporte.
    - Números para atención de reportes de robo, hurto y pérdida en caso de hacer uso de un call center, así como dirección de página web, si se lo puede efectuar vía Internet.
    - Datos que el usuario debe proporcionar al momento de efectuar el reporte.
    - Preguntas frecuentes.

Esta información es fundamental que sea correctamente entregada y que el usuario la tenga clara y a primera mano, en caso de que sea víctima de un asalto o pierda su celular. Es necesario también la contribución de otras instituciones privas y públicas en la difusión de acciones que son de su competencia, como son:

- Policía Nacional. – Campañas en medios públicos y redes sociales sobre normas de prevención, aspectos a tomar en cuenta antes y después de un robo.

[15] http://tucelularlegal.arcotel.gob.ec/tucelularlegal/preguntas_frecuentes.aspx

- Fiscalía General del Estado. – Campañas en medios públicos y redes sociales. En este punto es necesario recalcar al usuario la importancia de efectuar en la Fiscalía General del Estado la denuncia por el hecho sucedido, a fin de que se pueda ejecutar el seguimiento pertinente.
- Prestadores del servicio móvil avanzado. – Difusión en sus redes sociales sobre los requisitos y la forma de reportar un robo de un celular.

4.4.2. Considerar y emplear la base de datos de la GSMA.

La GSMA es una asociación internacional que agrupa a varias entidades y mantiene una base de datos a nivel global alimentada por los reportes de robo que cargan los diferentes prestadores del servicio móvil avanzado del mundo. En este sentido, la base citada es de vital importancia para los controles que se deseen realizar para combatir este ilícito, considerando principalmente que uno de los objetivos de los celulares robados es llevarlos a otros países donde son comercializados en el mercado negro, convirtiéndose en un negocio rentable para las personas que cometen este delito.

Por esta razón la base de datos de la GSMA se convierte en una herramienta a ser utilizada por las autoridades locales para ayudar a detectar el ingreso de equipos de otros países.

A más de mantener esta base de datos, la GSMA ofrece varios servicios como son:

- Inteligencia GSMA
- Servicios eSIM
- Servicios IMEI
- Intercambio de configuraciones de red
- GSMA PathFinder
- GSMA DNS
- Asignación de TACs

Dentro de los servicios IMEI, la GSMA ha diseñado una aplicación de consulta a su base de datos de listas negativas denominada GSMA DEVICE CHECK para ser usada por diversas instituciones como son: aseguradoras de equipos móviles, recicladores de dispositivos, minoristas de equipos y entidades gubernamentales.

Las autoridades de telecomunicaciones y especialmente las de seguridad y vigilancia de país como por ejemplo la Policía Nacional pueden hacer uso de esta información en sus operativos de control, así como en sus actividades puntuales de vigilancia.

Para utilizar este servicio se requiere el IMEI del equipo. Los datos que se pueden obtener al ingresar este parámetro son:

- Estado del IMEI en la base de datos
- Prestador del servicio móvil avanzado que realizó el reporte.
- Fecha del reporte

Con esta información las autoridades de vigilancia y seguridad pueden ampliar sus tareas de seguimiento e inteligencia y verificar de que países están ingresando los dispositivos robados, situación que es de vital importancia para aportar al combate del hurto de equipos. Además, esta validación puede ser realizada también por otras entidades del estado como son las aduanas, para complementar sus labores de supervisión respecto a los equipos que se internan al país, así como la propia autoridad de telecomunicaciones del país, quien dispondría de consultas directas con la base mundial de equipos robados, perdidos y hurtados y de esta manera puede complementar sus actividades y planificar de ser el caso controles adicionales, como por ejemplo, el bloqueo de equipos que ingresan de determinados países del mundo.

Para el empleo de este aplicativo se debe efectuar un requerimiento puntual a la GSMA, a fin de que se otorgue el acceso pertinente.

4.4.3. Uso de la aplicación Kill Switch.

Considerando que actualmente existe una proliferación de los teléfonos móviles inteligentes o smartphones es necesario utilizar las prestaciones que brinda esta tecnología. Los mayores fabricantes de esta clase de dispositivos han diseñado aplicaciones propias instaladas en el teléfono que pueden ser empleadas por los usuarios para protegerse ante el robo de su equipo.

Por otro lado, en la plataforma de aplicaciones de ANDROID denominada Play Store también se encuentran muchos programas gratuitos cuyo objetivo es proteger el dispositivo ante un robo y que pueden ser de mucha ayuda para los usuarios.

El uso de este tipo de herramientas constituye una solución complementaria a las acciones que implementen las autoridades nacionales, y que estaría al alcance directo de los usuarios, siempre y cuando mantengan instalada la aplicación en su dispositivo móvil.

En ciudades de varios países, como por ejemplo, en California Estados Unidos se aprobaron leyes que obligan a los productores de teléfonos celulares a instalar por defecto en su sistema una aplicación que permita el bloqueo del dispositivo. Posteriormente, en dicha localidad, se verificó que esta medida trajo resultados positivos, por lo que iniciativas de este estilo pueden ser consideradas en Ecuador.

CONCLUSIONES

El robo de terminales móviles es un problema que ocurre a nivel mundial, por lo que organismos referentes como la UIT y la CITEL han emitido recomendaciones y resoluciones al respecto. De igual forma, entidades internacionales como la GSMA han desarrollado una base de datos global y han puesto a disposición aplicaciones que contribuyan al combate de este ilícito.

Este problema tiene una mayor incidencia en países que no corresponden al primer mundo y en los cuales los equipos móviles constituyen un bien cuyo valor es elevado, debido a que no se producen allí y a los impuestos colocados para su internación, constituyéndose en un negocio de alta rentabilidad, con bandas bien organizadas y abriendo un mercado negro que perjudica notoriamente a la ciudadanía, causando afectación física e incluso la pérdida de vidas humanas.

Ecuador ha emitido normativa puntual en telecomunicaciones para tratar este problema, sin embargo, la última reforma es del año 2012, por lo que se requiere de manera prioritaria una actualización que contemple el avance de este ilícito y que contenga el tratamiento y la regularización de equipos duplicados, no registrados e inválidos, tal como ha sucedido en las naciones colindantes. Es preciso señalar que en el último año de este estudio ha existido un incremento de las cifras de reportes de equipos robados, perdidos y hurtados lo que hace que esta tarea se vuelva prioritaria.

La regulación de listas negativas expedida en Ecuador solo contempla el tratamiento que se debe dar a los equipos reportados como robados, perdidos y hurtados, en tanto que en Perú y Colombia a más de estas categorías se ha incluido otras como, por ejemplo: equipos notificados por fraude por suscripción, reincidentes, duplicados, que no han cumplido el intercambio seguro, entre otras, razón por la cual se hace indispensable actualizar la normativa. Además, al tener este tipo de categorías en los países limítrofes, los equipos que han sido bloqueados por estas causas pueden pasar a Ecuador en donde podrían operar sin restricción, siendo imperante la adopción de medidas sobre el bloqueo de este tipo de equipos.

A más de esta diferencia señalada, la normativa ecuatoriana difiere de la emitida en Colombia y Perú incluso en la conformación de las listas positivas. Esto se debe

principalmente a que estos dos países han efectuado varias reformas a su regulación en los últimos años.

La UIT ha generado recomendaciones importantes que deben ser analizadas detenidamente por las autoridades de Ecuador para que sea recogida en su marco regulatorio.

La utilización de aplicaciones generadas por instituciones externas es de suma importancia para contribuir a combatir este problema, como por ejemplo la herramienta GSMA device check que permite la consulta a nivel mundial de los equipos reportados como robados, perdidos y hurtados por lo que puede ser usada por las instituciones nacionales para fines de investigación y para determinar si hay internación en el país de equipos de otras nacionalidades diferentes a las que se tiene convenio.

Debido a la magnitud de este inconveniente, su tratamiento no debe ser aislado, sino más bien en conjunto y coordinado entre las autoridades de telecomunicaciones, aduanas y vigilancia y seguridad, de forma que pueda ser contrarrestado con mayor efectividad y reducir en cierta manera su impacto nacional. Si bien existen ciertas penalizaciones recogidas en el COIP, se requieren normas complementarias que demanden el trabajo en equipo de las autoridades citadas y de ser posible, emitidas en coordinación. Es necesario también la expedición de normas que involucren el control de los equipos móviles que ingresan al país mediante importaciones que no son masivas.

Se requiere un control para los equipos adulterados, no registrados e inválidos que sean detectados rutinariamente y su tratamiento respectivo, situación que ha sido abordada en este estudio.

Por otro lado, se considera necesario una mayor difusión de este problema que involucre a las autoridades de telecomunicaciones, vigilancia y seguridad, aduanas y prestadores del servicio móvil avanzado que observe entre otras, las siguientes acciones: campañas en medios públicos y redes sociales sobre normas de prevención, aspectos a tomar en cuenta antes y después del robo de un equipo celular, la importancia de efectuar la denuncia pertinente en la Fiscalía General del Estado, a fin de que se pueda ejecutar el seguimiento al hecho reportado, difusión en redes sociales y en las páginas web de los prestadores del servicio móvil avanzado sobre los requisitos, medios de reporte y los aspectos a considerar a la hora de reportar el robo de un celular.

La utilización de la herramienta Kill Switch constituye una alternativa importante a ser empleada por los usuarios en el caso de que su equipo haya sido robado, por lo que, se debe impulsar su uso tal como se ha hecho en otros países.

RECOMENDACIONES

Actualizar la norma vigente en telecomunicaciones sobre el registro de equipos perdidos, robados y hurtados, agregando el tratamiento y la regularización de los diferentes tipos de terminales irregulares citados en este documento.

Realizar una estrategia que incluya planes de trabajo conjuntos entre las autoridades de telecomunicaciones, aduanas y vigilancia y seguridad del estado tendientes a contrarrestar el problema del robo de equipos celulares, de ser necesario generar las normas complementarias que se requieran.

Efectuar una difusión de todos los aspectos que contiene la normativa citada, poniendo énfasis en la manera en que el usuario debe reportar el robo de su equipo, esto es: requisitos, lugares de reporte, formas de notificación, aspectos a considerar para realizar un adecuado reporte que concluya con el bloqueo del equipo.

Promover el uso de herramientas que contribuyan al combate de este problema considerando las recomendaciones internaciones emitidas, los desarrollos de la GSMA y aplicaciones como kill switch.

BIBLIOGRAFÍA

Agencia de Regulación y Control de las Telecomunicaciones (2017). Resolución No. 03-03-ARCOTEL-2017 "Reglamento para Homologación y Certificación de Equipos Terminales de Telecomunicaciones", Registro Oficial del Órgano del Gobierno del Ecuador No. 15, 48–56

Agencia de Regulación y Control de las Telecomunicaciones. (2018). *Homologación Boletín Estadístico.* Recuperado de https://www.arcotel.gob.ec/wp-content/uploads/2018/10/Bolet%c3%adn-Estadistico-Septiembre-2018.pdf

Agencia de Regulación y Control de las Telecomunicaciones. (2018). *Informe de presentación de proyecto de regulación*. Recuperado de https://www.arcotel.gob.ec/wp-content/uploads/2019/11/Informe-proyecto-norma-t%c3%a9cnica-listas-pos-neg-CCDH-CRDS-2019-11-12-pub.pdf

Agencia de Regulación y Control de las Telecomunicaciones (2019). Servicio Móvil Avanzado (SMA). Quito, Ecuador. Recuperado de http://www.arcotel.gob.ec/servicio-movil-avanzado-sma_3/

Agencia de Regulación y Control de las Telecomunicaciones. (2021). *Tu celular legal*. Recuperado de http://tucelularlegal.arcotel.gob.ec/tucelularlegal/

Agencia de Regulación y Control de las Telecomunicaciones. (2021). *Consulta por marca y modelo*. Recuperado de http://tucelularlegal.arcotel.gob.ec/tucelularlegal/consulta_Equipos.aspx

Agencia de Regulación y Control de las Telecomunicaciones. (2021). *Consulta por IMEI*. Recuperado de http://tucelularlegal.arcotel.gob.ec/tucelularlegal/consulta_Imeis.aspx

Agencia de Regulación y Control de las Telecomunicaciones. (2021). *Antes de comprar un teléfono celular*. Recuperado de http://tucelularlegal.arcotel.gob.ec/tucelularlegal/preguntas_frecuentes.aspx

Asamblea Nacional. (2015). Ley Orgánica de Telecomunicaciones. Registro Oficial Órgano del Gobierno del Ecuador, Tercer Sup, 1-40. Recuperado de

http://www.telecomunicaciones.gob.ec/wp-content/uploads/downloads/2016/05/Ley-Orgánica-de-Telecomunicaciones.pdf

Asamblea Nacional. (2014). Código Orgánico Integral Penal. Registro Oficial Órgano del Gobierno del Ecuador, Sup 180, 68-69. Recuperado de https://www.defensa.gob.ec/wp-content/uploads/downloads/2018/03/COIP_feb2018.pdf

Bandas que roban celulares operan con logística completa. (28 de noviembre de 2018). *El Comercio*. Recuperado de https://www.elcomercio.com

Bloke Tech (2021). Lockwarch – Atrapa ladrones. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=com.bloketech.lockwatch&hl=es_EC&gl=US

Bravo, D. (3 de junio de 2016). Celulares reportados como robados en Colombia y Perú fueron localizados en un local de La Marín. *El Comercio*. Recuperado de https://www.elcomercio.com/

Comisión de Regulación de las Comunicaciones. (2011). Resolución 3128. Recuperado de https://normograma.info/crc/docs/resolucion_crc_3128_2011.htm

Comisión de Regulación de las Comunicaciones. (2015). *Fortalecimiento de las bases de datos dentro de la estrategia nacional contra el hurto de equipos terminales móviles*. Recuperado de https://www.crcom.gov.co/uploads/images/files/Documento_soporte(1).pdf

Comisión de Regulación de las Comunicaciones. (2015). Resolución 4813. Recuperado de https://normograma.mintic.gov.co/mintic/docs/resolucion_crc_4813_2015.htm

Comisión de Regulación de las Comunicaciones. (2016). Resolución 4868. Recuperado de https://www.crcom.gov.co/resoluciones/00004868.pdf

Comisión de Regulación de las Comunicaciones. (2016). Resolución 4986. Recuperado de https://www.crcom.gov.co/resoluciones/00004986.pdf

Comisión de Regulación de las Comunicaciones. (2016). Resolución 5038. Recuperado de https://www.crcom.gov.co/resoluciones/00005038.pdf

Comisión de Regulación de las Comunicaciones. (2016). Resolución 5050. Recuperado de https://www.crcom.gov.co/es/pagina/resolucion-crc-5050-de-2016

Comisión de Regulación de las Comunicaciones. (2019). *Simplificación del marco regulatorio para la restricción de equipos terminales hurtados*. Recuperado de https://www.crcom.gov.co/uploads/images/files/Dto%20Problema%20Simplificaci%C3%B3n%20del%20marco%20regulatorio%20para%20la%20restricci%C3%B3n%20de%20equipos%20terminales%20hurtados.pdf

Comisión Interamericana de Telecomunicaciones. (2019), Declaraciones y resoluciones aprobadas por la Asamblea General, 69-73

Comité de Comercio Exterior (2013), Resolución No. 111, 1-3

Comité de Comercio Exterior (2015), Resolución No. 049-2015, 1-6

Comunidad Andina de Naciones (2013). Decisión 786, Gaceta Oficial del Acuerdo de Cartagena No. 2186, 1-8. Recuperado de http://intranet.comunidadandina.org/Documentos/gacetas/Gace2186.pdf

Consejo Nacional de Telecomunicaciones (2009). Resolución 006-01-CONATEL-2009, 1–6

Consejo Nacional de Telecomunicaciones (2009). Resolución 191-07-CONATEL-2009, Registro Oficial del Órgano del Gobierno del Ecuador No. 613, 1–6

Consejo Nacional de Telecomunicaciones (2011). Resolución TEL-214-05-CONATEL-2011, Registro Oficial del Órgano del Gobierno del Ecuador No. 421, 1–7

Consejo Nacional de Telecomunicaciones (2012). Resolución TEL-535-18-CONATEL-2012, Registro Oficial del Órgano del Gobierno del Ecuador No. 781, 1–11

Consejo Nacional de Telecomunicaciones (2012). Resolución 0752-TEL-25-CONATEL-2012, 1–4

Consejo Nacional de Telecomunicaciones (2013). Resolución TEL-878-30-CONATEL-2012, Registro Oficial del Órgano del Gobierno del Ecuador No. 872, 1–7

Constituyente, A. (2008). Constitución de la República del Ecuador.

Deitrick, C. (11 de junio de 2015). *Smartphone thefts drop as kill switch usage grows*. Customer Reports. Recuperado de https://www.consumerreports.org/cro/news/2015/06/smartphone-thefts-on-the-decline/index.htm

European Telecommunications Standards Institute. (2019). *ETSI TS 132 298 V15.6.0 Charging Data Record (CDR) parameter description (3GPP TS 32.298 version 15.6.0 Release 15)*. Recuperado de: https://www.etsi.org/deliver/etsi_ts/132200_132299/132298/15.06.00_60/ts_132298v150600p.pdf

Google LLC (2021). Encontrar mi dispositivo de Google. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=com.google.android.apps.adm&hl=es_EC&gl=US

GSMA. (2021). *GSMA Device Check™*. Recuperado de https://www.gsma.com/services/gsma-imei/about-device-check/

GSMA. (2021). *Services*. Recuperado de https://www.gsma.com/services/

GSMA. (2021). *GSMA Device Check™ for Law Enforcement*. Recuperado de https://www.gsma.com/services/gsma-imei/gsma-device-check-for-law-enforcement/

Harteg J. S. (2021). Crookcatcher - Seguridad. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=com.harteg.crookcatcher&hl=es_EC&gl=US

Kumar, K., Kaur, P. (2015). Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number. *International Journal of Computer Science and Mobile Computing*, *4* (5). 527-533.

Medina, F. (19 de noviembre de 2016). Los celulares robados son activados, pese a seguridades. *El Comercio*. Recuperado de https://www.elcomercio.com

Ministerio de Telecomunicaciones y de la Sociedad de la Información (2012), Acuerdo No. 005-2012, 1-5

MMAppsMobile (2021). Alarma antirrobo. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=mmapps.mobile.anti.theft.alarm&hl=es_EC&gl=US

Nieva, R. (1 de julio de 2015). *La ley 'kill switch' para celulares entra en vigor en California*. CNET. Recuperado de https://www.cnet.com/es/noticias/ley-kill-switch-celulares-california-android-google-apple/

Nicol, J., Garreton, A., & Schodt, C. (2018). Wiped, Flashed, and Rekitted: The International Black Market of Stolen Cell Phones. Recuperado de https://cloudfront.escholarship.org/dist/prd/content/qt14b2493b/qt14b2493b.pdf

Oaksed Technologies (2021). Encontrar teléfono perdido: protección antirrobo. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=com.antitheft.protection.findstolen.lostphone&hl=es_EC&gl=US

Presidencia Constitucional de la República del Ecuador. (2016). Reglamento General a la Ley Orgánica de Telecomunicaciones. Registro Oficial del Órgano del Gobierno del Ecuador Sup 676, 1–37. Recuperado de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2016/02/Reglamento-Ley-Organica-de-Telecomunicaciones.pdf

Presidencia de la República de Perú. (2017). Decreto Legislativo No. 1338.

Presidencia de la República de Perú. (2017). DECRETO SUPREMO Nº 009-2017-IN.

Presidencia de la República de Perú. (2019). DECRETO SUPREMO N° 007-2019-IN

Puente, D. (20 de diciembre de 2019). Los celulares robados son alterados en cuatro ciudades de Ecuador. *El Comercio*. Recuperado de https://www.elcomercio.com/

Roa, L. (2016). Extinción de dominio como herramienta contra el hurto de celulares en la ciudad de Bogotá. *Revista Criminalidad, 58* (2), 157-174. Recuperado de www.scielo.org.co/pdf/crim/v58n2/v58n2a06.pdf

Senado de la República de Colombia. (27 de febrero de 2020). *Radicado proyecto de ley que busca poner freno al robo de celulares en Colombia*. Bogotá, Colombia. Recuperado de

https://www.senado.gov.co/index.php/component/content/article/13-senadores/751-radicado-proyecto-de-ley-que-busca-poner-freno-al-robo-de-celulares-en-colombia

Servicio Nacional de Aduana del Ecuador (2017), Resolución No. SENAE-SENAE-2017-0345-RE, 1-16

Servicio Nacional de Aduana del Ecuador (2019), Resolución No. SENAE-SENAE-2019-0033-RE, 1-11

Twinone (2021). Selfie al Intruso™. GOOGLE PLAY. Recuperado de https://play.google.com/store/apps/details?id=org.twinone.intruderselfie&hl=es_EC&gl=US

Unión Internacional de Telecomunicaciones (2019), Solución marco para contrarrestar la falsificación de dispositivos TIC, 1-30

Velásquez, A., Tovar, A., y Vargas, A. (2017). Impacto socio-económico, financiero y legal del comercio de celulares lícito e ilícito en Florencia Caquetá. FACE: Revista de la Facultad de Ciencias Económicas y Empresariales, 16(2), 66-77.