

7879-SUTEL-SCS-2020

El suscrito, Secretario del Consejo de la Superintendencia de Telecomunicaciones, en ejercicio de las competencias que le atribuye el inciso b) del artículo 50 de la Ley General de la Administración Pública, ley 6227, y el artículo 35 del Reglamento interno de organización y funciones de la Autoridad Reguladora de los Servicios Públicos y su órgano desconcentrado, me permito comunicarle(s) que en sesión ordinaria 060-2020 celebrada el 3 de setiembre del 2020, mediante acuerdo 019-060-2020, de las 13:30 horas, el Consejo de la Superintendencia de Telecomunicaciones aprobó por mayoría, la siguiente resolución:

**RCS-234-2020**

**“SOBRE DISPOSICIONES Y ASPECTOS OPERATIVOS PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE TERMINALES MÓVILES”**

**EXPEDIENTE: GCO-NRE-REL-00123-2020**

**RESULTANDO**

1. Que la Unión Internacional de Telecomunicaciones (UIT) planteó la recomendación UIT-T Q.5050<sup>1</sup> del mes de marzo del 2019, que tiene por objeto describir un marco de referencia para tomar en consideración a la hora de desplegar soluciones para contrarrestar la circulación y utilización de dispositivos para telecomunicaciones falsificados. Específicamente en su Anexo A se refiere directamente a los dispositivos para telefonía móvil. Dado que los terminales móviles basados en tecnologías de la 3GPP utilizan un registro único conocido como IMEI, recomienda: *“bloquear en sus redes los dispositivos móviles con números IMEI no válidos (por ejemplo, sin IMEI, IMEI totalmente nulo, cadenas con formato no normalizado, IMEI duplicados, IMEI asignados por organizaciones no autorizadas y IMEI válidos no asignados por la organización designada)”*.
2. Que por medio de la resolución CCP.I/RES. 189 (XIX-11) de septiembre de 2011 de la Comisión Interamericana de Telecomunicaciones (CITEL) perteneciente a la Organización de los Estados Americanos (OEA) se invitó a los estados miembros y asociados de la CITEL para que adoptaran, reforzaran o complementaran las medidas necesarias para contrarrestar el hurto de equipos terminales móviles, su activación y comercialización a nivel regional.
3. Que el 8 de marzo de 2012, se logró un acuerdo para promover la seguridad ciudadana en el país mediante la firma de un Memorando de Entendimiento (MoU) entre los operadores de telefonía móvil y la Asociación de Operadores GSM (GSMA). En este acuerdo, se alcanzó el compromiso de integrar sus bases de datos de terminales robados con esta última organización y así bloquear el uso de dichos aparatos, no sólo a nivel local, sino por parte de cualquier otro operador/proveedor de servicios de telefonía móvil en cualquier país del mundo que participe de dicha *“lista negra”* de la GSMA.
4. Que por medio del acuerdo 012-023-2012 de la sesión ordinaria número 023-2012 del 12 de abril del 2012, el Consejo de esta Superintendencia reconoció al Memorandum de Entendimiento como la regulación aplicable para la compartición de listas negras.
5. Que en fecha 3 de febrero 2016, los operadores móviles de forma conjunta con el Viceministerio de Telecomunicaciones, la GSMA y esta Superintendencia firmaron un compromiso para adoptar nuevas iniciativas en el marco de la campaña *“Nos Importa Costa Rica”* liderada por la GSMA, con el objetivo de promover la seguridad de la ciudadanía en general en temas relativos al robo de celulares. Dicha iniciativa permitió la implementación de una plataforma Web para consulta en línea, a fin de conocer si un IMEI determinado ha sido hurtado o robado en algunos de los países miembros de la GSMA que contribuyen al intercambio de datos de IMEIs de listas negras.
6. Que, de acuerdo con en el informe ID-42028 del mes de mayo de 2019 remitido mediante oficio 504-

<sup>1</sup> Encontrado en el sitio Web: <https://www.itu.int/rec/T-REC-Q.5050/en>

**7879-SUTEL-SCS-2020**

OPO/UAC/S-2019, el Organismo de Investigación Judicial (OIJ) informó que para el periodo de 2015 hasta el mes de abril del 2019 se presentó un total de 45.583 denuncias por celulares sustraídos por hurto o asalto cuya incidencia viene en aumento en los últimos años.

7. Que, en fecha 25 de marzo de 2015, según indicó el señor Geovanni Rodríguez, en su momento director a.i. del OIJ, se refirió a la problemática de la alteración de IMEIs, donde se clona o “*gemelea*” dicho número, siendo que dicha práctica ha venido en aumento y existe un mercado negro que la facilita, lo cual repercute directamente en un aumento de hurtos y robos de teléfonos celulares.
8. Que, debido a que en el mercado existen disponibles dispositivos que permiten la alteración del número de IMEI de los terminales, hoy en día la lista negra resulta insuficiente para desincentivar el robo de terminales móviles, dada la relativa facilidad de modificación que permiten dichos aparatos. Esto presume un riesgo para la seguridad ciudadana, por lo que se busca mitigar los efectos del hampa con la conformación de listas blancas y un sistema de gestión de terminales móviles.
9. Que de conformidad con el artículo 2 inciso f) de la Ley General de Telecomunicaciones (Ley N°8642) y el artículo 56 inciso f) del Reglamento sobre el Régimen de Protección a los Usuarios Finales de Telecomunicaciones, la Sutel busca desarrollar un Sistema de Gestión de Terminales Móviles que permita identificar terminales con IMEI ilícito, detectar dispositivos falsificados, incluyendo clones; almacenando y analizando, al menos, los datos de operador, IMSI, IMEI, fecha, hora y Cell-ID de inicio y finalización asociados a las comunicaciones realizadas en las redes de telefonía móvil con la finalidad de evitar prácticas identificadas como fraude y para promover un intercambio de las bases de datos entre operadores y proveedores de telefonía móvil.
10. Que esta Dirección sometió a valoración del Consejo el proyecto del Plan Operativo Institucional (POI) QP012020 denominado “*Sistema Nacional de Gestión de Terminales y listas blancas*”, con el fin de brindar al país un sistema de gestión de terminales que sirva de soporte para el control de los dispositivos de telefonía móvil a través de la conformación de diversas bases de datos, lo cual fue acogido por el Consejo de la Sutel mediante acuerdo 06-42-2019 de la sesión ordinaria 42-2019 del 17 de septiembre de 2019; proyecto que finalmente fue aprobado en el POI por la Junta Directiva de la ARESEP mediante acuerdo comunicado mediante oficio OF-0609-SJD-2019 del 24 de setiembre de 2019.
11. Que por medio del oficio 05404-SUTEL-DGC-2020 de fecha 19 de junio de 2020, la Dirección General de Calidad emitió el “informe sobre disposiciones y aspectos operativos para la implementación del sistema de gestión de terminales móviles” en el cual analizó el tema del robo y hurto de terminales móviles en relación con la protección de los usuarios finales, el cual sirve como insumo para la emisión del presente acto.
12. Que se han realizado las diligencias administrativas necesarias para el dictado del presente acto.

## CONSIDERANDOS

### Descripción de la problemática a nivel nacional

- I. Que la sustracción<sup>2</sup> de terminales móviles es una actividad ilícita que ha tenido un incremento sostenido desde que estos se popularizaron en la población.

<sup>2</sup> Delgado, David. “Robo de celulares se duplicó en un año por su fácil reventa” La Nación. Encontrado en:

<https://www.nacion.com/sucesos/crimenes/robo-de-celulares-se-duplico-en-un-ano-por-su-facil-reventa/F4TYZHOVYBB6VI7K4YSCXH5AU4/story/>

Muñoz, Fernando. “OIJ alerta sobre aumento de hurtos durante fin de año: Delincuentes ponen la mira en celulares y tarjetas de crédito” Monumental. Encontrado en: <http://www.monumental.co.cr/2019/11/07/oij-alerta-sobre-aumento-de-hurtos-durante-fin-de-ano-delincuentes-ponen-la-mira-en-celulares-y-tarjetas-de-credito/>

**7879-SUTEL-SCS-2020**

- II. Que en el informe número ID-42028 del mes de mayo de 2019 remitido a esta Superintendencia mediante oficio 504-OPO/UAC/S-2019 se presentan los datos del OIJ para la provincia de San José en donde se evidencia que existe una gran cantidad de asaltos y robos de terminales móviles que afectan la paz social y seguridad de los ciudadanos, según se muestra a continuación:

**Tabla 1. Cantidad de robos y asaltos en San José**

Año	Asalto	Robo	Asalto + Robo
2015	3732	2341	6073
2016	6913	4450	11363
2017	7773	4060	11833
2018	8677	3907	12584
2019 (abril)	2511	1219	3730
<b>TOTAL</b>	<b>27095</b>	<b>15977</b>	<b>45583</b>

- III. Que a partir de las memorias institucionales del OIJ disponibles en línea<sup>3</sup>, es posible tabular los datos de incidencias de asalto y robo a nivel provincial desde el año 2015, según se indica:

**Tabla 2. Denuncias de asalto a nivel nacional**

Año	San José	Alajuela	Heredia	Cartago	Guanacaste	Puntarenas	Limón	TOTAL
2015	6568	1556	1341	1165	582	931	1349	13492
2016	7468	1637	1449	1043	650	1008	1507	14762
2017	7970	1549	1424	1009	596	881	1290	14719
2018	9151	1514	1572	1141	664	899	1549	16490
2019	8113	1604	1372	1113	702	885	1596	15385

Fuente: Memorias Institucionales del OIJ de los años 2016 a 2019

- IV. Que adicionalmente las siguientes son las incidencias de robo a nivel provincial desde el año 2015:

**Tabla 3. Denuncias por robo a nivel nacional**

Año	San José	Alajuela	Heredia	Cartago	Guanacaste	Puntarenas	Limón	TOTAL
2015	4217	1934	1064	642	1196	1832	707	11592
2016	4726	1693	963	762	889	1732	820	11585
2017	7258	2766	1674	1109	2010	2846	1614	19277
2018	6871	2970	1763	1115	924	2710	1469	17822
2019	7280	2785	1766	1185	1878	2600	1544	19038

Fuente: Memorias Institucionales del OIJ de los años 2016 a 2019

- V. Que de la información expuesta, es posible comparar los valores que pertenecen a la provincia de San José y calcular el porcentaje que representan los sucesos en asalto y robo de terminales respecto al total<sup>4</sup>. De esta forma, se tiene que, para el periodo 2016-2018 un 94,97% de las sustracciones por asalto ocurridas se deben a terminales móviles. Por otro lado, para el periodo 2015-2018 un 68,99% de las sustracciones por robo ocurridas en la provincia de San José fueron de un dispositivo móvil.
- VI. Que con el fin de obtener una estimación de la cantidad de delitos relacionados con terminales móviles en el país, se aplicó estos porcentajes a los datos de las memorias del OIJ para todas las provincias. Finalmente, con el fin de obtener un total nacional anual, se procedió a sumar los datos de asalto con los de robo.

**Tabla 4. Aproximación de sustracciones anuales de terminales móviles denunciadas al OIJ**

Año	Asalto	Robo	Total
-----	--------	------	-------

<sup>3</sup> <https://sitiooj.poder-judicial.go.cr/index.php/apertura/transparencia/estadisticas-policiales/memoria-institucional-oij>

<sup>4</sup> Para calcular porcentaje no se considerarán los valores que pertenecen al 2019 pues, respecto a las sustracciones de terminales únicamente se contó con el corte hasta abril de 2019.

7879-SUTEL-SCS-2020

<b>2015</b>	12813	7997	<b>20810</b>
<b>2016</b>	14019	7992	<b>22011</b>
<b>2017</b>	13979	13299	<b>27278</b>
<b>2018</b>	15661	12295	<b>27956</b>
<b>2019</b>	14611	13134	<b>27745</b>

VII. Que al graficar los datos obtenidos se puede observar una clara tendencia de crecimiento de sustracciones de móviles a nivel nacional según se muestra a continuación:

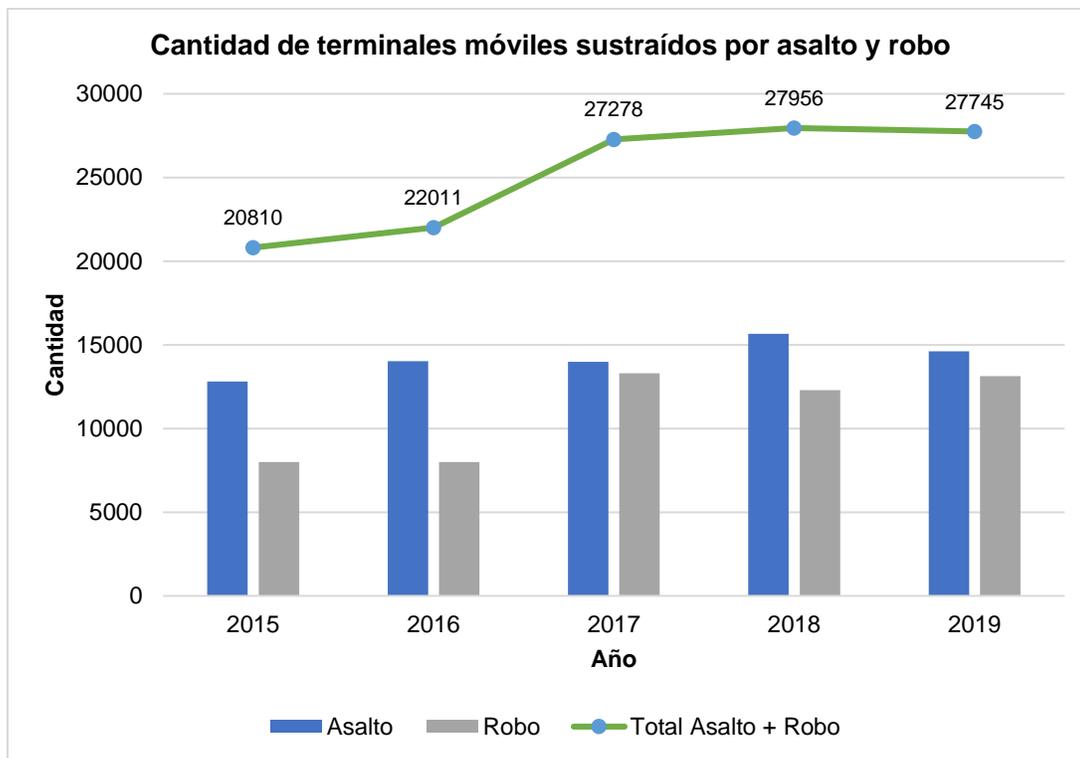


Imagen 1: Cantidad de terminales móviles sustraído por asalto y robo reportados al OIJ

VIII. Que la percepción de seguridad en el país<sup>5</sup> se ha visto afectada directamente por el tema de robo de celulares.

IX. Que el el Tribunal Contencioso Administrativo en la resolución de las 11:01 horas del 27 de mayo de 2015 ha dispuesto sobre el tema de los IMEIs lo siguiente:

*“Se debe indicar que, el IMEI es un número único que identifica cada aparato celular y que con el mismo, se puede determinar o rastrearlo en cualquier lugar del mundo, pues se cuenta con una plataforma de base de datos a nivel mundial que lo facilita. En efecto, precisamente dado este número de identificación, existe una asociación denominada GSMA (Organización Mundial de Operadores Móviles y Compañías relacionadas) que mantiene una base de información suministrada por los diferentes operadores mundiales, dispuesto para paliar, en parte, el problema que se ha generado con el robo de los aparatos y su trasego a nivel internacional, de allí que se haya dispuesto ese mecanismo. Con ocasión del mismo, varias de las operadoras del país, entre ellas*

<sup>5</sup> “Un 53,6% de los costarricenses percibe una inseguridad alta, según encuesta” Diario el País. 14 de diciembre de 2016. Encontrado en: <http://www.diarioextra.com/Noticia/detalle/399874/crimen-aumenta-y-baja-confianza-en-policia> Cascante, Sharon. “Crimen aumenta y baja confianza en policía” Diario Extra. 1° de octubre de 2019. Encontrado en: <https://www.elpais.cr/2016/12/14/un-536-de-los-costarricenses-percibe-una-inseguridad-alta-segun-encuesta/>

Claro, el ICE, Telefónica de Costa Rica TC S.A., Televisora de Costa Rica S.A. (Tuyo) y Virtualis S.A. (Fullmovil) en el mes de marzo de 2012, suscribieron un "**Memorando de entendimiento**" para tener acceso a la base de datos de los IMEI manejada y mantenida por GSMA y según los acuerdos suscritos por las empresas de telecomunicación nacionales con dicha asociación. El Objeto de dicho memorando de entendimiento, lo fue para el uso de los datos y con ocasión de las "terminales perdidas/robadas de sus suscriptores e incluir en la lista negra dichas terminales" (punto 6.1 del memorando folio 145 del expediente judicial) y en su punto 6.7 del mismo se indica: "Únicamente los teléfonos móviles que han sido reportados como perdidos o robados serán ingresados en la base de datos de imei. Los operadores decidirán sus propias políticas para listar dichos teléfonos móviles en sus propios EIR, basado en el principio de que solamente aquellos teléfonos móviles reportados por los propios clientes de los operadores y declarados como perdidos o robados serán incluidos en la lista" (el subrayado no es del original) y en su punto 6.12 se indica: "Las partes son responsables de asegurar que la razón para incluir un teléfono móvil en la Lista Negra es válida y acorde a las leyes de la República de Costa Rica" (Ver contenido del memorando visible a folio 146 del expediente judicial). Se debe indicar que, como lo expresó la Superintendencia de Telecomunicaciones al contestar la demanda que nos ocupa (Folio 312 del expediente judicial) ese órgano conoció el mencionado memorando en la sesión número 023-2012 del 12 de abril de 2012 y mediante acuerdo N° 012-023-2012 lo aprobó y como tal lo incorporó a la regulación nacional. Así las cosas, se puede determinar que, el responsable de ingresar o no el IMEI de un teléfono celular en la lista negra de la base de datos de la GSMA, es el propio operador con el cual mantenía el cliente o suscriptor una relación de servicio (...)

En el Memorando de Entendimiento de marzo de 2012, suscrito entre otras empresas por Claro y aprobado por la Sutel en abril de ese mismo año, se tiene que los únicos aparatos móviles que debían ingresar en esa lista, tal y como lo citamos, lo son aquellos aparatos que habían sido declarados como extraviados y o robados, ya sea por el operador o el suscriptor, en el tanto, ello lleva la lógica y orientación de que al utilizar la base de datos a nivel internacional y nacional, se puede minimizar el trasiego de celulares que en esas condiciones (perdido o robado) se den en el país, ya que al proceder una operadora, como única facultada para ello, a insertar el número de IMEI a la base de datos, éste quedará bloqueado para que no pueda ser usado por otra persona que solicite la habilitación de aquel aparato, ante otra operadora, y que haya sido reportado en las condiciones anormales indicadas."

- X. Que desde el año 2012 se firmó un Memorando de Entendimiento<sup>6</sup> ("MoU") entre los operadores de telefonía móvil y la GSMA que permitió proceder con el bloqueo de los terminales que son reportados como hurtados, robados o extraviados al ser incorporados en la lista negra de la GSMA. Dicho bloqueo se realiza no solo en Costa Rica, sino también con 122 operadores en 43 países y permite contar con estadísticas de la incidencia de dichos hechos. De acuerdo con lo anterior, desde la implementación en junio de 2012 y hasta marzo de 2020, se reportaron un total de 885.504 terminales como robados o extraviados. A continuación, se presenta una tabla donde se evidencian los datos recabados:

<sup>6</sup> Adoptado como regulación aplicable según Acuerdo 012-023-2012 de la sesión ordinaria número 023-2012 del Consejo de esta Superintendencia



**Imagen 2:** Cantidad de reportes de terminales anuales a la GSMA (2012-2020)

- XI.** Que pesar de la implementación de dichas medidas, tal y como se indicó, existen problemáticas que no se han logrado resolver, como particularmente es el caso del plazo en que los operadores intercambian sus registros con la base de datos de la GSMA. El convenio entre dicha institución y los operadores dispuso que deben conectarse de manera diaria entre las 22:00 y las 00:00 horas con la GSMA. No obstante, debido a las diferencias entre tiempos de conexión, podría llegar a transcurrir hasta 48 horas desde el reporte del evento hasta que éste sea reflejado como bloqueado en la red de todos los operadores conectados. Esta situación, permite a los delincuentes comercializar el terminal antes de que sea bloqueado, generando una afectación no sólo a la víctima, sino, también a aquel comprador de buena fe que pudiera adquirir el aparato.
- XII.** Que el sistema de la GSMA no permite la inclusión en las listas negras de terminales con un IMEI inválido, como los que han sido alterados para tener menos de 14 dígitos o con caracteres inválidos (como letras o secuencias consecutivas de números), por lo que estos no pueden ser bloqueados en las redes móviles y podrían ser utilizados para fines ilícitos. Otra deficiencia del sistema actualmente en uso es que actúa únicamente sobre el IMEI del aparato; lo anterior, implica la imposibilidad actual de realizar el bloqueo de IMEIs duplicados con un código válido, pues los dos terminales serían afectados, tanto el original como el que fue alterado con un número duplicado.
- XIII.** Que estas debilidades del sistema de bloqueo actual han permitido que distintos establecimientos comerciales irregulares ofrezcan el “flasheo” o “rooteo” de celulares de manera que se alteran los IMEIs originales con IMEIs clonados, con lo cual se ha restado credibilidad a la Lista Negra por parte de la población, por cuanto estos dispositivos con IMEIs adulterados son comercializados y conectados a las redes de los operadores. Sobre lo anterior, el 25 de marzo de 2015, el subdirector del OIJ Giovanni Rodríguez señaló: *“Ahora hay mucha tecnología que permite modificar el IMEI, eso es como modificarle el número de chasis o de VIN a un vehículo, se puede hacer pero de forma ilícita (...) Nos afecta el proceso de investigación porque nos desvía la atención, porque es más fácil detectar un teléfono con un IMEI original, virgen, que uno donde se haya modificado con alteración de seña y marca el IMEI.”*<sup>7</sup>
- XIV.** Que existe un mercado negro que se encarga de tomar esos teléfonos robados y alterar el IMEI para que de esta forma posea la apariencia de un IMEI válido, por lo cual se puede utilizar normalmente y un tercero

<sup>7</sup> Cabezas, Yaslin “En 2014 se disparó robo de celulares, OIJ dice que mercado negro favorece comercialización” CRHoy. 15 de marzo de 2015. Encontrado en: <https://archivo.crhoy.com/en-2014-se-disparo-robo-de-celulares-oij-dice-que-mercado-negro-favorece-comercializacion/nacionales/>

que lo adquiriera no percibiría su alteración.

- XV.** Que la adquisición del equipo para desbloquear terminales y alteración de los IMEI es muy accesible y relativamente asequible. Por ejemplo, a través del sistema de compras en línea llamado Ebay, se pueden encontrar diversas marcas de equipos especializados en desbloqueo de celulares. A manera de ejemplo, existen marcas como Octopus Box, Furious Gold, Polar Box, Easy Unlocker, Infinity Box, entre otros<sup>8</sup> cuyos precios<sup>9</sup> oscilan desde los ₡85.000,00. Existen otros métodos en donde, al contar con un ordenador, no es necesario adquirir la caja que altera el equipo como tal, sino que se obtiene un programa y, a partir de un código específico, se permite la alteración del IMEI así como el número de serie. El costo aproximado de estos es de unos \$5.<sup>10</sup>



- XVI.** Que, a partir de lo anterior, se requiere tomar acciones que complementen el control existente por parte de los operadores y proveedores con el uso de la lista negra, pues de continuar con la tendencia actual, gran cantidad de delitos de alteración de dispositivos podrían permanecer en la impunidad pues, a pesar de que el terminal robado haya sido reportado ante la GSMA, el delincuente cuenta con múltiples alternativas para su alterar el IMEI y comercializarlo. Es decir, no se cumple el objetivo de minimizar el valor de un terminal móvil robado, lo que implica que no existiría un impacto sobre la seguridad ciudadana.
- XVII.** Que la implementación de un sistema de gestión de terminales móviles nacional el cual administre los números de IMEIs asociados a un servicio, así como la celda en la cual se encuentran estos, permitiría desincentivar el robo y hurto de terminales, pues con dichos datos el sistema detectaría cualquier aparato adulterado y/o duplicado en la red permitiendo su eventual bloqueo inclusive de forma inmediata. Esta medida reduciría el valor de los dispositivos robados, con lo cual se puede llegar a disminuir la comisión de delitos y se reeduca a la población para que al momento de comprar un terminal verifiquen que no correspondan a dispositivos con IMEIs inválidos. Lo anterior generaría una reducción de los delitos patrimoniales a través de la disminución de los factores de riesgo asociados a su comisión, así como del acceso a los medios que los facilitan.

### Experiencia, mejores prácticas y normativa Internacional

#### Comisión Interamericana de Telecomunicaciones

<sup>8</sup> Tomado de: <https://www.ebay.com/itm/SAMSUNG-S6-UART-MICRO-USB-UST-PRO-OCTOPUS-FURIOUS-Z3X-BOX-UNLOCK-FLASH-CABLE/122280763795>

<sup>9</sup> Tomado de: [https://www.ebay.com/sch/i.html?from=R40&trksid=p2047675.m570.l1313.TR8.BC1.A0.H0.Xoctopus+box.TRS0&\\_nkw=octopus+box&\\_sacat=0](https://www.ebay.com/sch/i.html?from=R40&trksid=p2047675.m570.l1313.TR8.BC1.A0.H0.Xoctopus+box.TRS0&_nkw=octopus+box&_sacat=0)

<sup>10</sup> Tomado de: <https://www.ebay.com/itm/Octopus-Octoplus-Box-samsung-1-9-4-Full-Crack-Without-Box-No-Box-Needed/383408426626?>

**XVIII.** Que la Comisión Interamericana de Telecomunicaciones (CITEL) es una entidad de la Organización de Estados Americanos (OEA) que se centra en promover el desarrollo de las telecomunicaciones y tecnologías de las comunicaciones según principios de universalidad, equidad y accesibilidad. CITEL a su vez se encuentra conformada por diversos comités, uno de los cuales es el denominado Comité Consultivo Permanente I (CCP.I) el cual es el órgano asesor en todo lo relacionado a las telecomunicaciones y tecnologías de la información y comunicación.

**XIX.** Que la resolución CCP.I/RES. 189 (XIX-11) tomada en septiembre de 2011 invitó a los estados miembros y asociados para que adoptaran, reforzaran o complementaran las medidas necesarias para contrarrestar el hurto de equipos terminales móviles y su activación y comercialización a nivel regional como el uso de la base de datos negativa de la GSMA. Se instó a que se considerara incluir en sus marcos regulatorios la prohibición de la activación y uso de los IMEI de equipos reportados como hurtados, extraviados o de origen ilegal, tal y como se indica a continuación:

*(...)*

1. *“Invitar a los Estados Miembros y miembros asociados a que adopten, refuercen o complementen las medidas necesarias cada uno en el ámbito de sus competencias para contrarrestar el hurto de equipos terminales móviles y su activación y comercialización a nivel regional.*
2. *Invitar a los Estados Miembros a promover entre los operadores nacionales del servicio móvil que aún no lo dispongan, que consideren la implementación de bases de datos de listas negativas (listas negras), que contengan el registro de los IMEI o el número de serie electrónico del fabricante de los equipos terminales móviles con reporte de hurto o extravío a nivel nacional.*
3. *Invitar a los Estados Miembros a utilizar, entre otras alternativas existentes, plataformas como GSMA IMEI DB, dados los beneficios que puede brindar a los países, sus órganos reguladores y operadores en términos de costo, infraestructura operativa y experiencia en el intercambio de IMEI con reporte de hurto o extravío. (...)*”

**XX.** Que el anexo de dicha resolución planteó la necesidad de implementar las medidas de seguridad pertinentes que impidan la regrabación o duplicación del IMEI o número serial electrónico de identificación del fabricante de los dispositivos para telecomunicaciones móviles. Además, en el caso de que se detecten incidentes de adulteración de equipos, se recomendó que se reporten a la GSMA a fin de que el fabricante pueda remediar y mejorar la seguridad de los terminales en virtud de los convenios existentes entre fabricantes y dicha Asociación. Según se indica a continuación:

*(...)*

- a. *“Que los Operadores e Importadores de equipos terminales móviles de los Estados Miembros propendan hacia la compra de terminales que cumplan con las recomendaciones sobre seguridad contra regrabación o duplicación del IMEI o número serial electrónico de identificación del fabricante, tales como las que ha definido la GSMA.*
- b. *Que los Operadores Móviles de los Estados Miembros que utilicen la tecnología GSM reporten los incidentes de adulteración de equipos terminales móviles a la GSMA a fin de que el fabricante remedie y mejore la seguridad de los terminales en virtud de los convenios existentes entre fabricantes y dicha Asociación. (...)*”

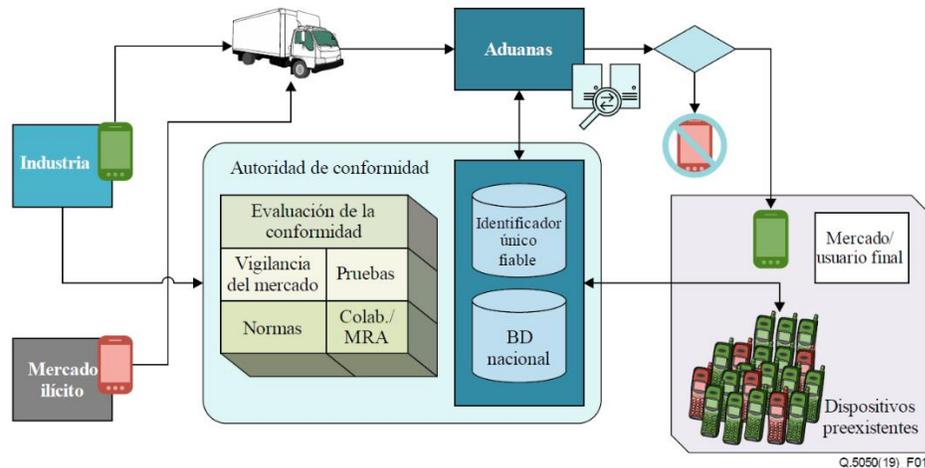
**XXI.** Que la Resolución RES. 68 de la VI Reunión de la Asamblea de la OEA celebrada en febrero de 2014 invitó a todos sus estados miembros a proceder al bloqueo de todos aquellos IMEIs que son reportados como robados o extraviados en otros operadores y países. Se instó a los diferentes países a conectar las bases de datos negativas de IMEI de sus operadores a la GSMA con el fin de que se haga efectivo el intercambio de IMEI con reporte de hurto, robo o extravío. Finalmente, la decisión No. 189 del CCP.I de abril de 2014 invitó a que se realice un intercambio efectivo y bloqueo de terminales móviles con reporte de hurto y/o extravío como se evidencia a continuación: *“5. Invitar a los Estados Miembros a tomar acciones pertinentes conforme a su normativa, con el fin de intercambiar de manera internacional las listas negativas de terminales móviles hurtados o extraviados, mediante la suscripción de acuerdos bilaterales o multilaterales.”*

## Unión Internacional de Telecomunicaciones

TEL.: +506 4000-0000 Apartado 151-1200  
FAX: +506 2215-6821 San José - Costa Rica

800-88-SUTEL gestiondocumental@sutel.go.cr  
800-88-78835

**XXII.** Que la Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de la Organización de las Naciones Unidas (ONU) encargado de regular las telecomunicaciones a nivel internacional entre las distintas administraciones y empresas operadoras. En marzo de 2019 planteó la recomendación UIT-T Q.5050 que tiene por objeto describir un marco de referencia para tomar en consideración a la hora de desplegar soluciones para contrarrestar la circulación y utilización de dispositivos para telecomunicaciones falsificados. A continuación, se presenta el marco general propuesto:



**Imagen 3.** Marco de referencia UIT-T Q.5050

**XXIII.** Que, de acuerdo con la imagen anterior, se propone el uso de bases de datos centralizadas que permitan identificar los dispositivos falsificados de los autorizados según se desprende de la sección 9.4 de la citada recomendación:

*“Se recomienda desplegar una base de datos de referencia centralizada de equipos autorizados en un determinado mercado, basada en identificadores únicos, para diferenciar eficazmente los dispositivos TIC auténticos de los falsificados.”*

**XXIV.** Que la recomendación también procura que se proteja al usuario final de los dispositivos adulterados mediante políticas de información oportunas de modo que se logre una implementación ágil para informar a la ciudadanía de los motivos por los que no se permiten los dispositivos adulterados. Se hace énfasis en que estos sean educados sobre los riesgos potenciales para su salud o la posibilidad de recibir una mala calidad de servicio.

**XXV.** Que la Recomendación UIT-T Q.5050 en su Anexo A es específica al referirse únicamente a los dispositivos para telefonía móvil. Dado que los terminales móviles basados en tecnologías de la 3GPP utilizan un registro único conocido como IMEI, la recomendación para impedir el hurto y proliferación de dispositivos adulterados se basa en: **“bloquear en sus redes los dispositivos móviles con números *IMEI no válidos* (por ejemplo, sin IMEI, IMEI totalmente nulo, cadenas con formato no normalizado, IMEI duplicados, *IMEI asignados por organizaciones no autorizadas y IMEI válidos no asignados por la organización designada*)”** (El resaltado es propio).

**XXVI.** Que el anexo anterior resulta más específico al sugerir el uso de bases de datos de referencia mediante las llamadas listas de colores, a saber:

- a) **Lista blanca:** dispositivos cuyo uso está autorizado.
- b) **Lista gris:** aparatos con estado no confirmado.
- c) **Lista negra:** terminales que se deben rechazar de la red.

**XXVII.** Que el anexo de la Recomendación UIT-T Q.5050 propone que se analicen datos de los operadores, importadores y autoridades aduaneras para generar la lista gris y negra y que, en el caso de que un aparato sea incluido en la lista gris, el propietario debería recibir un aviso con el fin de que confirme el origen legal del aparato en un plazo especificado. El análisis de los datos de los operadores permitiría detectar los IMEI que se clonen en las redes con el beneficio que se pueden tomar acciones para identificarlos y actuar en contra de estos.

### Prácticas Internacionales

**XXVIII.** Que la regulación comparada ha desarrollado sobre el tema de terminales móviles robados, hurtados y/o alterados lo siguiente:

**Tabla 5. Normativa y prácticas internacionales**

País	Regulación	Prácticas
<b>Brasil</b>	Artículo 10, Resolución N. 477/2007, sólo permite a los operadores activar terminales certificados o aceptados por ANATEL. Artículo 77, Resolución N. 477/2007, establece la obligación para la detección de fraudes con terminales móviles, así como la obligación de los proveedores de compartir los costos y beneficios de dichos procesos.	Se bloquean IMEIS de los aparatos reportados como robados/extraviados. Dado que se presentó una alta incidencia de IMEIS clonados, alterados y dispositivos falsificados, se implementaron requisitos de modo que sólo dispositivos certificados pueden ser utilizados. El gobierno de Brasil propuso el sistema llamado SIGA para identificar los dispositivos no certificados y adulterados.
<b>Colombia</b>	Decreto 1630, mayo 2011: medidas para restringir la operación de los equipos terminales hurtados que son utilizados para la prestación de servicio de telecomunicaciones móviles. Ley 1453 (Ley de Seguridad Ciudadana), junio 2011: se incluyeron los artículos 105 y 106 para medidas en materia de bases de datos contra el hurto de celulares y la penalización de la reprogramación o remarcación de equipos terminales móviles. Para garantizar la seguridad ciudadana y se penaliza la activación fraudulenta de los equipos incluidos en dichas bases de datos. Resolución CRC 3128, septiembre 2011: definió el modelo técnico, los aspectos operativos y las reglas para la implementación, carga y actualización de las bases de datos positiva y negativa para la restricción de operación en las redes de telecomunicaciones móviles de los equipos terminales móviles reportados como hurtados y/o extraviados. Resolución CRC 3530, febrero 2011: reglas asociadas a la autorización para la venta de equipos terminales móviles. Decreto 2365, noviembre 2012, medidas de control para las exportaciones de equipos terminales móviles. Decisión Andina No. 786, abril 2013: intercambio de información de equipos terminales móviles extraviados, robados o hurtados y recuperados en la Comunidad Andina.	Se considera delito la reprogramación o alteración de celulares como el cambio de IMEI. Mensualmente se detectan todos los cambios de equipo terminal móvil respecto a la SIM, y sobre una muestra se identifica si dicho equipo se encuentra o no registrado en la base de datos positiva, para así dar un plazo prudencial al usuario para su registro o de lo contrario se bloquea el equipo. Se usa una base de datos (BD) administrativa negativa y positiva centralizada. Se permite una consulta pública a la BD negativa. A las instituciones pertinentes se les permite hacer el registro de IMEIS con reporte por robo/hurto. Se da un acceso de consulta de la BD negativa en línea para la policía y la autoridad aduanera. Se permite el registro de equipos terminales móviles en las bases de datos positivas a través de centros de atención al cliente. Se lleva a cabo un proceso de detección de cambios de equipo para control y bloqueo de equipos que no se registran en la base de datos positiva. Se tiene una conexión a la base de datos de la GSMA a través de servidores de mediación (no directamente a los EIR) para el intercambio de IMEI con los operadores de otros países y la descarga y bloqueo en EIR de IMEI de otros países.
<b>Estados Unidos</b>	<i>Mobile Device Theft Deterrence Act S 1070</i> la cual prohíbe remover, alterar, manipular o destruir los identificadores de los terminales móviles. También penaliza el producir, traficar, tener o custodiar cualquier tipo de hardware o software que permita alterar un identificador móvil. <i>Smartphone Theft Prevention Act H.R. 4065 (2014)</i> el cual requiere que todos los terminales que se venden en Estados Unidos incluyan tecnología que limite el robo de terminales.	La FCC, la CTIA y la GSMA llevaron a cabo un convenio para reducir el robo de terminales mediante la implementación de una base de datos común y la educación de los consumidores. Se puso a disposición una página en línea para la consulta de la base de datos negativa por parte del usuario final y organismos policiales.
<b>Guatemala</b>	Resolución SIT- 1744-A-2013 Inscripción de personas por decreto 8-2013 ley de Equipos Terminales Móviles	Se creó un registro de comercializadores de equipos terminales y tarjetas SIM. Se prohíbe el uso de identificadores anónimas en los servicios, la importación de equipos con IMEI genéricos, el funcionamiento de equipos con IMEI duplicados o reportados como robados/extraviados.
<b>Honduras</b>	Normativa NR009/014 de CONATEL, se establecieron las condiciones de operación y de implementación de la Lista Negra	Se suscribió el Memorándum de Entendimiento (MoU) con la GSMA, mediante el cual se los operadores se

País	Regulación	Prácticas
	de IMEIs.	comprometieron a implementar acciones efectivas que inhabiliten eficazmente el uso de los dispositivos móviles robados, hurtados o extraviados. <i>"A casi un año de su implementación se han bloqueado más de 125.000 aparatos con lo cual se puede decir que la lista negra sí funciona. No obstante, debido a la proliferación de lugares en donde se clonan IMEIs, y en vista que la mayoría de los celulares utilizan sistema operativo tal como ANDROID, se ha generado un mercado de "flasheo" o "rooteo" de celulares para que trabajen con IMEI clonados con lo cual se ha restado credibilidad a la Lista Negra por parte de la población. Adicionalmente aún no existe una "base de datos central" en donde los Operadores compartan la información de celulares bloqueados oportunamente por lo tanto solamente pueden acceder a esta información hasta que se sube a la Lista Negra de la GSMA lo cual ocurre una vez al día a las 00:00 horas. En ese sentido existe oportunidad que los criminales utilicen los celulares que funcionan en distintas bandas ya que solamente fueron bloqueados por uno de los Operadores."</i>
<b>Ecuador</b>	Resolución No. 191-07-CONATEL-2009 del 25 de mayo de 2009, mediante la cual se dispuso: i) empadronamiento de todos los usuarios del sistema de telefonía, ii) Registro de terminales perdidos, robados o hurtados. Resolución TEL-214-05-CONATEL-2011, del 24 de marzo del 2011, mediante la cual: i) se modificaron plazos para el empadronamiento; ii) se establecieron disposiciones para que a los usuarios no empadronados se les suspenda el servicio; iii) se estableció la obligación a las operadoras de intercambiar la información de terminales reportados como robados; y, iv) que las operadoras del realicen la captura del IMEI en forma automática. Resolución TEL-535-18-CONATEL-2012 de 9 de agosto del 2012, mediante la cual se dispuso: i) implementación de las listas positivas y negativas; ii) detección de IMEI duplicados. El Código Orgánico Integral Pena tipificó como delito la reprogramación o modificación de información de equipos terminales móviles, el intercambio, comercialización o compra de información de éstos, así como el reemplazo de etiquetas de identificación y comercialización ilícita de terminales móviles. También se penaliza a la persona que posea infraestructura como programas, equipos, bases de datos o etiquetas para reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil.	Los IMEIs de los terminales reportados como robados son bloqueados todas las redes de los operadores del país. Se tiene un control de la información registrada en el EIR de cada uno de los operadores. Se registran en listas positivas los terminales que han ingresado legalmente al país. Se impide la activación de terminales clonados con números de IMEI inexistentes (como el 0000000000000000, activo en más 18000 terminales) Para la homologación de equipos terminales se exige que el TAC se encuentre registrado por la GSMA. Controlan que los terminales que se activen no se encuentren duplicados. Detectan terminales duplicados y no registrados que se encuentran operando en el Ecuador en líneas que ya se encuentran activas.

**XXIX.** Que la mayoría de los países tienen algún sistema de listas negras donde se bloquean los IMEIs reportados como robados o hurtados. No obstante, reconocen que estas no resultan suficientes debido a la problemática causada por el "flasheo" o "rooteo" de celulares para que trabajen con IMEI adulterados o clonados con lo cual se le ha restado credibilidad a la Lista Negra por parte de la población. Ante esta situación, varios de ellos han implementado sistemas con bases de datos centralizadas entre los operadores que permiten un acceso mucho más expedito a la información y verifica la integridad de los IMEIs.

**XXX.** Que en Colombia, por medio de la Resolución CRC 3128 del mes de setiembre del año 2011, se definió el marco regulatorio que tiene por objeto la restricción de la operación en las redes de telecomunicaciones móviles de los equipos terminales que han sido reportado como hurtados o extraviados. Lo anterior lo realizan por medio de una base de datos centralizada que almacena la información asociada a equipos dispositivos móviles, imponiendo obligaciones tanto para los operadores y proveedores de servicios de telecomunicaciones móviles y al administrador de la base de datos.

**XXXI.** Que en Guatemala se realizó la Resolución SIT-1744-A-2013, sobre la Inscripción de personas por decreto 8-2013 Ley de Equipos Terminales Móviles. En este sentido, se creó un registro de

comercializadores de equipos terminales y tarjetas SIM con el propósito de limitar el uso de equipos terminales que contengan IMEIs genéricos, duplicados o reportados como robados.

- XXXII.** Que Honduras posee una situación similar a la de Costa Rica, suscribieron un Memorandum de Entendimiento con la GSMA, mediante el cual los operadores se comprometieron a implementar acciones efectivas que inhabiliten eficazmente el uso de los dispositivos móviles robados, hurtados o extraviados a través de un reporte a la GSMA para su bloqueo. Tal y como se indicó, en dicho país se han presentado dificultades similares a las experimentadas en Costa Rica, siendo que existe práctica de alteración y clonación de IMEIs, lo cual evita su bloqueo e incorporación en la lista negra. De igual forma reportan graves problemas con el reporte de IMEIs, pues existe una ventana de tiempo mientras los operadores actualizan la base de datos de la GSMA, lo cual hace posible una manipulación por parte de terceros del terminal hurtado o robado previo a su bloqueo.
- XXXIII.** Que en países como Colombia y Estados Unidos existe legislación paralela en materia penal, en la cual existen tipos penales específicos para castigar la manipulación y alteración de los IMEIs, situación que no se encuentra claramente definida en nuestro país, y de ahí la importancia de poseer buenas herramientas regulatorias a nivel de las telecomunicaciones para que dichas prácticas sean disminuidas y eliminadas, en favor de la seguridad ciudadana.

#### **Marco jurídico y normativa aplicable**

- XXXIV.** Que el artículo 46 de la Constitución Política resguarda el derecho de los consumidores y usuarios finales de forma amplia, siendo que dicho artículo indica que: *“Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo.”*
- XXXV.** Que el artículo 60 de la Ley de la Autoridad Reguladora de los Servicios Públicos, Ley N°7593, establece dentro de las obligaciones fundamentales de la Superintendencia de Telecomunicaciones según lo indicado en los sub incisos d) y e) lo siguiente: *“d) Garantizar y proteger los derechos de los usuarios de las telecomunicaciones e) Velar por el cumplimiento de los deberes y derechos de los operadores de redes y la prestación de servicios de telecomunicaciones”.*
- XXXVI.** Que el artículo 73 de la Ley N° 7593, establece en sus incisos a), c) y j) como parte de las Funciones del Consejo de la Superintendencia de Telecomunicaciones lo siguiente:
- a) *Proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios (...).*
  - c) *Incentivar la inversión en el Sector Telecomunicaciones, mediante un marco jurídico que garantice transparencia, no discriminación, equidad y seguridad jurídica, a fin de que el país obtenga los máximos beneficios del progreso tecnológico y de la convergencia (...).*
  - k) *Establecer los estándares mínimos de calidad de las redes públicas y los servicios de telecomunicaciones disponibles al público y fiscalizar su cumplimiento (...)*
  - m) *Ordenar la no utilización o el retiro de equipos, sistemas y aparatos terminales que causen interferencia o que dañen la integridad y calidad de las redes y los servicios, así como la seguridad de los usuarios y el equilibrio ambiental. (...).*

- XXXVII.** Que la Ley General de Telecomunicaciones estipula los objetivos de dicha ley en el artículo 2, de los cuales interesa citar los siguientes:

- d) *Proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios, así como garantizar la privacidad y confidencialidad en las comunicaciones, de acuerdo con nuestra Constitución Política. (...)*
- f) **Promover el desarrollo y uso de los servicios de telecomunicaciones dentro del marco de la sociedad de la información** y el conocimiento y como apoyo a sectores como salud, **seguridad ciudadana,**

*educación, cultura, comercio y gobierno electrónico.” (destacado intencional)*

- XXXVIII.** Que la Ley N°8642 es conteste con lo desarrollado en la Ley N°7593, siendo que resulta de vital importancia la protección de los derechos de los usuarios finales, pero además, dicha Ley N°8642 y aboga por que exista un desarrollo de las telecomunicaciones que contribuya con la seguridad ciudadana, siendo el robo de terminales móviles a todas luces una problemática social que requiere de una atención preferente, desde una panorámica integral, lo cual justifica que el legislador decidiera incorporarlo en un área como las telecomunicaciones. Al mismo tiempo, el artículo 45 de la Ley N°8642 dispone los derechos de los usuarios finales de servicios de telecomunicaciones; al respecto, e importante indicar que este artículo es *numerus apertus* según lo establecido en el inciso 29) que señala que se incluye como derechos los demás establecidos en el ordenamiento jurídico.
- XXXIX.** Que la Ley General de Telecomunicaciones define en su artículo 49 como obligaciones de los operadores y proveedores de servicios de telecomunicaciones en lo que interesa: “(...) 3) *Respetar los derechos de los usuarios de telecomunicaciones y atender sus reclamaciones, según lo previsto en esta Ley y 4) Los demás que establezca la ley.*”
- XL.** Que el artículo 7 del Reglamento de Prestación y Calidad de los Servicios define como equipo terminal al: “*es todo equipo que, conectado a una red de telecomunicaciones, proporciona acceso a uno o más servicios específicos*”.
- XLI.** Que considerando lo anterior, los terminales son esenciales para la utilización de los servicios de telecomunicaciones. Al respecto, según las estadísticas del sector de telecomunicaciones, dado que los servicios de telefonía móvil son los que alcanzan las mayores proporciones de penetración y considerando la especialización de los dispositivos terminales y sus precios, es evidente que serán los más perseguidos por el hampa.
- XLII.** Que el artículo 56 del Reglamento sobre el Régimen de Protección al Usuario Final establece que los operadores/proveedores deberán garantizar que los terminales reportados como robados o extraviados no puedan ser utilizados para servicios de telefonía móvil, categorizando los fraudes en contra del usuario, y destaca lo siguiente:
- “Por otra parte, el operador tiene la obligación de **asegurar al usuario la desactivación del terminal robado o perdido**, evitando la duplicidad de un número asignado a varios terminales. Aquellos **equipos terminales reportados como robados o extraviados a los operadores y proveedores móviles y proveedores no podrán ser utilizados para la prestación de servicios de telecomunicaciones, ni para suscribir nuevos servicios. Los operadores y proveedores móviles y proveedores deberán compartir sus bases de datos de terminales robados o de dudosa procedencia (listas negras y grises) con el fin de evitar este tipo de prácticas**” (destacado intencional)*
- XLIII.** Que según lo anterior, los operadores y proveedores deberán garantizar que los terminales reportados como robados o extraviados no sean utilizados en sus redes, para lo cual se plantea su obligación de compartir las bases de datos respectivas, dado que la legislación reconoce la importancia de no permitir que los terminales se usen sin ningún tipo de control, en detrimento de los usuarios finales y de su seguridad.
- XLIV.** Que a diferencia de la regulación en materia penal específica que castiga la manipulación de los IMEIs como en Colombia y Estados Unidos, nuestro Código Penal no regula este tipo de delitos como un tipo específico. Por lo tanto, las autoridades costarricenses encuentran dificultades para perseguir estas actuaciones, y resulta necesaria la obligación de los operadores/proveedores de compartir sus bases de datos para conformar un sistema unificado que prevenga que se realicen conductas delictivas.
- XLV.** Que la implementación actual de listas negras con la GSMA, ni la citada disposición del Código Penal son suficientes para eliminar las prácticas ilícitas que actualmente se dan en este tema, razón por la cual es necesario un abordaje integral del problema, lo cual se logra a través de la aplicación del artículo 56 del Reglamento sobre el Régimen de Protección al Usuario Final y la compartición completa de

distintos tipos de bases de datos de terminales, pues dicha medida desincentiva la comisión de delitos de esta índole.

**XLVI.** Que a partir de todo lo antes expuesto, resulta claro que los operadores/proveedores tienen la obligación de evitar que los terminales que hayan sido robados o extraviados sean utilizados en sus redes, lo cual hace necesario una coordinación rápida y efectiva entre los operadores para el bloqueo de dichos terminales, lo cual se logra con la compartición de las listas según indica el artículo 56 del Reglamento sobre el Régimen de Protección al Usuario Final. Por lo que, en caso de confirmarse alguna irregularidad en el cumplimiento de dicha obligación le corresponde a esta Superintendencia proceder a aplicar el régimen sancionatorio dispuesto por Ley.

**XLVII.** Que en aras de procurar la protección de los derechos de los usuarios, debido a las limitaciones previamente indicadas, la Sutel tiene la competencia para establecer mecanismos que busquen el control de fraudes, tal y como dispone el artículo 54 del RPUF según se indica a continuación:

*“Potestad de la Sutel para establecer condiciones de seguridad para minimizar el fraude en servicios de telecomunicaciones. La Sutel tiene la potestad de establecer mecanismos o normativas de control de fraude ante los operadores o proveedores de servicio y éstos anualmente deberán presentar las actualizaciones en sus sistemas antifraude ante este Ente Regulador.” (Resaltado propio).*

**XLVIII.** Que existe una obligación de los operadores y proveedores para proveer la colaboración necesaria al Centro Judicial de Intervención de las Comunicaciones (CJIC) como parte de las políticas y disposiciones tomadas en la Ley Contra la Violencia Organizada, Ley N°8754, siendo que el artículo 17 señala lo siguiente:

*“Cualquier empresa, pública o privada, que provea servicios de comunicaciones en el país, estará obligada a realizar lo necesario para la oportuna y eficaz operación del Centro Judicial de Intervención de las Comunicaciones (CJIC), según los requerimientos de este Centro.*

*Serán obligaciones de las empresas y de los funcionarios responsables de las empresas o las instituciones públicas y privadas a cargo de las comunicaciones, las siguientes:*

- 1) Dar todas las facilidades para que las medidas ordenadas por el juez competente se hagan efectivas.*
- 2) Acatar la orden judicial, de manera tal que no se retarde, obstaculice ni se impida la ejecución de la medida ordenada.*

*El incumplimiento de esta norma traerá como consecuencia la sanción de cancelación de la concesión o el permiso de operación de la empresa, para la actividad de comunicaciones. (...)*

**XLIX.** Que dentro de la Ley N°8642 se establecen disposiciones relacionadas con la colaboración de operadores y proveedores de servicios de telecomunicaciones, siendo que el no hacerlo puede conllevar a la revocación del título habilitante según disponen los artículos 18 bis y 22 de la Ley N°8642. Así las cosas, la implementación de un sistema de gestión de terminales móviles permitiría un aprovechamiento del CJIC, siendo que dicha medida posibilitaría identificar plenamente y sin lugar a confusión a las personas involucradas en las investigaciones judiciales de los casos de delitos de delincuencia organizada nacional y transnacional, el cual es el propósito de dicha ley. Todo lo anterior cobra relevancia en vista de las prácticas de dichos grupos donde se busca un anonimato para evitar ser detenidos, práctica que se vería truncada en el caso de que exista un sistema como el propuesto que permita evitar que existan terminales móviles con IMEIs alterados.

**L.** Que según todo lo anteriormente mencionado y en concordancia con lo señalado previamente sobre las funciones de la Sutel, así como los principios y objetivos dispuestos en la legislación nacional, resulta claro que esta institución debe velar por implementar todos los mecanismos necesarios para evitar los fraudes hacia el usuario. A su vez, estos deberán ser adoptados por los operadores y proveedores en aras de buscar la disminución y eliminación de estos. A través de la creación de un sistema centralizado de gestión de terminales móviles se busca contar con un mecanismo idóneo para la disminución de los

fraudes señalados en el artículo 56 del reglamento previamente citado.

- LI.** Que con base en lo estipulado en el artículo 24 de la Constitución Política y el Régimen de Protección a la Intimidad contenido en la Ley General de Telecomunicaciones a partir del artículo 41, dichas medidas se aplicarían siempre en concordancia con el derecho a la privacidad, a la intimidad, a la libertad y al secreto de las comunicaciones, así como la protección de la confidencialidad de la información que los operadores y proveedores obtengan de sus clientes o abonados en atención a la relación comercial que surja entre ellos. En este sentido, toda la información de las bases de datos que sea compartida por parte de los operadores y proveedores no será disponible al público y se resguardará con los más estrictos controles. Dicha información, además de ser cifrada, no contendrá información sensible de los usuarios finales, pues para el correcto funcionamiento del sistema de gestión de terminales móviles no se requiere de información que permita ligar un servicio o número telefónico con la identidad del usuario final ni con el destino de su comunicación.
- LII.** Que a modo de resumen se presenta la legislación relativa al tratamiento que deben dar los operadores en relación a los terminales móviles, protección del derecho de los usuarios y prevención de fraudes:

Norma	Numeral	Texto
Constitución Política	Art. 46	<i>Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo."</i>
Ley N°8642	Art. 2 inciso f)	<b>Promover el desarrollo y uso de los servicios de telecomunicaciones dentro del marco de la sociedad de la información y el conocimiento y como apoyo a sectores como salud, seguridad ciudadana, educación, cultura, comercio y gobierno electrónico.</b> (Destacado intencional).
	Art. 45 inciso 4) y 29)	4) Recibir un trato equitativo, igualitario y de buena fe de los proveedores de servicios. (...) 29) Los demás que se establezcan en el ordenamiento jurídico vigente.
	Art. 49 inciso 3)	3) Respetar los derechos de los usuarios de telecomunicaciones y atender sus reclamaciones, según lo previsto en esta Ley.
Ley N°7593	Art. 73 incisos a), c) y m)	a) Proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas en la prestación de los servicios (...). c) Incentivar la inversión en el Sector Telecomunicaciones, mediante un marco jurídico que garantice transparencia, no discriminación, equidad y seguridad jurídica, a fin de que el país obtenga los máximos beneficios del progreso tecnológico y de la convergencia (...). m) Ordenar la no utilización o el retiro de equipos, sistemas y aparatos terminales que causen interferencia o que dañen la integridad y calidad de las redes y los servicios, así como la seguridad de los usuarios y el equilibrio ambiental. (...).
RPUF	Art. 54	<b>"Potestad de la Sutel para establecer condiciones de seguridad para minimizar el fraude en servicios de telecomunicaciones.</b> La Sutel tiene la potestad de establecer <b>mecanismos</b> o normativas de <b>control de fraude</b> ante los operadores o proveedores de servicio y éstos anualmente deberán presentar las actualizaciones en sus sistemas antifraude ante este Ente Regulador." (Resaltado propio).
	Art. 56	<b>"Por otra parte, el operador tiene la obligación de asegurar al usuario la desactivación del terminal robado o perdido, evitando la duplicidad de un número asignado a varios terminales. Aquellos equipos terminales reportados como robados o extraviados a los operadores y proveedores móviles y proveedores no podrán ser utilizados para la prestación de servicios de telecomunicaciones, ni para suscribir nuevos servicios. Los operadores y proveedores móviles y proveedores deberán compartir sus bases de datos de terminales robados o de dudosa procedencia (listas negras y grises) con el fin de evitar este tipo de prácticas".</b> (Destacado intencional).

- LIII.** Que como bien se puede observar, la regulación vigente establece la obligación por parte de los operadores de velar por la desactivación de aquellos equipos terminales reportados como robados o perdidos, y dispone que estos terminales no podrán ser utilizados para prestar servicios de telecomunicaciones cuando se encuentren en dicha situación. Igualmente se establece la obligación de los operadores para compartir bases de datos de terminales robados o dudosa procedencia. Asimismo, la normativa vigente confiere a la Sutel tiene la potestad y obligación de cumplir con los derechos de los usuarios finales, dentro del cual se encuentra la protección de este ante posibles fraudes en caso de pérdida o sustracción de sus equipos terminales para que estos no puedan ser utilizados por terceros. En

este sentido, la Sutel es la llamada a establecer los mecanismos de control y las condiciones de seguridad para minimizar los fraudes, lo cual forma parte del objetivo de la presente resolución. Lo anterior es prueba que la presente resolución pretende únicamente hacer cumplir un mandato estipulado en la legislación.

### Sobre la potestad regulatoria de la Sutel

**LIV.** Que la competencia regulatoria de la Sutel emana en primera instancia del Tratado de Libre Comercio entre Estados Unidos, Centroamérica y República Dominicana (en adelante TLC). Esta viene a concretarse en el artículo 59 de la Ley de la ARESEP que dispone: *“Corresponde a la Superintendencia de Telecomunicaciones (SUTEL) regular, aplicar, vigilar y controlar el ordenamiento jurídico de las telecomunicaciones (...);”*. (Destacado intencional). De tal forma, se consignó de manera expresa en la ley la competencia reguladora de la SUTEL; como órgano regulador de las telecomunicaciones en el país.

**LV.** Que Sobre este aspecto, la Sala Constitucional de la Corte Suprema de Justicia, señaló que: “A partir del año 2008, con la apertura del mercado de Telecomunicaciones en el país, se dio un cambio en el esquema existente, pasando de un modelo de monopolio estatal a otro en el que existen varios competidores, pero con una fuerte intervención del Estado. La institución encargada de regular este mercado, es la Superintendencia de Telecomunicaciones (SUTEL), que fue creada por el artículo el artículo 59 de la Ley número 8660 “Ley de Fortalecimiento y Modernización de las Entidades Públicas del Sector Telecomunicaciones”, como un órgano de desconcentración máximo adscrito a la Autoridad Reguladora de los Servicios Públicos, con personalidad jurídica propia para administrar el Fondo Nacional de Telecomunicaciones, realizar actividad contractual, administrar sus recursos y presupuesto, así como para suscribir los contratos y convenios que requiriera para el cumplimiento de sus funciones”. (Sala Constitucional de la Corte Suprema de Justicia, Resolución N° 11212-2017 del 14 de julio del 2017)

**LVI.** Que la la Procuraduría General de la República por medio del Dictamen 281 del 14 de agosto de 2008, señaló que:

*“La función reguladora es una técnica de intervención de los poderes públicos en el mercado, que entraña un control continuo sobre una actividad, a fin de hacer prevalecer el interés público sobre el interés privado. A través de la regulación se procura controlar el poder de los monopolios, sobre todo de hecho, asegurar a los consumidores una información adecuada en orden a la calidad, garantías frente a productos defectuosos o precios excesivos, corregir el incremento de los costos, de manera que los precios reflejen los costos de producción, corregir beneficios inesperados resultado de cambios súbitos en los precios; evitar una excesiva competencia que tienda a afectar el mercado; en último término, solucionar inconvenientes que produce la organización del mercado... Función de imperio, la regulación debe estar a cargo de organismos públicos. En la época en que el servicio público era prestado por la propia Administración Pública, ésta ejercía la regulación. No es sino con los procesos de “desregulación” y la apertura de mercados, que surge la necesidad de separar la función de gestión del servicio de la de regulación, con el fin de favorecer la competencia y la autonomía de gestión. Lo que explica la creación de entidades como la Autoridad Reguladora de los Servicios Públicos.”<sup>1</sup>*

**LVII.** Que tal y como se expuso, la Procuraduría se refirió a la función regulatoria como una potestad de imperio mediante la cual los poderes públicos intervienen en el mercado, a fin de ejercer un control sobre dicha actividad, en el caso de la SUTEL sobre las telecomunicaciones, teniendo en cuenta el interés público.

**LVIII.** Que es claro que la SUTEL no posee competencia para dictar normas de carácter reglamentario, no obstante, cuenta con instrumentos y mecanismos a través de los cuales se encuentra facultada para ejercer su competencia regulatoria. En este sentido, los artículos 6 y 124 de la Ley General de la Administración Pública, Ley N° 6227, son claros en establecer otros instrumentos de carácter general de inferior jerarquía a los reglamentos, siendo éstos: *“circulares, instrucciones y demás disposiciones administrativas”*; la inferioridad de estos instrumentos jurídicos en relación con los reglamentos es establecida por la ley, véase que en ese sentido es claro el artículo 6 de la LGAP en contemplar normas de inferior jerarquía a los reglamentos, a saber:

“(…)”

- d) Los decretos del Poder Ejecutivo que reglamentan las leyes, los de los otros Supremos Poderes en la materia de su competencia;
- e) Los demás reglamentos del Poder Ejecutivo, los estatutos y los reglamentos de los entes descentralizados;
- y
- f) **Las demás normas subordinadas a los reglamentos, centrales y descentralizadas.** (Destacado intencional).

**LIX.** Que la Procuraduría General de la República en la Opinión Jurídica número 018-J del 09 de mayo de 1996, destacó que las *circulares, instrucciones y demás disposiciones administrativas*, son inferiores a los reglamentos: “*Artículo 124. Los reglamentos, circulares, instrucciones y demás disposiciones administrativas de carácter general no podrán establecer penas ni imponer exacciones, tasas, multas ni otras cargas similares. De lo anterior se deriva que no se podría, sea vía reglamentaria o disposición de inferior rango normativo (…)*”. (Destacado intencional).

**LX.** Que de acuerdo con lo anteriormente expuesto, la SUTEL en el ejercicio de su competencia regulatoria emite actos administrativos de nivel inferior al reglamento, ya sean *disposiciones, instrucciones, resoluciones o lineamientos de alcance general*; dirigidas a los proveedores y operadores de los servicios de telecomunicaciones, así como a los usuarios de estos servicios, todo ello con el fin de regular materias de su competencia, dentro de los límites fijados en el artículo 124 de la Ley General de la Administración Pública que establece: “*Los reglamentos, circulares, instrucciones y demás disposiciones administrativas de carácter general no podrán establecer penas ni imponer exacciones, tasas, multas ni otras cargas similares*”. (Destacado intencional).

**LXI.** Que de acuerdo con lo anteriormente expuesto, la SUTEL en el ejercicio de su competencia regulatoria emite actos administrativos de nivel inferior al reglamento, ya sean *disposiciones, instrucciones, resoluciones o lineamientos de alcance general*; dirigidas a los proveedores y operadores de los servicios de telecomunicaciones, así como a los usuarios de estos servicios, todo ello con el fin de regular materias de su competencia, dentro de los límites fijados en el artículo 124 de la Ley General de la Administración Pública que establece: “*Los reglamentos, circulares, instrucciones y demás disposiciones administrativas de carácter general no podrán establecer penas ni imponer exacciones, tasas, multas ni otras cargas similares*”. (Destacado intencional).

**LXII.** Que una *instrucción, disposición o circular*, según el artículo 124 Ley N°6227, es un acto administrativo de carácter normativo no reglamentario, un instrumento a través del cual se materializa la función de regulación. Así las cosas, las instrucciones son actos del ámbito de la potestad de regulación, de la función de ordenación, de naturaleza normativa, que se distingue al ejercicio de facultades distintas a ésta, como la potestad reglamentaria, que en el marco jurídico de las telecomunicaciones está reservada a la ARESEP.

**LXIII.** Que las instrucciones o resoluciones –como se han llamado por mera denominación interna de la SUTEL- dirigidas a los operadores (en general o individualmente) son en esencia disposiciones específicas que tienen asidero y sustento en normas legales o reglamentarias, que vienen a complementarlas e implementarlas, o a aclarar y facilitar su aplicación, y que constituyen un mecanismo esencial e indispensable para el ejercicio de la función regulatoria.

**LXIV.** Que esta Superintendencia tiene la competencia para dictar instrucciones o disposiciones administrativas, como la presente, que no tienen un carácter reglamentario y están dirigidas a sus regulados con el fin de interpretar y hacer cumplir el contenido de la normativa vigente. Asimismo constituyen disposiciones que se circunscriben, cumplen y respetan con las normas de mayor rango, como reglamentos, las leyes, tratados y convenios internacionales y la Constitución Política.

## Conclusiones

**LXV.** Que a partir de los datos del OIJ, se evidencia que existe una gran cantidad de hurtos y robos de

terminales que afectan la paz social y seguridad de los ciudadanos costarricenses.

- LXVI.** Que, según los datos de la GSMA, entre junio de 2012 y marzo de 2020, se han presentado un total de 885.504 terminales reportados como robados o extraviados.
- LXVII.** Que a pesar de que Costa Rica se encuentra dentro de los países que han firmado un convenio con la GSMA para bloquear los equipos terminales reportados como robados o extraviados, persiste el robo y hurto de éstos debido a debilidades del sistema actual, como la amplia ventana de tiempo existente para la actualización de las bases de listas negras y la imposibilidad de bloquear IMEIs irregulares.
- LXVIII.** Que además de las limitaciones del sistema de listas negras de la GSMA, existe una proliferación de comercios donde se ofrece el “*rooteo*” o “*flasheo*” de terminales móviles adulterando sus IMEIs lo cual permite la comercialización de estos dispositivos y acrecienta la problemática del robo de terminales.
- LXIX.** Que por medio de la resolución CCP.I/RES. 189 (XIX-11) de septiembre de 2011 se invitó a los estados miembros y asociados de la CITEL para que adoptaran, reforzaran o complementaran las medidas necesarias para contrarrestar el hurto de equipos terminales móviles y su activación y comercialización a nivel regional.
- LXX.** Que la Recomendación UIT-T Q.5050 en su Anexo A establece las medidas a tomar por parte de los operadores y proveedores de servicios de telecomunicaciones móviles para que sean bloqueados los números de IMEIs no válidos y los duplicados, para lo cual se sugiere la categorización de bases de datos según una lista de colores a saber; blanca, gris, negra.
- LXXI.** Que en Latinoamérica varios países que realizan el intercambio de listas negras con la GSMA comparten las problemáticas locales sobre el robo, hurto y alteración de terminales móviles, para lo cual países como Colombia han optado por implementar la centralización de una base de datos que almacena la información asociada a equipos terminales móviles, imponiendo obligaciones tanto para los operadores y proveedores de servicios de telecomunicaciones móviles y al administrador de la base de datos.
- LXXII.** Que la UIT ha propuesto que los países miembros desplieguen una base de datos de referencia centralizada donde se identifiquen los equipos válidos y de esta forma se diferencien de los adulterados.
- LXXIII.** Que la implementación de un sistema centralizado a través de una entidad de referencia donde los operadores y proveedores suministren la información sobre sus bases de datos permitiría un mayor rango de control para eliminar la práctica el “*flasheo*” o “*rooteo*” de IMEIs y desincentivaría el robo y hurto de terminales.
- LXXIV.** Que el artículo 54 del RPUF dispone que la Sutel es la entidad competente para establecer las condiciones de seguridad y mecanismos para minimizar el fraude en servicios de telecomunicaciones.
- LXXV.** Que la Sutel tiene la potestad para establecer mecanismos para regular el fraude en telecomunicaciones, por lo cual las presentes disposiciones buscan la instrumentalización de las citadas potestades.
- LXXVI.** Que el artículo 56 del Reglamento sobre el Régimen de Protección al Usuario Final dispone la obligación por parte de los operadores y proveedores de servicios de telecomunicaciones de asegurar la desactivación de aquellos terminales reportados como robados o extraviados y de compartir sus bases de datos de terminales robados o de dudosa procedencia con el fin de evitar la comisión de delitos y la alteración o modificación de los IMEIs.
- LXXVII.** Que la normativa vigente establece la obligación de los operadores de asegurar que los terminales perdidos, robados o de dudosa procedencia no sean utilizados para la provisión o utilización de servicios de telecomunicaciones.

**LXXVIII.** Que en congruencia con las recomendaciones de la UIT y de la CITELE, así como de forma consistente con el proyecto POI QP012020, resulta necesario establecer la regulación que permita administrar en Costa Rica, las listas negras, grises y blancas.

Por consiguiente, y con fundamento en la Ley General de Telecomunicaciones, ley número 8642, la Ley de la Autoridad Reguladora de los Servicios Públicos, ley número 7593, y la Ley General de la Administración Pública, ley número 6227,

**EL CONSEJO DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES,  
RESUELVE:**

Definir las siguientes instrucciones de acatamiento obligatorio para a la protección de los derechos de los usuarios finales y con el propósito de buscar soluciones ante la creciente comisión de delitos asociados al hurto y robo de terminales móviles.

**1. Sobre los procesos operativos del Sistema de Gestión de Terminales Móviles (SGTM)**

De conformidad con el artículo 56 inciso f) del Reglamento sobre el Régimen de Protección a los Usuarios Finales de Telecomunicaciones y en congruencia con el proyecto POI QP012020, se dispone la creación del Sistema de Gestión de Terminales Móviles que permite identificar terminales con IMEI's ilícitos, detectar dispositivos falsificados, incluyendo clones; almacenando y analizando, al menos los datos de operador como IMSI, IMEI, fecha, hora y Cell-ID de inicio y finalización asociados a las comunicaciones realizadas en las redes de telefonía móvil con la finalidad de evitar prácticas identificadas como fraude y para promover un intercambio, de las bases de datos entre operadores y proveedores de telefonía móvil.

**1.1 Definiciones**

- a) **Cell-ID:** es utilizada para identificar de manera única a una celda de cada radiobase.
- b) **Código de Luhn:** décimo quinto dígito de un IMEI que se calcula a partir de los 14 dígitos anteriores según el algoritmo que se define en el Anexo B de la norma ISO/IEC 7812.
- c) **GSM (Global System for Mobile Communications):** sistema global para comunicaciones móviles, que utiliza el estándar de segunda generación (2G).
- d) **GSMA:** asociación de operadores móviles que brindan servicios basados en GSM.
- e) **Entidad de Referencia de Terminales Móviles (ERTM):** empresa seleccionada para proveer el servicio de gestión completa del intercambio de listas, blancas, grises y negras entre operadores y proveedores.
- f) **Equipo terminal:** es todo equipo que, conectado a una red de telecomunicaciones, proporciona acceso a uno o más servicios específicos.
- g) **IMEI (International Mobile Equipment Identity):** identidad internacional de equipo móvil que corresponde al identificador único de 15 dígitos que distingue un terminal en la red móvil a nivel mundial, cuya estructura se define en la sección 6.2.1 de la norma 3GPP TS 23.003.
- h) **IMEI Duplicado:** corresponde a un IMEI que está siendo utilizado de manera simultánea por dos o más servicios con independencia de la red u operador.
- i) **IMEI irregular:** corresponde a una condición atípica del identificador del terminal cuando el mismo no ha sido otorgado por la GSMA por medio de un TAC, falla la comprobación del código de Luhn o cuando existen dos o más servicios que utilizan el mismo IMEI en las redes de telecomunicaciones, dentro de una determinada ventana de tiempo y distancia.
- j) **IMSI:** Identidad Internacional del Abonado Móvil, código de identificación único para cada dispositivo de telefonía móvil.
- k) **Lista Blanca de IMEI:** contiene los registros de IMEI válidos generados por la GSMA y el de los terminales homologados generada por Sutel.
- l) **Lista Gris de IMEI:** contiene los registros de IMEI irregulares que requieren un análisis para su eventual transición a la lista blanca o lista negra.
- m) **Lista Negra de IMEI:** registros de IMEI que no pueden ser empleados para suscribir o utilizar

servicios de telecomunicaciones debido a un reporte de robo, hurto, extravío del terminal, cuando el operador/proveedor aplica la desconexión definitiva del servicio debido al incumplimiento de pago del subsidio o pago en tractos del terminal, cuando el IMEI no es otorgado por la GSMA o falla la validación del código de Luhn, o si una autoridad judicial competente lo solicita directamente a la Sutel o al operador/proveedor.

- n) **Operador de servicios de telecomunicaciones:** persona física o jurídica, pública o privada, que explota redes de telecomunicaciones con la debida concesión o autorización, las cuales podrán prestar o no servicios de telecomunicaciones disponibles al público en general.
- o) **Proveedor de servicios de telecomunicaciones:** persona física o jurídica, pública o privada que proporciona servicios de telecomunicaciones disponibles al público sobre una red de telecomunicaciones con la debida concesión o autorización.
- p) **Servicios de mensajería corta (SMS):** servicio que permite el intercambio de mensajes cortos alfanuméricos (máximo 160 caracteres) entre equipos terminales conectados a través de una red pública de telecomunicaciones.
- q) **Superintendencia de Telecomunicaciones (Sutel):** órgano de la Autoridad Reguladora de los Servicios Públicos encargado de regular, supervisar, aplicar, vigilar y controlar el ordenamiento jurídico de las telecomunicaciones. Equipárese al término Regulador.
- r) **TAC (Type Allocation Code):** corresponde al código de ocho (8) dígitos asignado por la GSMA de acuerdo con el proceso GSMA TS.06 para identificar a una marca y modelo específico de un terminal de telefonía móvil.
- s) **TAC inválido:** corresponde a un TAC que no ha sido otorgado por la GSMA.
- t) **Usuario final:** persona física o jurídica, que recibe y utiliza un servicio de telecomunicaciones, sin explotar redes públicas de telecomunicaciones y sin prestar servicios de telecomunicaciones disponibles al público. El mismo podría ostentar la condición de cliente.

## 1.2 Sobre la Entidad de Referencia de Terminales Móviles (ERTM)

La Entidad de Referencia de Terminales Móviles (ERTM) corresponde a la empresa que determine el órgano regulador por medio del debido proceso y, será la encargada del intercambio de los IMEIS entre operadores y la GSMA para las listas negras, grises y blancas en lo que corresponda.

## 1.3 Sobre el Sistema de Gestión de Terminales Móviles (SGTM)

El Sistema de Gestión de Terminales Móviles (SGTM) estará a cargo de la ERTM en cuanto a su implementación y mantenimiento. Este consiste en todo el equipo necesario (*software* y *hardware*) que permite la administración y gestión de la totalidad de dispositivos conectados a las redes de telefonía móvil en el país. La Sutel a su vez se encontrará a cargo de su administración.

## 1.4 Sobre el Comité para la Gestión de Terminales Móviles (CGTM)

El Comité para la Gestión de Terminales Móviles (CGTM) consiste en un ente consultivo el cual se encargará de definir las políticas de operación del SGTM que serán atendidas por la ERTM. El CGTM estará conformado por dos representantes (uno titular y uno suplente) por cada área (técnica y legal) de cada operador y proveedor de redes de telefonía móvil en el país que cuenten con numeración asignada, así como los funcionarios de la Sutel que sean designados por esta. Todos los miembros deberán ser autorizados mediante una nota emitida por parte del representante legal de cada operador o proveedor a fin de que se le faculte para la toma de decisiones relacionadas. Dicho comité estará dirigido por un presidente quien se encargará de llevar el orden de la sesión; y un secretario, ambos funcionarios de la Sutel, y este último se encargará de convocar a las reuniones y registrar mediante actas los asuntos tratados y acuerdos alcanzados durante las sesiones de trabajo.

Las decisiones que adopte el Comité deben ser tomadas de manera unánime. En el caso de que estas versen sobre aspectos de operación interna del Comité, no requerirán ser elevados para la aprobación del Consejo de la Sutel. No obstante, en el caso que estas decisiones afecten el funcionamiento del SGTM serán ratificadas por el Consejo de la Sutel en el tanto se encuentren apegadas a la normativa

vigente. Por su parte, en caso de que no exista una posición consensuada, el Consejo de la Sutel resolverá las discrepancias que surjan entre los operadores a lo interno de dicho Comité de conformidad con lo dispuesto en el artículo 73 inciso f) de la Ley N°7593.

#### 1.4.1 Funciones del CGTM

- a. Fortalecer la relación entre los operadores y proveedores de telecomunicaciones en el entorno de la gestión de terminales móviles para aportar a la seguridad ciudadana.
- b. Definir las opciones para la conexión y entrega de información por parte de los operadores a la ERTM.
- c. Proponer alternativas para el desarrollo y mejora de las condiciones y servicios asociados con la administración y gestión de terminales de telefonía móvil en Costa Rica.
- d. Establecer y sugerir lineamientos para asegurar el cumplimiento del marco legal y demás disposiciones regulatorias relacionadas con la administración y gestión de terminales de telefonía móvil.
- e. Generar recomendaciones sobre cualquier otra actividad relacionada con la implementación, operación, mejora de la administración y gestión de terminales de telefonía móvil.
- f. Recomendar al Consejo de la Sutel los aspectos técnicos y administrativos que funjan como parámetros para el bloqueo de terminales con un IMEI irregular.

#### 1.5 Sobre la Entidad de Referencia de Terminales Móviles (ERTM) y el Sistema de Gestión de Terminales Móviles (SGTM)

La Entidad de Referencia de Terminales Móviles (ERTM) administrará un conjunto de bases de datos de forma tal que se garantice no solo el bloqueo de los dispositivos reportados como robados o extraviados, sino también que no se puedan conectar a las redes de los operadores o proveedores aparatos con IMEIs irregulares (los cuales pueden ser inválidos, duplicados o con código de Luhn adulterado) como parte del Sistema de Gestión de Terminales Móviles (SGTM). Para el correcto funcionamiento este sistema, los operadores o proveedores deberán velar por el cumplimiento de diversas condiciones operativas relativas a la conformación y aplicación de las citadas bases de datos en sus equipos y plataformas, así como suministrar la información que les sea requerida para conformar y operar dichas bases de datos.

##### 1.5.1 Obligaciones de la Entidad de Referencia de Terminales Móviles (ERTM)

Las siguientes son obligaciones de la ERTM:

- a. Implementar, generar, administrar, mantener e integrar una base de datos centralizada de Listas Blancas, Listas Grises y Listas Negras a partir de la información que obtiene a través de los operadores y proveedores móviles. Dicha información será propiedad exclusiva de la Sutel, así como de los operadores y por sus características no será disponible al público para lo cual se establecerán los mecanismos idóneos para el cifrado de esta información y garantizando la confidencialidad de esta.
- b. Utilizar y analizar los datos de IMSI, IMEI, fecha, hora y Cell-ID de inicio y finalización asociados a las comunicaciones realizadas en las redes de telefonía móvil para operar las bases de datos necesarias (lista blanca, gris y negra). No deberá obtener o almacenar de forma alguna información de la identidad de los usuarios de servicio de telecomunicaciones.
- c. Garantizar el registro anónimo de la información que se almacene en sus bases de datos.
- d. Descartar los insumos de información que no determinen a un IMEI duplicado.
- e. Proporcionar los mecanismos que permitan asegurar el bloqueo de IMEIs reportados como robados o extraviados, así como los procedimientos para la detección y gestión de IMEIs irregulares.
- f. Permitir, a través de la información ligada al TAC que otorga la GSMA, la detección de las características asociadas a los IMEIs que se conectan a las redes de telefonía móvil para la toma de decisiones que permitan su eventual bloqueo según las reglas que defina el CGTM.

- g.** Desarrollar y mantener en línea un módulo WEB alojado en un dominio de la Sutel, que permita a los usuarios finales de telecomunicaciones móviles consultar el estado de su terminal a través del IMEI, que le indique la marca y modelo asociados a éste en los registros de la GSMA. Este deberá permitir un máximo de dos (2) consultas por dirección IP y su acceso será permitido únicamente para una dirección origen en Costa Rica. Los operadores tendrán disponible este servicio a través de las interfases apropiadas que se definan en las sesiones del CGTM, sin límites de consulta o restricciones.
- h.** Desplegar la infraestructura que permita la notificación por SMS y llamada de voz a los usuarios finales de telecomunicaciones para dispositivos que se encuentren en una situación irregular y que se notifique al usuario en caso de uso de IMEIs válidos no homologados. El SGTGM deberá registrar los acuses de recibo de los SMS y CDR de las llamadas de voz realizadas. Debido al carácter informativo y regulatorio de las comunicaciones, en concordancia con el artículo 44 de Ley N°8642, estas no serán consideradas como no solicitadas.
- i.** Enrutar las llamadas del SGTGM hacia la red del operador en la cual el usuario recibe los servicios de telefonía móvil. Para estos efectos deberá interconectar el módulo de notificación de llamada de voz del SGTGM a la base de datos de números portados del Sistema Integral de Portabilidad Numérica (SIPN).
- j.** Garantizar una disponibilidad de la totalidad de sistemas y plataformas del SGTGM igual o superior a un 99,6% mensual.
- k.** Identificar, a través del SGTGM, los IMEIS válidos no homologados, así como los IMEIS irregulares, a partir de las siguientes situaciones: IMEI cuyo TAC no ha sido otorgado por la GSMA, falla la comprobación del código de Luhn, IMEI duplicado o clonado (dentro o fuera de la red de un operador).
- l.** Implementar las reglas para el manejo de las diversas listas según los acuerdos del CGTM y las regulaciones que disponga Sutel.
- m.** Deberá realizar y mantener la interconexión del SGTGM con la GSMA de modo que permita el registro y difusión de los IMEIS de la lista negra internacional de la GSMA y no se puedan activar terminales reportados como robados o hurtados en otros países. En caso de que se presenten incidencias de bloqueo de IMEIS destinados para el mercado costarricense, hecho que deberá ser comprobado por el fabricante del terminal, y que Sutel determine que han sido duplicados y reportados como robados o extraviados en el extranjero, el SGTGM deberá permitir que la persona utilice su servicio en dicho aparato.
- n.** Permitir el acceso a instituciones gubernamentales competentes debidamente acreditadas para realizar el ingreso fundamentado de IMEIS a la lista negra.

## 1.6 Acciones por tomar por parte de los operadores

De acuerdo con la legislación nacional, específicamente los artículos 54 y 56 inciso f) del RPUF, los operadores deberán garantizar lo siguiente:

- a.** Impedir la conexión o el uso de servicios de telecomunicaciones móviles con IMEI de los equipos terminales móviles reportados como robados, extraviados o hurtados por sus clientes, así como los que sean ordenados por el SGTGM.
- b.** Aplicar en su red las listas blancas, grises y negras que sean establecidas por el SGTGM.
- c.** Atender los procedimientos de atención vigentes que defina el CGTM, que cuenten con el aval del Consejo de Sutel, para el tratamiento de los usuarios finales con los diversos tipos de IMEIs irregulares y, cuando corresponda, deberá estar en la capacidad para proceder a la suspensión temporal de un servicio mientras se mantenga asociado a un IMEI irregular para la operación en su red.
- d.** Remitir los mensajes y llamadas de advertencia a los abonados o usuarios sobre los casos relativos a equipos terminales móviles con IMEI irregulares, alterados, duplicados, clonados o con IMEI no homologado que genere el SGTGM.
- e.** Habilitar el equipo terminal móvil recuperado por un usuario cuando demuestre que ha recuperado el dispositivo que había solicitado bloquear por motivo de robo, hurto o extravío y

presente la documentación pertinente (como factura de compra y verificación de su documento de identidad, entre otros que puedan ser definidos por el CGTM).

- f. Remitir al SGTM la información que sea necesaria para su funcionamiento adecuado, considerando como mínimo los datos de IMSI, IMEI, fecha, hora y Cell-ID de inicio y finalización asociados a las comunicaciones realizadas en sus redes.
- g. Atender en primera instancia las incidencias y reclamaciones que reciban de sus usuarios por el bloqueo del IMEI de su terminal o la suspensión temporal de su servicio asociado a un IMEI irregular con independencia de si el terminal fue comprado en el mismo operador o fue aportado por el cliente y su condición de homologación.
- h. Designar a los responsables que participarán en las Mesas de Ayuda para la resolución de controversias relativas a la operación normal del SGTM.

### 1.7 Sobre las acciones por ejecutar por parte la Sutel

La Sutel ejecutará las siguientes acciones:

- a. Disponer las condiciones operativas del SGTM.
- b. Requerir información a los operadores o proveedores de telefonía móvil y determinar si procede la incorporación de equipos terminales móviles en la Lista Blanca o Lista Negra del SGTM.
- c. Supervisar y fiscalizar el cumplimiento de las obligaciones de los operadores y proveedores establecidas en el marco de sus competencias.
- d. Requerir a los operadores o proveedores de telefonía móvil, cuando corresponda, la suspensión temporal de las líneas, remisión de mensajes de advertencia a los usuarios de IMEIS irregulares y a aquellos que se determinen como no homologados.
- e. Coordinar y dirigir las Mesas de Ayuda para la atención de las controversias que se puedan generar a través de la operación normal del SGTM en caso de que los conflictos no se puedan resolver entre los operadores y los usuarios finales. En casos de especial complejidad, la Sutel podrá recurrir a uno de los peritos autorizados que hayan cumplido con la resolución del Consejo de la Sutel RCS-286-2018 y sus eventuales reformas para que proceda a realizar las pruebas correspondientes que permitan resolver dicha controversia.
- f. Establecer las instrucciones operativas relativas al SGTM para lo cual valorará las decisiones y acuerdos tomados por el CGTM.

### 1.8 Disposición transitoria

Una vez que el SGTM entre en funcionamiento y el CGTM defina los aspectos administrativos y operativos pertinentes, se dará un plazo de seis (6) meses para que los usuarios con dispositivos en condición irregular normalicen dicho estado de manera previa al bloqueo masivo inicial de los aparatos.

### ACUERDO FIRME PUBLÍQUESE

*La anterior transcripción se realiza a efectos de comunicar el acuerdo citado adoptado por el Consejo de la Superintendencia de Telecomunicaciones.*

## CONSEJO DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES

**Luis Alberto Cascante Alvarado**  
Secretario del Consejo