INSTITUTO FEDERAL DE TELECOMUNICACIONES

Estudio para identificar acciones para disminuir el robo de equipos terminales móviles

Instituto Federal de Telecomunicaciones

Diciembre 2023

Aviso legal

El Instituto Federal de Telecomunicaciones, es el órgano autónomo regulador y autoridad de competencia económica, con facultades exclusivas, en los sectores de telecomunicaciones y radiodifusión, conforme lo dispuesto en el artículo 28°, párrafo décimo cuarto, décimo quinto y décimo sexto de la Constitución Política de los Estados Unidos Mexicanos; 7° de la Ley Federal de Telecomunicaciones y Radiodifusión; además del 5°, párrafo primero, de la Ley Federal de Competencia Económica. Este documento se publica con el objeto de darle a conocer al público general y especializado, la situación en México, respecto al robo de equipos terminales móviles, por su incidencia pone en riesgo la seguridad de usuarios de redes públicas, se aborda la problemática generada por este acto delictivo y se comparan las medidas a nivel internacional para su combate, con el objeto de dar a conocer diversas acciones aplicables al problema.

Es importante resaltar que el contenido de este documento no refleja la postura institucional, ni es vinculante para el Pleno del Instituto Federal de Telecomunicaciones, así como tampoco para los sectores regulados, sujetos obligados o el usuario.

ÍNDICE

Introducción. 1

I. Contexto general del problema. 3

a. Ecosistema de la venta de equipos móviles robados. 3

b. Afectación desde la perspectiva técnico y económica. 5

PUNTOS CLAVE DEL CAPÍTULO I 9

II. Acciones generales a la problemática. 10

a. Asociación Global de Sistemas Móviles de Comunicación-GSMA, Base de datos global (*Lista negra* o *Block List* o *Black List*). 10

b. Unión Internacional de Telecomunicaciones (*UIT*) 12

c. Combinación de Listas Blancas y Listas Negras. 14

d. Soluciones antirrobo basadas en el dispositivo (*Kill switch*). 15

e. Vinculación *IMSI-IMEI*. 17

f. Servicios de comprobación de dispositivos. 20

PUNTOS CLAVE DEL CAPÍTULO II 22

III. Experiencia Internacional. 23

a. Panorama general y políticas implementadas en Latinoamérica 23

ARGENTINA 23

BOLIVIA 23

COLOMBIA 24

CHILE 27

PERÚ 29

PARAGUAY 31

ECUADOR 33

COSTA RICA 35

b. Panorama general y políticas implementadas Estados Unidos de América. 37

c. Panorama general y políticas implementadas Europa 39

REINO UNIDO 39
GRECIA 39
FRANCIA 40
d. Acciones más utilizadas a nivel internacional 40
PUNTOS CLAVE DEL CAPÍTULO III 42
IV. Situación actual y medidas tomadas en México. 43
a. Antecedentes del robo de ETM en México. 43
b. Uso de la *Block List* o Lista Negra en México 49
c. Políticas y acciones para reducir el robo de ETM en México. 52
PUNTOS CLAVE DEL CAPÍTULO IV 58
V. Acciones posibles para disminuir el robo de ETM. 59
a. *Kill switch*. 59
b. Listas Blancas. 59
c. Obligaciones de los operadores. 60
d. Responsabilidad de Usuario: Campaña de difusión por parte el Instituto. 61
PUNTOS CLAVE DEL CAPÍTULO V 62
VI. Conclusión. 63
Referencias 67

Introducción.

Actualmente, los equipos terminales móviles (en lo sucesivo, "ETM") forman parte indispensable de la vida de los usuarios, debido a las diversas funciones, actividades y/o tareas que se realizan a través de ellos. Además del acceso a los servicios de telecomunicaciones, entre otros usos principales se encuentran: su uso como herramienta de trabajo; para la búsqueda de información general o especializada; almacenamiento de archivos e información diversa; como punto de acceso a redes sociales; en ocio u entretenimiento; gestión de información personal; manejo de contactos telefónicos; administración de correos electrónicos; así como registro de la actividad financiera, bancaria, ubicación geográfica, intereses diversos o datos biométricos; auxilian en el pago de diferentes servicios; e incluso son útiles para enfrentar emergencias; y demás aplicaciones.

En los últimos años con el afán de mantenerse a la vanguardia, los usuarios tienden a comprar ETM de mayor rendimiento, mejores características y funciones avanzadas, según sus necesidades y/o posibilidades.

Aunado a la disponibilidad en el mercado de esta clase de productos y consecuente acceso a mejores ETM por parte de los usuarios, resulta importante destacar que los poseedores de estos dispositivos, lidian con el riesgo constante del robo de los mismos, derivado que son objetos que despiertan atención por parte de la delincuencia, debido a la existencia del mercado ilegal, dado su precio de reventa y a la facilidad de comercialización a nivel nacional e internacional. Cabe señalar, que un riesgo grave que corren los usuarios al momento del robo del ETM, es el mal uso de la información personal o sensible.

Por lo anterior, es relevante contar con este estudio para identificar prácticas y mecanismos a nivel internacional, así como diagnosticar el marco normativo vigente en México, con la finalidad de coadyuvar a mitigar el robo de los ETM. Dicho estudio podrá tomarse como base para, entre otros, el desarrollo de una disposición administrativa de carácter general o especializada, que regule la implementación de las distintas técnicas que se exponen.

El presente estudio se divide en cinco apartados: el *Contexto general del problema*, en el que se analiza la importancia de los ETM en la sociedad, así como el problema colateral al adquirir uno de ellos, es decir, el robo del equipo móvil y las implicaciones que derivan de este acto ilícito; *Acciones generales a la problemática*, se explica las acciones que se han adoptado para disminuir el robo de los ETM; *Experiencia Internacional* tiene por objetivo mostrar las acciones que se han implementado en otros países y que son comúnmente utilizadas;

Situación actual y medidas tomadas en México se muestra las cifras en diferentes periodos respecto al robo de los **ETM**, así como las acciones y políticas utilizadas en nuestro país; finalmente, en el apartado de *Recomendaciones para disminuir el robo de **ETM***, se proponen diversas acciones que se pudieran implementar de manera convergente para lograr el objetivo de este estudio.

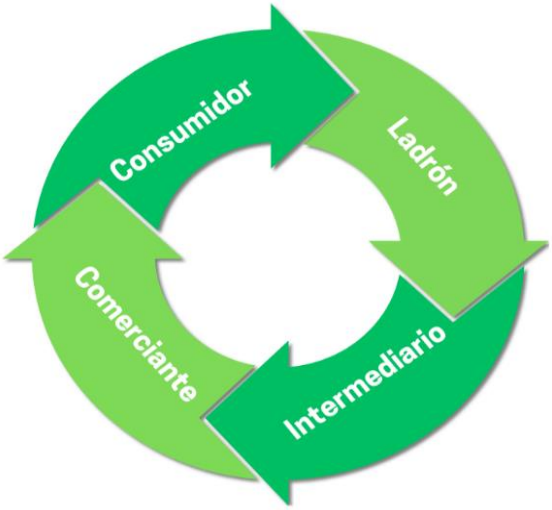
I. Contexto general del problema.

De acuerdo con la Asociación del Sistema Global de Comunicaciones Móviles (en lo sucesivo, "*GSMA*", por sus siglas en inglés), año con año, se registra un aumento considerable en el robo de **ETM** lo que, dada la importancia que tienen, su disponibilidad y la tendencia a un mayor acceso a estos dispositivos, hace necesario crear conciencia sobre la existencia de un mercado ilegal, así como del riesgo que implica la compra de equipos en dicho mercado, desde la perspectiva jurídica, además de dar a conocer las implicaciones técnicas y económicas derivadas de la participación de los usuarios en este acto (GSMA, 2015).

Por otra parte, resulta notorio que el robo de **ETM**, está asociado con el negocio de compra y venta ilegal de los mismos dispositivos, ya que, estos artículos, son comercializados en mercados irregulares, para venderlos a un precio menor al comercial. Por si esto fuera poco, en el caso de que los propietarios bloqueen los **ETM**, los equipos pueden terminar desarmados para su venta por partes, siendo las pantallas y los procesadores las piezas más buscadas, lo que genera beneficios económicos continuos para los delincuentes.

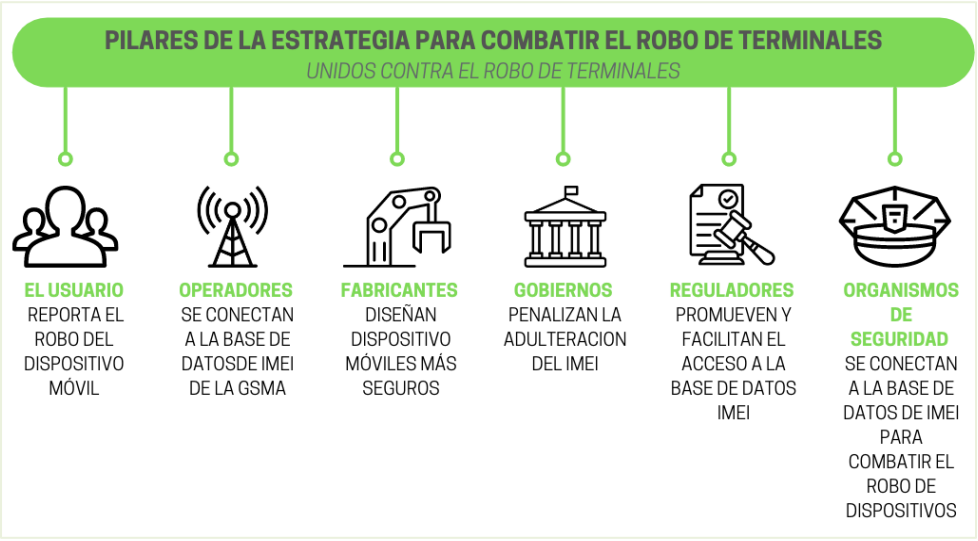
a. Ecosistema de la venta de equipos móviles robados.

Existe un ciclo económico de generación de ingresos que se presenta cada vez que un **ETM** es robado en cualquier parte del mundo. Dicho ciclo consta de tres etapas: en la primera etapa, el ladrón roba el **ETM**; en la segunda etapa, los dispositivos son vendidos a algún intermediario, quien será el encargado de revender los **ETM**; en la tercera etapa, se comercializan de manera ilegal los **ETM** robados directamente a consumidores finales en los países en que les sustrajeron, o donde exista la demanda de ellos y los usuarios paguen por este tipo de dispositivos, lo que resulta en un gran margen de ganancia (Karachi, 2015).



Fuente: Elaboración propia con base en el estudio realizado por el Departamento de Ciencias de la Computación de la Universidad de Karachi (2015), disponible en: https://www.researchgat2e.net/publication/306017525_Economic_Review_and_Street_crime_Analysis_Using_Cell_Phone_Snatching_and_Theft

Ahora bien, conforme a lo señalado por la *GSMA*, para poder atacar el robo de terminales, es necesario abordar el problema de manera coordinada de acuerdo con la responsabilidad que recae en los llamados "pilares", que resultan ser Usuarios, Operadores, Fabricantes, Gobiernos, Reguladores y Organismos de Seguridad (GSMA, 2017).



Fuente: Elaboración propia con base en *Maddison*, disponible en: https://www.gsma.com

Como se observa la imagen anterior, cada pilar debe realizar las acciones correspondientes a su grado de responsabilidad, pero también actuar de manera conjunta para llevar a cabo una implementación efectiva para la disminución del robo de los ETM.

Por ejemplo, dentro de las acciones atribuidas al usuario, se encuentra el reportar al operador móvil el robo del ETM, para que éste, a su vez, proceda a bloquear la línea y evitar su uso. También, se le recomienda al usuario cambiar contraseñas de las cuentas guardadas en el dispositivo hurtado.

Por su parte, los operadores deben avisar a la *GSMA* para mantener actualizada la Base de Datos Central Global, que contiene información básica sobre el Identificador Internacional de Equipo Móvil (en lo sucesivo, "*IMEI, por sus siglas en inglés*") de millones de dispositivos móviles de todo el mundo.

La actividad principal de los fabricantes es centrarse en la seguridad de los ETM, desde un punto de vista técnico y de su diseño. Los dispositivos, ofrecen una gran cantidad de beneficios a los usuarios, no obstante, al estar conectados a Internet se vuelven objetivos deseables para los delincuentes, ya que la información del usuario se vuelve vulnerable. Por lo anterior, los fabricantes de dispositivos móviles deben implementar soluciones de seguridad para contrarrestar amenazas y disminuir riesgos.

A su vez, los gobiernos de diversos países trabajan desde el ámbito de sus atribuciones y conforme a las normas aplicables en cada caso, en la implementación de regulaciones para restringir, desincentivar, o penar la compra y venta de equipos robados, además de las otras conductas antijurídicas que la actividad aglomera.

b. Afectación desde la perspectiva técnico y económica.

Las afectaciones que implica el robo de un ETM se relacionan a los delitos vinculados que se cometen con ayuda de estos dispositivos, así como con la vulneración de la información personal o sensible del usuario y a la afectación económica derivada de comprar un equipo nuevo, ya que los usuarios se ven obligados a gastar de imprevisto, para adquirir un nuevo ETM.

Adicionalmente, existen pérdidas que van más allá de la afectación directa al usuario, también se observa el daño sufrido a los fabricantes, quienes dejan de percibir ingresos por la venta de un equipo legítimo; o el de los distribuidores que se encargan de la venta legal de los dispositivos móviles. Por su lado, a los gobiernos, les afecta en la disminución de ingresos

de importación y/o impuestos de ventas de equipos legítimos, además del costo político, así como social de la pérdida de empleos legales directos e indirectos, con los que se relaciona la actividad comercial.

Según el estudio "*The economic cost of IPR infringement in the smartphones sector",* investigación realizada por la Unión Internacional de Telecomunicaciones (en lo sucesivo, la "*UIT*") y la Oficina de Propiedad Intelectual de la Unión Europea, los teléfonos móviles ilegales, (su comercialización) en todo el mundo, contribuyeron en el año 2015, al 12.9% de pérdidas en ventas para fabricantes y distribuidores legítimos (UIT, 2017 A).

Así, el robo de ETM genera costos derivados de la prevención, el combate, así como de la reparación del daño provocado por este ilícito, debido a los recursos gastados, por ejemplo, en seguridad pública, privada, seguros u otros elementos atenuantes de la actividad o en su defecto, del daño causado.

Por otra parte, el usuario que ha sido víctima de un robo de ETM, además de perder el dispositivo, es decir parte de su patrimonio, también sufre la vulnerabilidad de su información personal, la cual puede ser difundida, vendida o usada para el robo y suplantación de identidad; sufrir acceso sin autorización a cuentas (correo electrónico, bancarias, redes sociales, entre otros); afrontar extorsiones, acosos; e incluso podrían generarle tarjetas de crédito virtuales; o le perjudican ilícitamente de algún otro modo.

Al respecto, de acuerdo con una investigación forense de la empresa *Deloitte* (Deloitte, 2023) existen dos escenarios derivados de los peligros del robo de información de los dispositivos móviles:

Escenario 1: celulares robados, de los cuales 50% contenía la información encriptada y 90% estaban bloqueados con contraseña:

- En el 90% de los casos, fue posible identificar las direcciones de correo electrónico de los dueños.
- En el 75% de los casos, fue posible identificar quien era el dueño.
- En el 75% de los casos, se recuperaron los contactos de los dueños.
- En el 40% de los casos, se recuperaron una variedad de contraseñas.

- En el 25% de los casos, los números de servicio público personal (en lo sucesivo, "*PPS*"), se pudieron identificar ya que estaban almacenados en contactos o en el servicio de mensajes cortos (en lo sucesivo, "*SMS*").

Escenario 2: celulares de segunda mano formateados con la configuración inicial de fábrica, de los cuales 40% de la información estaba encriptada y 0% bloqueados con contraseña:

- En el 70% de los casos, se pudo identificar al dueño.
- En el 85% de los casos, fue posible acceder a los registros de texto y chat.
- En el 60% de los casos, fue posible recuperar contactos.
- En el 60% de los casos, fue posible identificar las direcciones de correo electrónico de los dueños.
- En el 30% de los casos, se recuperaron una variedad de contraseñas.
- En el 15% de los casos, se recuperaron los números de PPS.

Estos resultados podrían implicar, que una vez que se concreta el robo del ETM, los usuarios están expuestos a que se vulnere su información personal y que su uso sea perjudicial para ellos u otros individuos, mediante la comisión de delitos conexos.

Por otra parte, en cuanto a la afectación económica, *TRUSTONIC*, empresa dedicada a ofrecer servicios de ciberseguridad para equipos móviles, señala que tan solo en los Estados Unidos de América se estima que más de cuatro millones de dispositivos de prepago se trafican anualmente, con un costo total de tráfico de prepago de novecientos millones de dólares estadounidenses (Trustonic, 2019). Esa es una pérdida asombrosa de doscientos veinticinco dólares estadounidenses por dispositivo traficado. Además, se debe considerar que estas cifras son solo del segmento prepago en Estados Unidos de América.

Las cifras agregadas a nivel mundial de dispositivos traficados, tanto de los mercados de pospago como de prepago, representan un mayar tráfico ilegal de ETM. Aunado a ello, se estima que el fraude basado en ETM robados, puede tener un impacto anual en los operadores móviles de al menos diez millones de dólares estadounidenses por año, siendo probable que esta sea una cifra conservadora, según sus clientes y prospectos de operadores móviles que les reportan, que la actividad ilegal afecta entre el 5% y el 30% de los ETM que venden (Trustonic, 2019).

Otro ejemplo del impacto económico es aquel señalado por el Instituto Peruano de Economía. El precio de un teléfono móvil de prepago oscila entre 94 y 1,501 dólares estadounidenses[1]. Entre 2015 y 2021 se han sustraído o perdido casi 18 millones de terminales móviles, es decir, más de 7,000 equipos cada día o 2.5 millones de teléfonos al año. Un cálculo simple arroja pérdidas entre 566,834 y 9,017,808 dólares estadounidenses[2] al día, que son asumidas por los usuarios. Por ende, la ciudadanía debe asumir anualmente entre 242 y 3,618 dólares estadounidenses por los teléfonos perdidos, robados o hurtados, que alimentan el enorme mercado informal e ilegal que funciona abiertamente. En Perú las personas que perciben un bajo ingreso mensual tardan entre cuatro y once meses en recuperarse del robo, de sus equipos, mientras que en el resto de los segmentos socioeconómicos toma dos meses o menos (IPE, 2022).

Aunado a lo anterior, se observa que la delincuencia está involucrada en varios niveles y por medio de distintas actividades, como en las siguientes:

- Con el fin de borrar datos personales y restaurar los dispositivos robados, se transportan en grandes cantidades a otros países.
- Se envían a granel **ETM** robados para venderlos en países sin *Listas Negras* de dispositivos.
- La cadena de suministro se ha visto afectada, ya que mientras se transportan del fabricante al almacén y al minorista, los dispositivos son robados.
- Robo en establecimientos minoristas, a veces por parte de personas con información privilegiada donde se preparan los productos para la venta.

En atención a lo anterior, según información de la *GSMA*, los sectores público y privado trabajan en conjunto, así como de manera colaborativa, para evitar la activación de los dispositivos robados, en un intento por frenar el mercado negro, además de contrarrestar los delitos y crímenes vinculados a este fenómeno (GSMA, 2015).

Es así, como en este estudio, se resalta la utilidad de contar con un **ETM**, debido a sus diferentes usos y que son una herramienta para aprovechar los beneficios de la conectividad, no obstante, existen riesgos que se derivan del simple hecho de adquirir un dispositivo móvil. De igual manera, se destaca el mal uso de la información contenida en los **ETM** robados, por lo que se busca reforzar el entendimiento de las implicaciones presentes cuando el usuario

[1] Cifras con tipo de cambio promedio anual 2019 con información del *Banco Central de Reserva del Perú*.
[2] Cifras con tipo de cambio promedio anual 2021 con información del *Banco Central de Reserva del Perú*.

accede a ser partícipe en este acto, es decir; cuando compra un ETM en el mercado ilegal, lo que contribuye a que se genere una afectación social y económica continuada.

Por todo lo anterior, resalta la importancia de buscar con base en las facultades del Instituto Federal de Telecomunicaciones (en adelante, "Instituto", o "IFT"); las medidas, mecanismos, procesos y procedimientos eficientes para contribuir a la disminución del robo de ETM.

PUNTOS CLAVE DEL CAPÍTULO I

- *De acuerdo con la información de la GSMA, existe un aumento considerable del robo de los ETM durante los últimos años, por eso, la importancia de buscar métodos efectivos para su disminución.*
- *Derivado del proceso del robo de ETM, no solo el delincuente resulta ser beneficiado por el hurto de los dispositivos móviles, sino también resultan beneficiados todos aquellos revendedores de los dispositivos a los consumidores finales, por lo que este acto sigue dejando grandes ganancias entre la delincuencia.*
- *El porcentaje de comentar actos ilícitos con la información de los usuarios obtenida de los ETM robados aproximadamente del 90%.*
- *Es sumamente importante el trabajo conjunto de los usuarios, operadores móviles, fabricantes, gobierno, entes reguladores y organismos de seguridad, para lograr métodos más efectivos para la disminución del robo de los ETM.*
- *Se debe alfabetizar a los usuarios, de las consecuencias que implica el adquirir un ETM dentro del mercado ilegal.*
- *Las consecuencias derivadas del robo de ETM implican afectaciones económicas para el usuario, los comercializadores legalmente establecidos, los fabricantes e incluso el gobierno.*

II. Acciones generales a la problemática.

En este capítulo se describen diferentes acciones o mecanismos a través de los cuales los operadores de los servicios móviles, los fabricantes de ETM, los usuarios, entre otros participantes, abordan la problemática del robo de equipos móviles.

a. Asociación Global de Sistemas Móviles de Comunicación-GSMA, Base de datos global (*Lista negra* o *Block List* o *Black List*).

La *GSMA*, creada en 1995, con sede en Londres es una organización global que une al ecosistema móvil para descubrir, desarrollar y ofrecer innovación esencial para entornos comerciales positivos (GSMA, 2023 A).

Asimismo, reúne a operadores y compañías del ecosistema de telecomunicaciones móviles, incluyendo a los fabricantes de dispositivos móviles, empresas de *software* y proveedores de equipos, así como a organizaciones que representan sectores adyacentes de la industria (GSMA, 2016).

La *GSMA,* ofrece a los reguladores del mercado la herramienta denominada *Device Check,* misma que permite a usuarios, recicladores, operadores móviles de red, agencias de seguridad y policía, identificar dispositivos sospechosos.

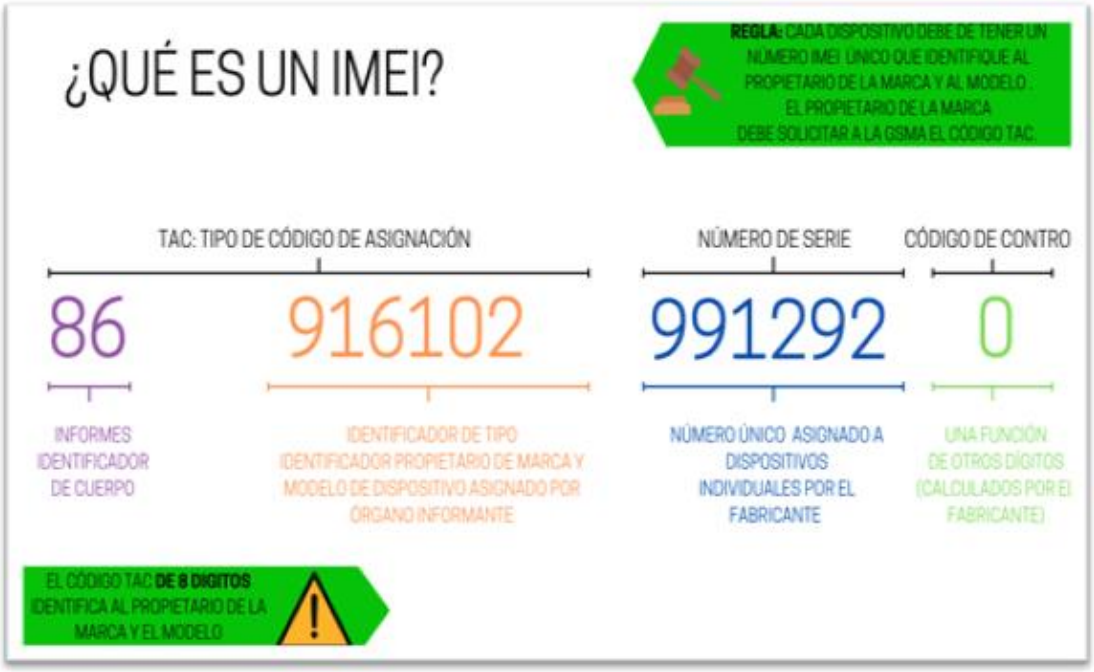
Además, con dicha herramienta, se puede consultar si un dispositivo ha sido reportado como perdido o robado, debido al registro de dispositivos en su base de datos, la cual proporciona hasta 10 años del historial de un equipo a partir de su ingreso a la lista, así como la información de este (marca y modelo). El objetivo de la herramienta *Device Check,* es:

- Ayudar a los revendedores a identificar y eliminar los dispositivos robados antes de que puedan ingresar a las cadenas de suministro;
- Confirmar la autenticidad del modelo real del dispositivo;
- Desalentar el robo de dispositivos al reducir el valor de un dispositivo robado;
- Confirma el operador móvil que denunció el robo o la pérdida del dispositivo, lo que ayuda con el retorno al propietario legítimo (GSMA, 2023 B).

La herramienta *Device Check* consulta la base de datos de los números *IMEI* de los equipos terminales móviles con reporte de robo o extravío. El número *IMEI*, es definido por *GSMA* como

un código de 15 dígitos pregrabado en los ETM, el cual identifica al aparato unívocamente a nivel mundial y es transmitido a la red del operador al conectarse.

Los primeros 8 dígitos del *IMEI* se denominan Código de Asignación de Modelo (en lo sucesivo "*TAC*"), los cuales son asignados por la *GSMA* a los fabricantes, que permiten identificar marca y modelo de cada equipo. Esta información (TAC LIST) está disponible tanto para los operadores móviles como para los reguladores, así como para otras entidades públicas interesadas (GSMA, 2014).



Elaboración propia con base en GSMA, disponible en: https://www.gsma.com/services/wp-content/uploads/2019/05/GSMA-TAC-Allocation-and-IMEI-Training-Module-No.1_Governing-Rules-2.0.pdf

Con el número *IMEI* es posible saber si un ETM ha sido incluido en la lista global de dispositivos móviles robados o extraviados. El objetivo principal del código *IMEI,* es permitir a los operadores identificar los ETM y sus características, es decir; modelo, marca, etc., para bloquear el acceso a la red de los ETM reportados por robo o extravío.

Con base en lo anterior, la *GSMA* crea y administra la *Lista Negra* (*Black List*) ahora conocida como *Block List*, siendo esta, una base de datos que contiene los códigos *IMEI* reportados como extraviados o robados (es la base de datos que consulta la herramienta *Device Check*), además es la acción más empleada para inhabilitar un equipo terminal móvil.

La *Block List,* también se ha utilizado para combatir el tráfico ilegal dentro y fuera de un país, un ejemplo del uso cooperativo entre varios países de esta herramienta en Latinoamérica surge a través de la resolución 189 de la Comisión Interamericana de Telecomunicaciones *CITEL- PCC.I/RES. 189,* en la que los países latinoamericanos acordaron formar un frente contra el robo de dispositivos en la región. Asimismo, a través de la Resolución 786, la Comunidad Andina llamó a los países a establecer un intercambio de información sobre equipos terminales móviles robados y combatir el tráfico ilegal transfronterizo de estos ETM (GSMA, 2014).

b. Unión Internacional de Telecomunicaciones (*UIT*).

La *UIT* señala que para combatir el robo de los ETM alterados (aquellos dispositivos que han sido manipulados alterando características del software, por ejemplo, su número IMEI) y falsificados (aquellos dispositivos que emulan a los originales en hardware y software), primero; se debe contar con un marco jurídico, y segundo; apoyarse con el registro de *IMEI* para identificar terminales móviles auténticos y legalmente importados.

También recomienda, bloquear los dispositivos móviles con números *IMEI* no válidos, es decir; un *IMEI* nulo, es aquel que se encuentra reportado en la base de datos *Block List*; un *IMEI* clonado, que se encuentra replicado en "N" número de dispositivos y; un *IMEI* falsificado, que fue asignado en un equipo por organizaciones no autorizadas.

La *UIT*, en torno a los marcos legales y regulatorios, sugiere aplicar medidas restrictivas contra los dispositivos alterados y falsificados, contemplando los siguientes puntos:

- Limitar la activación de dispositivos de tecnologías de la información y las comunicaciones (en lo sucesivo, "*TIC*") alterados o falsificados en las redes de telecomunicaciones.
- Se debe restringir la importación, circulación, venta de dispositivos y accesorios *TIC* alterados o falsificados, que no cumplan con el marco legislativo y regulatorio del país.
- Crear medidas para que las autoridades y los consumidores puedan distinguir los productos auténticos de los falsificados.
- Se debe disuadir la fabricación de productos falsificados y otros productos ilegales a través de medidas de seguridad.
- Establecer un marco legal contra el cambio de identificadores únicos.
- Debe hacerse la debida referencia a la legislación nacional existente y los marcos regulatorios que ya pueden cubrir ciertos aspectos (UIT, 2019).

En septiembre de 2017 la *UIT*, planteó en el documento **UIT-T X.1127**, la recomendación de los requisitos funcionales de seguridad y la arquitectura funcional para los mecanismos contra el robo de teléfonos inteligentes basados en los requisitos generales descritos por la GSMA (UIT, 2017 B).

Además, la *UIT* a través del documento **Rec. UIT-T Q.5050 (03/2019)**, señala que al conectarse y registrarse por vez primera un **ETM** en la red de un operador, éste envía el código *IMEI* del equipo terminal a la base de datos. El sistema comprueba los códigos *IMEI* indisponibles en la *Lista Blanca*, identifica los dispositivos móviles inválidos y registra los códigos *IMEI* correspondientes en la *Lista Gris*. El propietario del equipo terminal recibe un aviso vía *SMS* y tiene que confirmar el origen legal del equipo terminal, dentro del plazo especificado desde la fecha en que se inscribe en la *Lista Gris*. Adicionalmente, la recomendación **5050** da un marco para tener en cuenta al implementar soluciones para combatir la proliferación y el uso de equipos de telecomunicaciones alterados (UIT, 2019).

Posteriormente, la *UIT* planteó la recomendación **UIT-T Q.5051** del mes de marzo de 2020, que tiene por objeto, describir un marco de referencia a tomar en consideración, para luchar contra la utilización de dispositivos móviles robados, el cual sugiere lo siguiente:

- Deben combinarse diversas actividades y sistemas de información, gestionados por diferentes organizaciones, con el fin de colaborar para controlar, así como, proporcionar información esencial, para identificar y luchar contra el uso de dispositivos móviles extraviados, robados y de aquellos cuyos identificadores no sean válidos.
- Los consumidores y demás partes interesadas deben poder consultar si un cierto dispositivo está afectado por alguna restricción (robado, extraviado o con un identificador no válido).
- La solicitud de bloqueo de un dispositivo robado puede presentarse a través de diferentes instancias (consumidores, fuerzas y cuerpos de seguridad, operadores móviles o directamente en el sistema central).
- Deben adoptarse medidas para la validación de la identidad del usuario y la titularidad del dispositivo, con independencia del lugar donde se haya presentado la solicitud de bloqueo del dispositivo en uso.
- Para los dispositivos que no se hayan vendido a un consumidor, por ejemplo, los robados en tránsito, en los comercios minoristas, etc., la denuncia legal debe venir acompañada de la solicitud de bloqueo del dispositivo.
- Para que sea posible limitar la circulación de dispositivos robados en el mercado, otros organismos nacionales pertinentes (por ejemplo, las fuerzas y cuerpos de seguridad y las administraciones de aduanas), deben tener la capacidad de consultar el estado

de los dispositivos en todas las bases de datos de referencia y fuentes de información disponibles.

- Es indispensable que se pueda intercambiar información con instituciones internacionales, ya sea con carácter bilateral o a través de una base de datos de referencia mundial.
- Para garantizar la eficacia del bloqueo de los dispositivos robados en las redes móviles del país, todos los operadores deben sincronizarse con una base de datos de referencia nacional y mundial.
- Es necesario que la gestión de los identificadores único-fiables se integre con el proceso de bloqueo de móviles robados, ya que es posible que se manipulen los identificadores únicos de ciertos dispositivos, para eludir el proceso de bloqueo.
- Es necesario, implementar un proceso de identificación y control de dispositivos móviles con identificadores no válidos en las redes que se hayan manipulado con posterioridad al bloqueo de los dispositivos robados.

c. Combinación de Listas Blancas y Listas Negras.

En contraste con las *Listas Negras*, que impiden el acceso a las redes de los ETM extraviados o robados, existen las *Listas Blancas (White List),* que constan de una base de datos con los registros de los números *IMEI* autorizados para acceder a las redes de los operadores, las *Listas Blancas* se emplean a nivel nacional y son administradas por los reguladores. Específicamente, las *listas blancas*, también conocidas como "*Listas Positivas"*, buscan resolver el problema de actualización de las *Block List* para capturar el número *IMEI* de los ETM que han sido manipulados en su código o que no son válidos para acceder a la red. (TMG, 2018)

Para ser ingresado en una *Lista Blanca* y así acceder a la red, los ETM deben cumplir ciertos requisitos, como estar registrados por los importadores y por el usuario final, estas acciones delegan mayor responsabilidad a estas dos partes. No obstante, implementar una *Lista Blanca* es más difícil que una negativa, son más complejas y cuestan más, debido a que se tienen que agregar a todos los usuarios que estén registrados, por esta razón el número de registros de equipos móviles de una *Lista Blanca* es superior al de una *Lista Negra*.

A su vez, los números *IMEI* también se emplean para la alimentación de bases de datos de *Listas Grises*, donde se enlista a los ETM cuyo estado carece de confirmación, es decir; no se

encuentran registrados en la *Lista Negra* o *Lista Blanca*. Un ejemplo se da cuando se detecta un *IMEI* clonado en la red de uno o varios operadores.

Por tanto, si se combina el uso de las *Listas Negras* y *Blancas*, se adquiere una mayor efectividad contra el acceso a la red de los **ETM**, que no se encuentren registrados o tengan reporte de robo o extravío.

Generalmente, las *Listas Negras* operan en varios niveles. El primer nivel, consiste en que los consumidores y/o la policía, informen sobre los dispositivos robados a los operadores. El segundo nivel, consiste en que los operadores compartan esta información a la base de datos nacional o con todos los operadores del país. Por último, en el tercer nivel, los operadores sincronizan sus bases de datos con la base de datos global de la *GSMA*. Llevar a cabo esta acción, es gratuita para los miembros de la asociación, y, a menudo, también se otorga acceso a través de una cortesía a los reguladores oficiales.

No obstante, las *Listas Negras* son efectivas cuando su contenido se encuentra actualizado y homologado, lo que garantiza la precisión de la información que contienen, a nivel nacional e internacional.

Al incluir las *Listas Blancas*, los reguladores han ampliado el alcance de las medidas de bloqueo del *IMEI*. A diferencia de las *Listas Negras*, que evitan que los **ETM** marcados como robados o perdidos se conecten a la red, la *Lista Blanca* contiene los dispositivos autorizados para vincularse a redes móviles.

El uso de *Listas Blancas* es el ejemplo de la lucha no solo contra el robo sino también el comercio de equipos terminales móviles alterados o clonados, además de completar las soluciones de la *Lista Negra*.

d. Soluciones antirrobo basadas en el dispositivo (*Kill switch*).

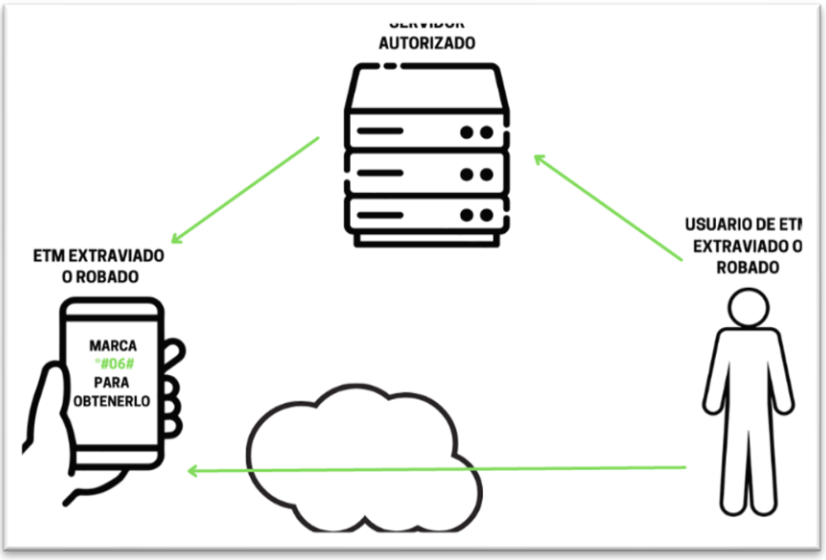
Kill switch es un mecanismo de seguridad desarrollado y empleado por los fabricantes y operadores cuando ocurre un robo o extravío de un **ETM,** que permite al usuario la desactivación de forma remota de este, quitándole la posibilidad del uso de todas sus funciones (incluyendo los relativos a servicios móviles y la navegación en la red de internet a través de *wifi*, así como el uso de cualquier aplicación), dejándolo inhabilitado.

Una de las ventajas del *Kill switch*, es que es de fácil incorporación a través de software, mismo que puede actualizarse a la par. De acuerdo con la recomendación UIT-T X.1127, el *Kill switch* debe ofrecer la capacidad para:

- borrar a distancia los datos personales de usuario que se encuentran en el ETM, en caso de robo o pérdida;
- dejar inoperable un ETM para una persona no autorizada;
- almacenar, en caso de necesidad, los datos personales de usuario en el servidor;
- realizar copia de seguridad, el proceso es gestionado por los operadores de servicio celular o los fabricantes de dispositivos;
- impedir la reactivación sin la autorización del usuario, y
- anular la inutilización cuando el usuario autorizado recupere el ETM y volver a cargar los datos personales en este mismo, en la medida de lo posible desde el servicio de copia de seguridad.

A su vez, existen dos escenarios para iniciar la ejecución de desactivación:

1) Cuando el propietario del dispositivo contacta con el operador de su servicio celular y este ejecuta la operación de desactivación del dispositivo móvil.
2) En el momento en que el propietario del dispositivo ejecuta una aplicación en otro dispositivo móvil o accede a una herramienta de desactivación que deja inoperable el dispositivo móvil perdido/robado.



Kill switch elaboración propia con base en UIT-1127, https://www.itu.int/rec/T-REC-X.1127/es

Además, existen dos tipos de desactivación en el *Kill switch*:

1) **Desactivación dura:** es la inutilización permanente del dispositivo móvil robado.
2) **Desactivación suave:** es la desactivación temporal para que un usuario no autorizado no pueda utilizar el dispositivo móvil hasta que el propietario active el equipo.

Para poder ejecutar los servicios de *Kill switch*, el propietario del dispositivo móvil deberá configurar el **ETM** para permitir las funciones contra el robo.

Asimismo, la *UIT* señala que cuando un teléfono móvil es robado o se pierde, el propietario del dispositivo contacta a su operador celular o utiliza un sitio *Web* administrado por el operador celular, para enviar una instrucción de "desactivación del dispositivo" al dispositivo móvil. La instrucción bloqueará el dispositivo móvil y si lo selecciona el propietario, podrá borrar algunos datos personales del mismo o permitir el almacenamiento de algunos datos personales en el servidor de copia de seguridad.

La instrucción de desactivación del dispositivo provocará que no pueda funcionar en la red de ningún proveedor de servicios móviles comerciales o de servicios de datos móviles comerciales en todo el mundo, incluso si se apaga el dispositivo y se extrae la memoria de almacenamiento de datos. La única manera de reactivar un dispositivo bloqueado será a través de una contraseña proporcionada por el propietario del dispositivo. (UIT, 2017 B)

e. Vinculación *IMSI-IMEI*.

Un **ETM**, se integra por el equipo físico y la tarjeta "*SIM*" por sus siglas en inglés (*Suscriber Identity Module*, en lo sucesivo "*SIM*") denominada como módulo de identificación de usuario, las cuales son intercambiables entre los **ETM**, es decir, el usuario tiene la oportunidad de retirar la tarjeta *SIM* de un **ETM** y colocarla en otro. Las *SIM* contienen un *chip* digital llamado *IMSI* por sus siglas en inglés (*International Mobile Subscriber Identity*, en lo sucesivo "*IMSI*") denominada identidad del usuario para su identificación a nivel internacional (UIT, 2020).

Con base en el *IMSI*, se asigna un número de suscriptor en la estación móvil de la red digital de servicios integrados (en lo sucesivo, "*RDSI*"), que permite a los usuarios acceder a los servicios contratados, mientras que al proveedor le da el control sobre la información requerida para realizar la facturación correspondiente.

Derivado de lo anterior, al insertar la tarjeta *SIM* en un equipo terminal móvil, se vincula el código *IMSI* y el código *IMEI*, es en este momento cuando el proveedor capta la información

del *IMSI* y del *IMEI* identificativo del **ETM**. Por lo que, el proveedor de servicios puede saber qué usuario (nombre) utiliza su red, ubicación, marca y modelo del terminal. (ICONECTIV, 2017)

Cabe resaltar, que también se vincula de manera fija el número *IMSI,* con el número *IMEI*, con el propósito de que, en caso de robo o extravío, se pueda bloquear el **ETM** de tal manera que, aunque se le inserte otra tarjeta *SIM* no funcione, debido a que solo reconocerá al número *IMSI* de la tarjeta *SIM* previamente vinculada. En este caso el bloqueo del dispositivo se logra con una colaboración a nivel nacional con los proveedores del servicio (por parte del número *IMSI*) y a nivel internacional con las bases de datos de *IMEI* bloqueados (*Block List*). La desventaja de este método es que impide la facilidad de intercambiar la tarjeta *SIM* a otro **ETM** sin previa autorización.

A continuación, se presentan las ventajas y desventajas de las acciones que se han implementado para reducir el robo de **ETM**:

Tabla 1 Ventajas y desventajas de *Listas Negras, Listas Blancas, Kill switch* y Vinculación *IMSI-IMEI*.

Listas Negras o Block List	
Ventajas	Desventajas
• Son aceptadas e implementadas a nivel internacional. • Son de fácil implementación porque solo involucran **ETM** que han sido reportados por usuarios. • Son listas homologadas, es decir; existe una coordinación entre países.	• Consumen muchos recursos, porque utilizan información actualizada y certera. • Existen pocas pruebas de su efectividad contra el robo de **ETM**. • Involucra un mayor número de actores, lo que se traduce en un gran esfuerzo para la coordinación entre los países y usuarios, además de lo complicado del mantenimiento de la base de datos. • La delincuencia ha creado opciones para clonar, falsificar y alterar los códigos *IMEI*.

Listas Blancas	
Ventajas	Desventajas
• Son efectivas al combatir los códigos *IMEI* clonados y falsificados. • Se realiza un registro de la mayoría de los usuarios de una región, lo que permite un ecosistema seguro de delitos cometidos con el uso o a través de un **ETM**.	• Depende de gran esfuerzo para la coordinación entre los países, además de lo complicado del mantenimiento de la base de datos. • Depende de la coordinación con los usuarios, lo que genera tiempo y ciertas dificultades para estos. • Emplean gran cantidad de datos, por lo tanto, tiene un alto costo y nivel de complejidad para su mantenimiento, además existe poca evidencia de su efectividad. • Se requiere mayor coordinación para integrarse a una nueva base de datos, es decir; trasladar un **ETM** de un país a otro y este siga operando.

Kill switch o desactivación total	
Ventajas	Desventajas
• Una vez ejecutado, este método bloquea cualquier función del **ETM**. • Resguardan la privacidad del usuario, con la capacidad de eliminar toda la información del **ETM**. • No hay problemas con trasladar los **ETM** de un país a otro. • Es fácil de instalación y operación mediante *software*, además la responsabilidad de la efectividad recae en mayor parte del fabricante y operador del servicio. • No existe costo por mantenimiento de bases de datos.	• Su efectividad depende de la rapidez del usuario al activarlo y de la señal que tenga el **ETM**; por ejemplo, si no hay señal (modo avión) o está apagado. • Únicamente se puede usar en dispositivos inteligentes. • Dependen de características del **ETM** (buena recepción) y el servicio del operador. • No es un mecanismo infalible ya que todo *software* es propenso al *hackeo*.

Vinculación *IMSI-IMEI*	
Ventajas	Desventajas
• Al realizar este vínculo se obtiene una base de datos más completa, el proveedor de servicios puede saber diversa información sobre el dispositivo. • Si se desconoce el número *IMEI* para bloquearlo; el proveedor del servicio lo puede proporcionar.	• En caso de vincular el *IMSI* y el *IMEI* de manera fija, impide la facilidad de intercambiar la tarjeta SIM sin previa autorización, quitando así la portabilidad de la tarjeta *SIM*. • Su aplicación es a nivel local.

f. Servicios de comprobación de dispositivos.

Los servicios de comprobación permiten un mejor desempeño del ecosistema de las redes de dispositivos móviles, su función principal es informar sobre la identidad del **ETM**, es decir la marca, modelo y estatus actual (si se encuentra reportado en la *Block List*).

A nivel mundial se están implementando diferentes servicios de comprobación de dispositivos, estos utilizan para su operación las bases de datos proporcionadas por los operadores y los reguladores, ejemplo de ello se encuentra la plataforma antes mencionada *Device Check* de *GSMA*, la página para verificar el estatus del número *IMEI* dentro del portal del IFT y la página de *CTIA's Stolen Phone Checker* de los Estados Unidos de América., entre otros.

Por su parte, *QUALCOMM* ha desarrollado una plataforma más completa, comparada con aquellas que solo tienen la capacidad de búsqueda en bases de datos, la herramienta de *QUALCOMM* es el sistema de registro y bloqueo de identificación de dispositivos (*Device Identification, Registration, and Blocking System*, en lo sucesivo "*DIRBS*" por sus siglas en inglés), este es implementado a través de una plataforma de *software* que se puede utilizar para detectar dispositivos ilegales y robados en una ubicación especifica. La Plataforma *DIRBS*, consulta la base de datos de *GSMA* y las proporcionadas a nivel local (*listas blancas*), además de las propias que son obtenidas por su apartado de registro; al aprovechar la funcionalidad de registro de dispositivos de la plataforma *DIRBS*, podría usarse en cualquier país para garantizar que los dispositivos falsificados, no certificados o ilegales no se vendan, aunado a lo anterior, detecta códigos *IMEI* no válidos, clonados y falsificados en el ecosistema de telecomunicaciones analizado.

DIRBS se comunica en varios niveles con fabricantes locales, operadores, importadores, aduanas, consumidores, reguladores y la base global de *IMEI* de la *GSMA* (QUALCOMM, 2018).

En este apartado, se ha hecho referencia a las principales herramientas y plataformas que han creado diversas organizaciones involucradas en el desarrollo de las telecomunicaciones, cuyo objetivo es que estas sean de fácil consulta para los usuarios, operadores móviles e incluso gobiernos, con la finalidad de dar a conocer los ETM que han sido reportados como robados o extraviados y así reducir la demanda, el uso o circulación de estos.

Ahora bien, con ayuda de los mecanismos previamente descritos, los gobiernos, fabricantes y operadores combaten el robo de equipos terminales móviles; los países implementan el mecanismo que creen más conveniente complementándolo con su propia normatividad.

Los fabricantes y/o empresas de telecomunicaciones deben implementar un mayor uso de las tecnologías de punta, para desincentivar el robo de ETM, esto incluye el uso de sistemas de bloqueo más eficientes que impidan que los ETM robados sean utilizados por personas no autorizadas o reactivados.

También se observó que, en cada acción para combatir el robo de equipos terminales móviles, se presentan ventajas y desventajas, cabe resaltar que también se pueden combinar estas con la finalidad de obtener un mejor resultado. No obstante, hasta el momento no existe una acción infalible y la elección de una u otra dependerá del contexto de aplicación.

PUNTOS CLAVE DEL CAPÍTULO II

- *La principal función de la herramienta Device Check creada por la GSMA, es identificar los **ETM** robados a través de la consulta del número IMEI, que es el código de 15 dígitos pregrabado en los **ETM**, el cual identifica al aparato a nivel mundial.*
- *La UIT sugiere crear medidas de los **ETM** identificados con IMEI no válidos, es decir; un IMEI nulo, clonado y/o falsificado, entre ellas; recomienda el bloqueo de dichos equipos.*
- *Existe la Lista Blanca (contiene el registro de los IMEI autorizados para acceder a las redes de los operadores), la Lista Negra (contiene el registro de los IMEI reportados como robados) y la Lista Gris (contiene el registro de los IMEI no localizados en la Lista Blanca y Negra).*
- *El Kill switch es un mecanismo que permite al usuario la desactivación de su dispositivo de forma remota, quitándole la posibilidad del uso de todas las funciones, considerando que puede ser una propuesta en México para la disminución del robo de los **ETM**.*
- *La vinculación de manera fija del número IMSI, con el número IMEI, tiene como propósito que, en caso de robo o extravío, se pueda bloquear el **ETM** de tal manera que, aunque se le inserte otra tarjeta SIM no funcione, debido a que solo reconocerá al número IMSI de la tarjeta SIM previamente vinculada.*

III. Experiencia Internacional.

En esta sección, se abordará la experiencia internacional de las acciones tomadas por fabricantes, operadores, reguladores de telecomunicaciones y gobiernos para combatir el robo de equipos terminales móviles.

Es importante recordar que ningún mecanismo contra el robo es cien por ciento efectivo, su efectividad depende del contexto donde se implemente, es decir, la situación social, económica, política y del marco jurídico con el que se cuente.

a. Panorama general y políticas implementadas en Latinoamérica

REGULACIÓN/ ACCIONES	PUNTOS NOTORIOS
ARGENTINA *Ente Nacional de Comunicaciones (ENACOM)*	
Resolución 2459/2016 **(ENACOM, 2016)** a) **Lista Negra**	Base de Datos Negativa (en lo sucesivo, "*BDN*") que contendrá: • *IMEI* de **ETM** con o sin línea telefónica asignada con reporte de robo o extravió. • *IMEI* duplicados detectados por los Prestadores de Servicios de Comunicaciones Móviles (en lo sucesivo, "*PSCM*") dentro de su red. • *IMEI* inválidos detectados por los *PSCM* dentro de su red. • *IMEI* de **ETM** con reporte de robo o extravío descargados de la *BDN* que cursen tráfico en las redes de los *PSCM*.
BOLIVIA *Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes (ATT)*	
Decreto Supremo N° 353 (Gaceta Oficial, 2009) a) **Lista Negra** b) **Lista Blanca**	Se prohíbe la manipulación de *IMEI* y se crearon dos Registros cuya finalidad es proveer información veraz y oportuna que posibilite inhabilitar el servicio en las redes móviles del país, a equipos terminales móviles robados, hurtados o extraviados, así como contribuir a la identificación de los responsables del uso de los servicios de telecomunicaciones móviles en la comisión de delitos. • El Registro de Propiedad de **ETM** que incluye:

	○ Nombre del propietario. ○ Número de documento de identificación personal. ○ *IMEI*. • Y el Registro Nominal de Titulares de Cuenta que contiene: ○ Nombre del titular de cuenta. ○ Número de documento de identificación personal. ○ Número telefónico. Señala que se suspenderá el servicio cuando: • Los **ETM** no hayan sido registrados por sus propietarios en el plazo establecido. • Cuando los números de cuenta no hayan sido registrados por sus titulares en el plazo establecido. • Cuando los propietarios de **ETM**, soliciten la suspensión del servicio por robo o extravío. • Cuando los números de cuenta utilicen equipos terminales móviles denunciados como robados o extraviados. • Cuando los números de cuenta utilicen equipos terminales móviles con *IMEI* repetido.
Verificación IMEI (ATT, 2009) c) **Servicios de comprobación**	Esta herramienta web, es un servicio de información gratuito que permite consultar si el *IMEI* que identifica a un **ETM**, se encuentra reportado (robado o extraviado) por los operadores de telecomunicaciones, o si ha sido liberado (desbloqueado al haberse recuperado). La información desplegada por la herramienta web al hacer la consulta es actualizada 24 horas después de haber sido reportado el **ETM** como robado o extraviado por el titular propietario ante el operador del servicio móvil.
COLOMBIA *Comisión de Regulación de Comunicaciones (CRC)*	
Resolución 3066 (CRC, 2011 A) y	Los proveedores que ofrecen servicios de telefonía móvil están obligados a mantener actualizada una base de datos operativa negativa de los **ETM** que hayan sido reportados como hurtados o

Resolución 3128 (CRC, 2011 B) a) Lista Negra	extraviados, en la cual se indicará la identificación completa de tales equipos (*IMEI*), los datos del usuario que celebró el contrato que originó el reporte y la fecha y hora en que se produjo el hurto o extravío del equipo. Además, dichos proveedores deberán mantener actualizada una base datos positiva en la que se incorporarán todos los *IMEI* con el (los) nombre (s) y apellido (s), dirección, teléfono de contacto y tipo de documento de identidad con el respectivo número de identificación del propietario del equipo o del propietario autorizado por éste. A su vez los proveedores deberán implementar a su costo y bajo la administración de un tercero una base de datos centralizada y cuando se encuentre un *IMEI* duplicado en la red, el proveedor respectivo procederá con la suspensión de los servicios de telefonía móvil.
Ley 1453 – Sanciones modificación ETM (Código Penal, 2011)	Se introdujo la siguiente modificación en el artículo 105 *"El que manipule, reprograme, remarque o modifique los terminales móviles de los servicios de comunicaciones en cualquiera de sus componentes, con el fin de alterar las bases de datos positivas y negativas que se crearán para el efecto y que administrará la entidad regulatoria correspondiente, incurrirá en prisión de seis (6) a ocho (8) años y multa de seis (6) a setecientos (700) salarios mínimos mensuales legales vigentes."*
Sistema de Registro de Terminal Móvil (SRTM) (Inetum, 2011) b) Servicios de comprobación	El *SRTM* habilita la consulta de *IMEI* en la base de datos negativa para dar cumplimiento a la Resolución 3128 de 2011 en su artículo 4.14, expedida por la *CRC*, señalando lo siguiente: "Suministrar las herramientas e interfaces adecuadas para la realización de consultas en línea, registro a registro, por parte del Ministerio de Tecnologías de la Información y las Comunicaciones, la *CRC* y demás organismos autorizados para acceder a la Base de Datos Administrativa (*BDA*). Así como, poner a disposición del público una consulta para conocer si un equipo se encuentra reportado en la Base de Datos Negativa" habilitada en Colombia, y por lo tanto ha sido bloqueado para uso en las redes del país, así como la causal de dicho bloqueo.

Resolución 4813 (CRC, 2015) c) Lista Blanca	Se establecieron medidas de identificación de *ETM* dentro de la estrategia nacional contra el hurto de equipos terminales en la que se definieron tres etapas a fin de controlar los *IMEI*, las cuales serían: 1) validación y diagnostico preliminar (identificación, registro y análisis de *IMEI* duplicados, inválidos, no registrados en la Base de Datos Positiva o no homologados), 2) verificación centralizada (procesamiento y análisis diario de la información de identificación de ETM llevándose a cabo en 3 fases, implementación, pruebas y operación a fin de clasificar los *IMEI* en grupos según su estado) y 3) control (actividades a realizar para la depuración de *IMEI* de ETM que no cumplan con los requisitos previos para seguir operando en la red).
Ley 1801 – Sanciones relacionadas con los delitos de robo ETM (Código Penal, 2016)	Se añadió el Capítulo IV "De la seguridad de los equipos terminales móviles y/o tarjetas *SIM Card*", que contempla sanciones para las siguientes conductas: • Comprar, alquilar o usar un ETM hurtado, extraviado o cuyo número de identificación físico o electrónico haya sido alterado; • Comercializar ETM sin la autorización del Ministerio de Tecnologías de la Información y las Comunicaciones o por un proveedor de redes; • Tener, poseer y almacenar tarjetas madre o *blackboard* de forma ilícita; • Distribuir, almacenar, transportar u ofrecer al público ETM robados o extraviados y ETM o tarjetas madre cuyo número de identificación físico o electrónico haya sido alterado; • Vender, alquilar, aceptar, permitir o tolerar la venta, almacenamiento o bodegaje de ETM de origen ilícito o sin comprobante de importación; • Incumplir las condiciones, requisitos u obligaciones para la importación; • No solicitar o no realizar el registro individual del ETM con su *IMEI*; • No enviar, transmitir, o registrar en la manera y tiempos previstos, la información sobre la importación del ETM; • Alterar, manipular, borrar o copiar sin autorización el *IMEI*;

	• Reprogramar, remarcar, modificar o suprimir el número de identificación físico o electrónico del **ETM**; • Activar líneas telefónicas sin que el usuario haya suministrado al prestador del servicio, los datos biográficos en el momento de la activación; • Activar *SIM Card* (*IMSI*) sin que el usuario haya suministrado al prestador del servicio, los datos biográficos en el momento de la activación.
Proyecto de ley (Velasco Chaves, 2021) d) **Kill switch**	Se pretende establecer la obligatoriedad que todos los **ETM** que se importen o vendan en el país incluyan de fábrica una opción tecnológica que inutilice el dispositivo cuando no esté en posesión del propietario. (Por dirimir).
CHILE *Ministerio de Transporte y Telecomunicaciones (MTT)*	
Decreto 157 (MTT, 2011) a) **Lista Negra**	Se publicó el procedimiento que regula el bloqueo de **ETM** robados y extraviados, en el que obligan a las concesionarias de telefonía móvil a habilitar un número telefónico funcionando las 24 horas del día para que los suscriptores y usuarios puedan realizar llamadas a fin de suspender los servicios provistos por la red móvil y bloquear los equipos reportados, así como la *SIM Card* y posteriormente las concesionarias deberán enviar al Organismo Administrador de la Portabilidad y deberán compartir entre concesionarias, la siguiente información: a) Fecha y hora de la comunicación del robo o extravío, por parte del suscriptor o usuario y, en su caso, fecha de la denuncia de robo o extravío. b) Marca, modelo, tecnología, número de *SIM Card* o su equivalente, si procediera, y número de serie del equipo robado o extraviado.
Resolución 1068 Exenta – Condiciones bloqueo ETM	Se dio la facultad a las concesionarias de bloquear **ETM** en los siguientes casos:

(MTT, 2013)	• Por solicitud expresa del dueño del equipo terminal móvil, propiedad que debe ser acreditada ante las concesionarias de acuerdo con la normativa vigente; • En caso de robo o extravío del **ETM**, cuyo procedimiento de bloqueo se rige por lo establecido en el decreto; • En casos en que el suscriptor o usuario se encuentre en mora en el pago de los acuerdos previamente establecidos respecto del equipo terminal móvil; • En caso de robo de uno o más equipos terminales móviles en forma previa a su comercialización a un usuario o suscriptor y/o en forma previa a la activación del equipo terminal móvil respectivo en la red de un operador, se requerirá que quien solicite el bloqueo de éste se identifique señalando el nombre, número de cédula de identidad y domicilio del titular o representante, así como la razón social, Rol Único Tributario (*RUT*) y domicilio, de la persona jurídica de que se trate, según corresponda; que exista una solicitud expresa del dueño de tales equipos; que éste acredite la propiedad sobre los mismos ante las concesionarias, de acuerdo a la normativa vigente; que, tratándose de una persona jurídica, acredite, además, la personalidad o representación jurídica de esta última; y que acredite haber efectuado la denuncia por el robo ante las policías, el Ministerio Público o los tribunales con competencia criminal.
Resolución 1463 Exenta (MTT, 2016) b) **Lista Blanca**	Se incluyó un Protocolo Básico de Homologación de cada modelo de los distintos **ETM** y una vez verificada la correspondencia de aquellos equipos con el modelo homologado, podrán ingresar al circuito de distribución comercial correspondiente y se deberá conformar y mantener actualizada una base de datos única y centralizada con la información del número *IMEI* de cada uno de los equipos que hayan sido validados incluyendo el *IMSI* y el *RDSI* de todos los **ETM**, así como los siguientes datos: o Tipo de dispositivo: Teléfono, Modem, otro (especificar). o Marca. o Modelo Técnico. o Modelo Comercial.

	○ Versión de *Hardware*. ○ Tipo de Sistema Operativo. ○ Versión de Sistema Operativo. ○ Versión de *Software* de personalización del fabricante. ○ Versión de *Software* de personalización de la concesionaria. ○ Empresa solicitante de la homologación. ○ Inscripción Administrativa: Sí/No. ○ Empresa Certificadora que realiza la homologación. ○ Fecha de homologación. ○ *IMEI*. ○ Clasificación de la Homologación, entendiéndose por tal el código representativo de aquella característica del terminal que permita la utilización del mismo de modo transversal en todas las redes del país, según la tecnología y equipo respectivos, y el cual corresponderá a: 1) soporte sólo 2G; 2) soporte sólo 3G; 3) soporte sólo 4G; 4) soporte 3G e inferiores; 5) soporte 4G e inferiores; 6) soporte 4G y 3G, sin soporte de 2G; 7) soporte 4G y 2G, sin soporte de 3G; 8) No soporta todas las bandas para ninguna tecnología, aplicable únicamente para homologación administrativa. Podrán definirse otros códigos en el futuro en la medida que ingresen al país nuevas tecnologías. ○ Estado cumplimiento apto Sistema de Alerta de Emergencia (*SAE*): Sí/No ○ Fecha de inscripción en la base de datos. ○ Nombre empresa certificadora que inscribe en la base de datos. ○ Dispone de servicio de radiodifusión: SI/NO/NA (Sin Información).
PERÚ *Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL)*	
Decreto Legislativo 1338 (OSIPTEL, 2016) a) **Lista Negra** b) **Lista Blanca**	Se creó el Registro Nacional de Equipos Terminales Móviles para la Seguridad (en lo sucesivo, "*RENTESEG*"), orientado a la prevención y combate del comercio ilegal de **ETM** y al fortalecimiento de la seguridad ciudadana, *OSIPTEL* es el encargado de implementar y

Vinculación IMSI-IMEI	administrar el *RENTESEG*, requerir información a entidades públicas o privadas para incorporar **ETM** en la lista blanca o lista negra, así como supervisar el cumplimiento de obligaciones, requerir a operadoras de servicios la suspensión temporal de las líneas y el bloqueo del *IMEI* detectado como clonado, alterado, nulo o que no se encuentre la lista blanca y por último sancionar a las operadoras por incumplimiento. De igual forma, el Ministerio del Interior puede solicitar al *OSIPTEL* información de los **ETM** que resulten necesarias para el cumplimiento de sus funciones respecto a la seguridad ciudadana contra la criminalidad, también podrá acceder y analizar la información contenida en el *RENTESEG*. El *RENTESEG* contiene la información de la *Lista Blanca* y la *Lista Negra*, sólo se encuentran habilitados para operar en la red del servicio público móvil de telecomunicaciones los equipos terminales móviles importados legalmente e incorporados en la *Lista Blanca*. Se incorporan a la *Lista Negra* los equipos terminales móviles reportados como perdidos, sustraídos e inoperativos; y que, por lo tanto, se encuentran inhabilitados para operar en la red del servicio público móvil de telecomunicaciones. La reincorporación de los **ETM** a la *Lista Blanca* implica su retiro o baja de la *Lista Negra*. Sólo se pueden activar en un **ETM** los *IMSI* cuya identidad del abonado coincida con la identidad del abonado que tenga registrado dicho equipo terminal móvil. Para efectos del *RENTESEG*, se considera usuario registrado de un equipo terminal móvil al titular de la *IMSI* que active por primera vez dicho equipo terminal. Para activar el *IMSI* en un **ETM** que ha sido objeto de transferencia, el usuario registrado se desvincula previamente de la titularidad del *IMEI*. No se puede brindar servicio público móvil de telecomunicaciones en dos o más equipos terminales móviles que tengan el mismo *IMEI*.
Decreto Supremo 009-2017-IN – Normas complementarias para el registro de	Se publicaron las normas complementarias para la implementación del **RENTESEG** en la que incluye la forma en la que los concesionarios entregan la información del registro de abonados y los datos que contiene: nombre del abonado, *IMSI*, modalidad de contrato, *IMEI*, fecha y hora de activación del servicio, marca, modelo del **ETM**, etc.

ETM y usuarios (OSIPTEL, 2017)	Aunado al anterior, también existe un registro de ETM importados, información correspondiente a la lista negra de ETM sustraídos, perdidos y recuperados en Perú y en otros países con los que Perú tiene acuerdos internacionales, ETM inoperativos, ETM devueltos, ETM exportados, ETM que no cumplen con el intercambio seguro y tienen un *IMEI* alterado, condiciones para bloquear y desbloquear un ETM.
Consulta de equipos celulares robados, perdidos o recuperados (OSIPTEL, 2019) c) Servicios de comprobación	Dicho aplicativo permite consultar si el *IMEI* se encuentra registrado como robado, perdido o si ha sido desbloqueado al haberse recuperado. Dentro de los ETM bloqueados se encuentran: • *IMEI* inválido: *IMEI* cuyo código no aparece en la lista de la GSMA. Aquí también están considerados los celulares con *IMEI* incompleto. • *IMEI* alterado: código que no coincide con el otorgado por el fabricante. • Equipo falsificado: son equipos adquiridos legalmente, pero cuyos *IMEI* no se encuentran registrados en la *GSMA*. Estos celulares se encuentran prohibidos en el Perú y representan menos del 1% del total de equipos que se bloquearon.
PARAGUAY *Comisión Nacional de Telecomunicaciones (CONATEL)*	
Ley 5629 (Congreso de la Nación, 2016) a) Lista Negra	Se estableció la obligación de que los proveedores de servicio deberán proceder al registro, y bloqueo del *IMEI* del ETM denunciado, independientemente de que el ETM haya sido adquirido de la misma empresa o de otras empresas comerciales.
Resolución 647/2017 - normas complementarias para registro ETM robados (CONATEL, 2017 A)	Se publicaron condiciones que permitan disponer de un sistema de registro de ETM, así como normas complementarias en las que los prestadores de servicio están obligados a registrar el *IMEI* de ETM denunciados como robados o extraviados, también tienen prohibido activar en su red los ETM con *IMEI* asentado en el Registro Nacional de ETM bloqueados y cada 30 minutos actualizan el

	registro. A su vez se definieron los datos a registrar por los Prestadores de Servicio en la solicitud de bloqueo:
	• Datos de la Solicitud.
	  o Número de solicitud de bloqueo.
	  o Nombre y apellido del solicitante.
	  o Número de documento de identidad del solicitante.
	  o Fecha y hora de la solicitud de bloqueo.
	• Datos de la Denuncia.
	  o Nombre y apellido del denunciante.
	  o Número de documento de identidad del denunciante.
	  o Fecha de la denuncia policial.
	  o Motivo de la denuncia policial (robo o extravío).
	  o Tipo de **ETM** (marca y modelo).
	  o *IMEI*.
	  o Ubicación del evento.
	• Datos del Cliente.
	  o Número de línea telefónica asociado.
	  o Nombre y apellido del titular de la línea telefónica.
	  o Número de documento de identidad del titular de la línea telefónica.
	  o Domicilio del titular de la línea telefónica.
	• Datos del Prestador.
	  o Nombre del Prestador.
	  o Nombre y apellido del agente del Prestador que recibe la solicitud.
	Se pueden realizar diferentes consultas o registros dependiendo quien las realice (usuario, prestador del servicio, gobierno o regulador).

Registro Nacional de Equipos Terminales Móviles Bloqueados (REMOB) (CONATEL, 2017 B) b) **Servicios de comprobación**	Este portal público permite la consulta para ver si un *IMEI* corresponde a un **ETM** que se encuentra denunciado como robado o extraviado, en el país.

ECUADOR *Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL)* *antes Comisión Nacional de Telecomunicaciones (CONATEL)*	
Resolución 191-07-CONATEL-2009 (CONATEL, 2009 A) a) *Lista Negra* b) *Lista Blanca* c) Vinculación IMSI – IMEI	Se creó el Procedimiento para el Empadronamiento de Abonados del Servicio Móvil Avanzado (en lo sucesivo, "*SMA*") y registro de teléfonos perdidos o robados. Los operadores de *SMA* recaban de los abonados la siguiente información: nombres y apellidos, número de cédula de identidad o ciudadanía o pasaporte cuando se trate de extranjeros, profesión o actividad y dirección domiciliaria) para el caso de personas física, y para el caso de personas morales, razón social o denominación, actividad empresarial, número de Registro Único de Contribuyentes (*RUC*) y dirección, vinculados con los números identificadores del equipo terminal telefónico y de línea de abonado; con fines de garantizar la protección de sus datos personales y seguridad pública, a su vez vinculan los datos consignados por el abonado, con el (los) número(s) telefónico(s) y con el código *IMEI* o número serial del equipo en el momento de la activación del servicio y con el número de *SIM Card* según corresponda de acuerdo a la tecnología comercializada y los abonados tienen la obligación de consignar cualquier cambio a sus datos personales y de *IMEI*, de ser el caso. También los operadores cuentan con un sistema para recepción y registro de reporte de los abonados por robo o pérdida de **ETM**, que permita al operador suspender de forma inmediata el servicio y a su vez bloquear el terminal y el *chip* reportado y mantendrán actualizadas diariamente las listas de teléfonos reportados como perdidos o robados. Esta base de datos es intercambiada entre éstas y quedará a disposición de la Policía Nacional u Autoridad Competente, cuando así lo requiera, previo cumplimiento de los requisitos y procedimientos de Ley.
Resolución TEL-535-18-CONATEL-2012 – Normas complementarias	La Norma que regula el Procedimiento para el Empadronamiento de Abonados/Clientes del *SMA* y registro de terminales perdidos o robados, añadiendo un capítulo denominado Comercialización y Activación de Equipos Terminales así como artículos que hacen referencia a la creación de Base de datos de listas positivas, así

para el registro de ETM (CONATEL, 2012)	como el mantenimiento de las listas negativas cuya creación, coordinación y operatividad será centralizada, y se implementará y operará por medio de un Administrador de Base de Datos de Listas Positivas y Negativas (en lo sucesivo, "*ABO*"), el cual será seleccionado y contratado por los prestadores del *SMA*. Las bases de datos de listas positivas y negativas bajo gestión del *ABO*, permite 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. La base de datos de listas positivas contiene la información de los ETM: • En modalidad prepago y pospago; • Importados por los operadores del SMA u otros importadores legalmente autorizados; • Aquellos que los prestadores del *SMA* ofrezcan para venta al público de manera directa o a través de sus canales de distribución, previo a su comercialización; • Aquellos que se encuentren para comercialización al público en los diferentes centros de expendio, distribución o venta previo a su comercialización: • Ensamblados o fabricados en el país; • Adquiridos en el exterior con fines de consumo que ingresen al país por arribos internacionales o fronteras, así como terminales nuevos o usados adquiridos a través de intercambio, regalo o cesión, previo a realizar la activación de dicho equipo, los abonados/clientes deberán acudir a los puntos de venta y activación autorizados o implementados por los prestadores del *SMA* y presentar la documentación legal que demuestre la adquisición lícita de los mismos; • Aquellos que sean liberados de la lista negativa por solicitud y autorización de su propietario.

Resolución 03-03-ARCOTEL-2017 (ARCOTEL, 2017 A)	Se expidió el Reglamento para Homologación y Certificación de Equipos Terminales de Telecomunicaciones y en él los prestadores de servicios de telecomunicaciones, no podrán implementar mecanismos o formas de bloqueo que impidan que equipos homologados que hayan sido utilizados u operados en su red, puedan ser puestos en operación en redes de otros prestadores de servicios de telecomunicaciones, o implementar mecanismos o formas de bloqueo que impidan que equipos homologados que hayan sido utilizados u operados en otras redes, puedan ser puestos en operación en su red; excepto en los casos de equipos terminales cuyo certificado ha sido revocado conforme el reglamento o se encuentren reportados como robados o perdidos y en ambos casos debidamente autorizado por la *ARCOTEL*.
Tu Celular Legal (ARCOTEL, 2017 B) a) Servicios de comprobación	Es una herramienta que ayuda a verificar que la marca y modelo del teléfono celular se encuentre homologado y además se puede saber si el teléfono celular no ha sido reportado como robado, perdido o hurtado. En caso contrario no podrá ser utilizado en el país.
COSTA RICA *SuperIntendencia de Telecomunicaciones (SUTEL)*	
Resolución RCS-234-2020 (SUTEL, 2020) a) Lista Negra b) Lista Gris c) Lista Blanca	La resolución en comento, se refiere a las disposiciones y aspectos operativos para la implementación del Sistema de Gestión de Terminales Móviles (*SGTM*), el cual permite identificar terminales con *IMEI* ilícitos, detectar dispositivos falsificados, incluyendo clones; almacenando y analizando, al menos los datos de operador como *IMSI*, *IMEI*, fecha, hora y *Cell-ID* (identificador que permite saber a qué *radiobase* está conectado un **ETM**), lo anterior para promover un intercambio de las bases de datos entre operadores y proveedores de telefonía móvil. La Entidad de Referencia de Terminales Móviles (*ERTM*), es la empresa determinada por el órgano regulador, encargada de: • Implementar, generar, administrar, mantener e integrar una base de datos centralizada de *Listas Blancas, Listas Grises y Listas Negras.*

	• 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. • Garantizar el registro anónimo de la información que se almacene en sus bases de datos. • Descartar los insumos de información que no determinen a un *IMEI* duplicado. • Proporcionar los mecanismos que permiten asegurar el bloqueo *IMEI* reportados como robados o extraviados, así como los procedimientos para la detección y gestión *IMEI* irregulares.
Plataforma de Validación de Celulares (PVC) (SUTEL, 2022) d) Servicios de comprobación	*PVC* es un sistema el cual detecta e impide la conexión de celulares irregulares o adulterados a las redes móviles de los operadores prestadores de los servicios móviles en Costa Rica. A la página de consulta solo se puede acceder estando en Costa Rica a través del siguiente enlace: https://pvc.sutel.go.cr/, ahí el usuario podrá conocer la condición en la que se encuentra un *IMEI,* arrojando una de las siguientes tres opciones: • Válido: Tendrá acceso a las redes móviles. • Duplicado: Existe otro dispositivo con el mismo *IMEI* y podría ser bloqueado. • Adulterado: Es un celular irregular que no podrá conectarse a las redes móviles.

b. Panorama general y políticas implementadas Estados Unidos de América.

ESTADOS UNIDOS DE AMÉRICA *Federal Communications Commission (FCC)*	
REGULACIÓN/ ACCIONES	PUNTOS NOTABLES
Ley S.1070 - Mobile Device Theft Deterrence Act (Congreso, 2013)	Se decretó que, es ilegal alterar o eliminar el número *IMEI* de un **ETM** por lo que resulta estrictamente prohibido eliminar, borrar, alterar el número de identificación; o usar, producir, traficar, tener control, custodia, o poseer *hardware* o *software*, a sabiendas de que ha sido configurado para lograr modificar o alterar el *IMEI* y de incumplir será acreedor a una multa y en su caso 5 años de cárcel.
H.R.4065 - Smartphone Theft Prevention Act (Congreso, 2014) *a) Kill switch*	Se exigió a los proveedores de servicios móviles y a los fabricantes de dispositivos móviles que brinden a los consumidores la capacidad de eliminar datos de forma remota de los dispositivos móviles y dejar dichos dispositivos inoperables. Un proveedor de servicio móvil o servicio de datos móvil pondrá a disposición en un dispositivo **ETM**, una función que solo puede ser utilizado por el titular de la cuenta y que incluye la capacidad de eliminar remotamente o hacer inaccesible desde el dispositivo, toda la información almacenada relacionada con el titular de la cuenta ; hacer que el dispositivo deje de funcionar en la red de cualquier proveedor de servicio móvil comercial o servicio de datos móvil comercial a nivel mundial, incluso si el dispositivo está apagado o se le ha quitado el medio de almacenamiento de datos; evitar que el dispositivo sea reactivado o reprogramado sin un código de acceso o autorización similar después de que el dispositivo haya sido inoperable o sujeto a un restablecimiento de fábrica no autorizado; y se pueda revertir cualquier acción si el titular de la cuenta recupera el dispositivo(*CTIA*, 2015). Después de julio de 2015, los nuevos modelos de **ETM** fabricados para la venta minorista en los Estados Unidos de América ofrecen, sin costo alguno para los consumidores, una herramienta básica

	antirrobo precargada o descargable en los teléfonos inteligentes inalámbricos, la aplicación permite lo siguiente: • Borrar de forma remota los datos del usuario autorizado (es decir, borrar la información personal que se agrega después de la compra, como contactos, fotos, correos electrónicos, etc.) que se encuentran en el teléfono inteligente en caso de pérdida o robo. • Hacer que el ETM quede inoperable para un usuario no autorizado (p. ej., bloquear el teléfono inteligente para que no se pueda usar sin una contraseña o *PIN*), excepto y de conformidad con las normas de la *FCC* para comunicaciones de emergencia al 911 y los números de emergencia programados por el usuario autorizado. • Impedir la reactivación sin el permiso del usuario autorizado (incluidos los intentos de restablecimiento de fábrica no autorizados) en la medida de lo posible desde el punto de vista tecnológico. • Revertir la inoperabilidad si el usuario autorizado recupera el teléfono inteligente y restaurar los datos del usuario en el ETM en la medida de lo posible.
Ley de prevención del robo de teléfonos móviles de 2016 (Congreso, 2016) b) Delito tipificado	Modifica la Ley de Comunicaciones de 1934 para prohibir a los proveedores comerciales de servicios móviles o de datos brindar servicios en teléfonos inteligentes que: 1) hayan sido reportados a dicho proveedor como robados por un usuario autorizado, o 2) estén listados como robados en la Registro Central de Identidades de Equipos (CEIR). Cuando se denuncia el robo de un teléfono inteligente a un proveedor de servicios, el proveedor debe notificar al CEIR la información necesaria para identificar el teléfono. Los teléfonos inteligentes deben estar equipados con: 1) funcionalidad antirrobo precargada sin costo adicional para los compradores, o ser capaces de descargar dicha funcionalidad sin costo; y 2) un número de identificación de dispositivo móvil.

Stolen Phone Checker (CTIA, 2017) c) Servicios de Comprobación	Se puso en marcha la página "*Stolen Phone Checker*" la cual es un servicio público que tiene acceso a distintas bases de datos incluida la de la *GSMA Device Check*, cuyo propósito es limitar la reventa de dispositivos móviles perdidos o robados en los Estados Unidos de América, a través del cual se puede saber si un dispositivo móvil ha sido reportado como perdido o robado antes de realizar una compra.

c. Panorama general y políticas implementadas Europa

REGULACIÓN/ ACCIONES	PUNTOS NOTABLES
REINO UNIDO *Office of Communications (OFCOM)*	
Mobile Telephones (Re-programming) Act 2002 – Sanciona los delitos relacionados con el robo de ETM (UK Legislation, 2002)	En 2002, Reino Unido emitió la "Ley sobre la reprogramación de teléfonos móviles", la cual señala que una persona está cometiendo delito si cambia, ofrece o interfiere con el funcionamiento de los *IMEI*, así como poseer o suministrar cualquier objeto que pueda utilizarse para cambiar o interferir en el funcionamiento de cualquier *IMEI*. Los responsables de estas actividades serán acreedores de una pena mínima de 6 meses a 5 años en prisión, o una multa monetaria, o ambas. Por lo anterior, contar con equipo o cualquier herramienta con fines de reprogramación se considera delito.
GRECIA Ethniki Epitropi Tilepikoinonion kai Tachydromeion (EETT)	
Deactivation of stolen mobile phones through IMEI (EETT, 2014) a) Lista Negra	Los operadores de telefonía móvil tienen la obligación de bloquear a través del código *IMEI* todos los ETM que se hayan declarado como robados. Los suscriptores deben notificar el código *IMEI* del dispositivo robado al proveedor.

	La empresa que inhabilita un dispositivo robado dentro de su red asume la responsabilidad de informar a los demás operadores móviles, quienes posteriormente también deberán deshabilitar el dispositivo robado en sus redes.
FRANCIA Autorité de Régulation des Communications Électroniques (ARCEP)	
Article L34-3 (France Legislation, 2011) a) Lista Negra	Los operadores, que exploten una red de comunicaciones radioeléctricas abierta al público o que presten servicios de radiocomunicaciones al público, están obligados a prohibir, con excepción de los números de emergencia, el acceso a sus redes o a sus servicios de comunicaciones enviadas a través de terminales móviles, identificados o que hayan sido declarados robados. Estos terminales deberán ser bloqueadas por parte del operador dentro de los cuatro días hábiles siguientes a la recepción de la declaración oficial de robo, emitida por los servicios de policía.

d. Acciones más utilizadas a nivel internacional

A continuación, se muestra una tabla en la que se observan las acciones implementadas por los países señalados anteriormente, a manera de resumen:

Tabla 2: Acciones implementadas a nivel internacional

País	*Lista Negra*	*Lista Blanca*	*Lista Gris*	*Servicios de comprobación*	*Vinculación IMSI-IMEI*	*Kill switch*	*Delito tipificado*
Argentina	✔						
Bolivia	✔	✔		✔			
Colombia	✔	✔		✔			✔
Chile	✔	✔					
Perú	✔	✔		✔	✔		
Paraguay	✔			✔			
Ecuador	✔	✔		✔	✔		

Costa Rica	✔	✔	✔	✔			
USA	✔			✔		✔	✔
Reino Unido							✔
Grecia	✔						
Francia	✔						

En el cuadro se observa que la acción más utilizada a nivel internacional para combatir el robo de ETM es el uso de *Listas Negras,* que en la mayoría de los países trabajan en conjunto con un *Servicio de comprobación* para impedir que se conecte a las redes de los operadores móviles; la segunda más usada son las *Listas Blancas* mismas que son implementadas como complemento a las *Listas Negras* a fin de solo darle acceso a la red de telefonía móvil a los ETM que además de no estar en la *Lista Negra,* han sido registrados con el fin de comprobar que es auténtico y legítimo y si esto aún no fuera suficiente, se ha usado una tercera estrategia, la cual es vincular el *IMSI* de la *SIM* junto con el *IMEI* del ETM para evitar que este tenga el servicio de la red del operador con una *SIM* que no fue vinculada anteriormente.

Por otra parte, se observa que las *Listas Grises* no resultan ser de las más utilizadas para su implementación, mientras que el *Kill switch* no ha sido implementado toda vez que requiere de un trabajo en equipo entre fabricantes y operadores el cual muchas veces es difícil de lograr, pero de hacerlo, sería la opción más viable para combatir el robo de ETM, ya que lo deja totalmente inoperable, en lugar de solamente impedir el acceso a la red del operador móvil.

PUNTOS CLAVE DEL CAPÍTULO III

- *En la experiencia internacional se denota que no existe un mecanismo infalible para erradicar el robo de **ETM**.*

- *Argentina, Bolivia, Colombia, Chile, Perú, Paraguay, Costa Rica, Grecia, Francia, son algunos de los países que optaron por implementar el registro de los equipos reportados como robados o extraviados en las Listas Negras.*

- *Se observa que la segunda acción más utilizada son las Listas Blancas, como complemento a las Listas Negras.*

  *En Estados Unidos de América, los operadores y fabricantes en coordinación con el gobierno, han ido implementando como acción en algunos estados, el Kill switch, con lo cual se ha instalado en los dispositivos un software que permite la desactivación total de un **ETM** reportado como robado o extraviado.*

- *Dentro de la normatividad en los diversos países, se abrogaron algunas leyes estableciendo nuevas sanciones para los delitos relacionados con el robo de **ETM**.*

- *Con la implementación de una combinación de los métodos analizados, se podría obtener mayor efectividad en el combate al robo de **ETM.***

IV. Situación actual y medidas tomadas en México.

El servicio de telefonía móvil ha incrementado su demanda, derivado de la utilidad y los beneficios que tiene para los usuarios, es así, que a mayo de 2023 se registraron 129.5 millones de líneas de telefonía móvil en México (IFT, 2023), a la par se ha observado que el robo de **ETM** ha sido constante, es por ello que México se ha sumado a la implementación de acciones relacionadas a disminuir este tipo de situaciones, como lo son, el uso de la *Lista Negra,* uso de la herramienta *Device Check*, entre otras acciones como la difusión de información a través de campañas enfocadas a conocer el *IMEI* y la presentación de reportes por robo o extravío de **ETM**.

a. Antecedentes del robo de ETM en México.

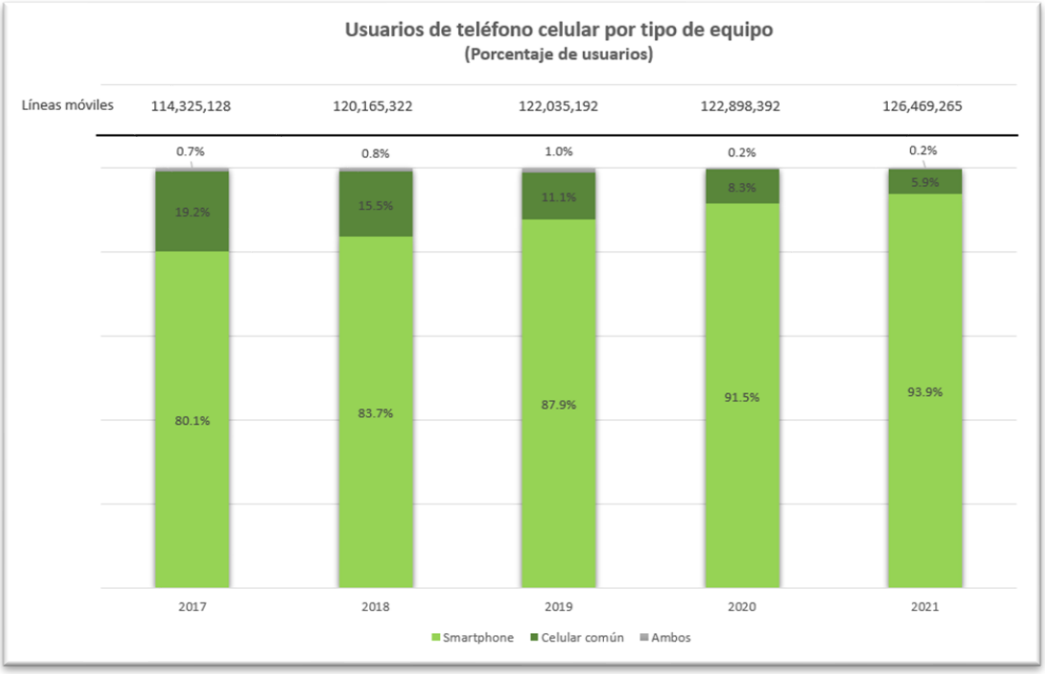
En 2010, el país experimentó un aumento en la adopción de **ETM** inteligentes (BIT, 2023), por lo que el alto valor de los mismos provocó el incremento del robo debido a la facilidad con la que los delincuentes pueden llevar a cabo la sustracción de estos equipos, dado que son pequeños, portátiles, de igual forma contienen información importante o sensible, la cual puede ser utilizada para sacar provecho de los usuarios.

La Encuesta Nacional referente a la Disponibilidad y Uso de Tecnologías de la Información en los Hogares (en lo sucesivo, "*ENDUTIH*"), realizada por el Instituto Nacional de Estadística y Geografía y el Instituto, reveló datos interesantes sobre los usuarios de telefonía celular en México. En 2020 la proporción fue de 75.5% (88.2 millones de usuarios) (ENDUTIH, 2020), un crecimiento anual en la adopción de teléfonos celulares de 2.8 puntos porcentuales. En el año 2021, se contaba con 91.7 millones de usuarios de teléfono celular (78.3% de la población de seis años o más) (ENDUTIH, 2021).

En 2021, nueve de cada diez personas disponían de un **ETM** inteligente. Entre 2017 y 2021 los usuarios que sólo dispusieron de un celular inteligente registraron un crecimiento de 13.8 puntos porcentuales al pasar de 80.1 a 93.9 porciento (ENDUTIH, 2021).

De acuerdo con el Banco de Información de Telecomunicaciones (en lo sucesivo, "*BIT*") del Instituto, al cuarto trimestre de 2021, se contabilizan un total de 126.4 millones de líneas móviles en nuestro país (BIT, 2023), cifra equivalente a una adopción de 93.9% de **ETM** inteligentes entre el total de líneas móviles. Ello nos deja un diferencial de 7.7 millones de dispositivos o 5.9%

del total de usuarios móviles que aún corresponden a equipos básicos o celular común con capacidades limitadas frente a las terminales inteligentes (ENDUTIH, 2021).

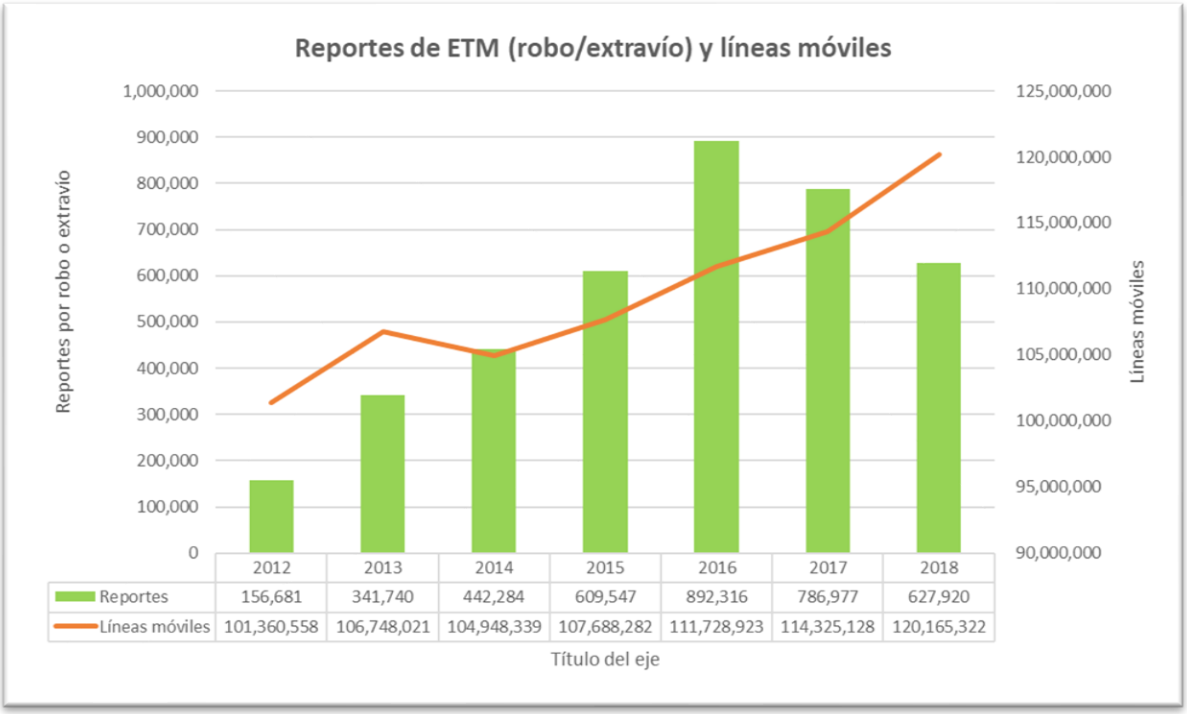


Fuente: Elaboración propia con información de ENDUTIH 2021 y BIT 2022

El robo de los **ETM** es un problema común en México, ya que los reportes por robo o extravío aumentaron casi seis veces, pasando de 156,000 en 2012 a más de 892,000 en 2016, esto según lo reportado por la Asociación Nacional de Telecomunicaciones (en lo sucesivo, "*ANATEL*").

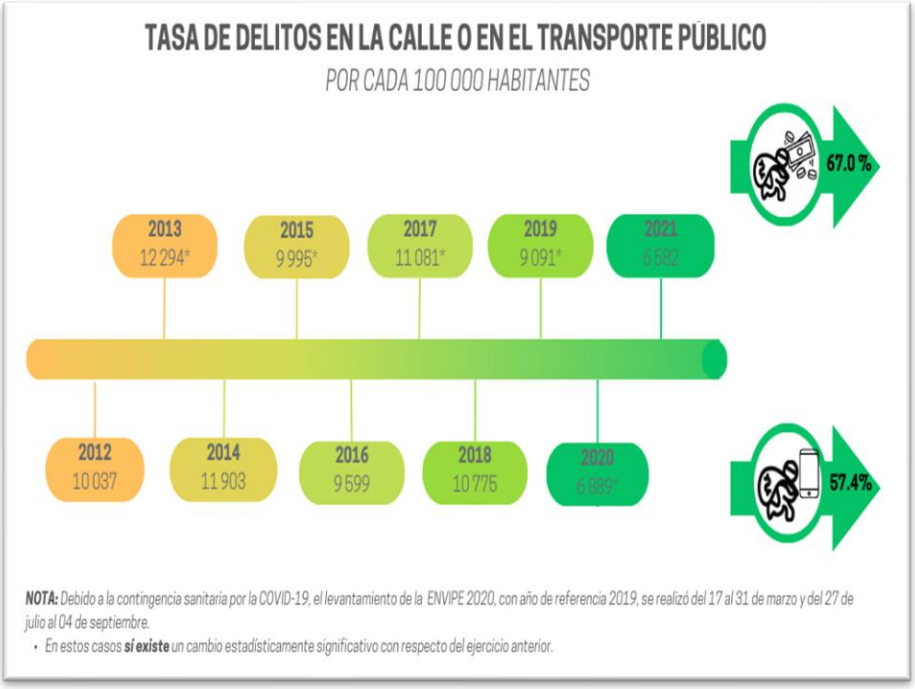
A través de los años son muchos los esfuerzos que los operadores móviles han llevado a cabo en colaboración con las autoridades federales, estatales, municipales y reguladores para fortalecer la seguridad de los mexicanos frente al robo de ETM, y aunque el robo de estos sigue presente, se reflejó una disminución en los reportes por robo y extravío para los años 2017 y 2018 (ANATEL, 2020).

La siguiente gráfica muestra el crecimiento de las líneas móviles (BIT, 2023) contra el reporte de robo o extravío en México (ANATEL, 2020):



Fuente: Elaboración propia con información de ANATEL, 2020 y BIT, 2023

Por otro lado, la Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (en lo sucesivo, "*ENVIPE*") en sus reportes anuales, muestra el total de robos o asaltos por año, el porcentaje de robo de **ETM** por cada uno de estos, así como la tasa de delitos por cada 100 mil habitantes, en la siguiente imagen se ilustran las cifras antes señaladas para el periodo de 2012 a 2021.



Fuente: Elaboración propia con información de ENVIPE, 2022

De la información antes expuesta se realizó el análisis por cada 100 mil habitantes, obteniendo como resultado, una disminución en los robos de **ETM** a partir del año 2019, tal como se muestra en la siguiente tabla.

Tabla 3: Análisis de robos de ETM por cada 100 mil habitantes

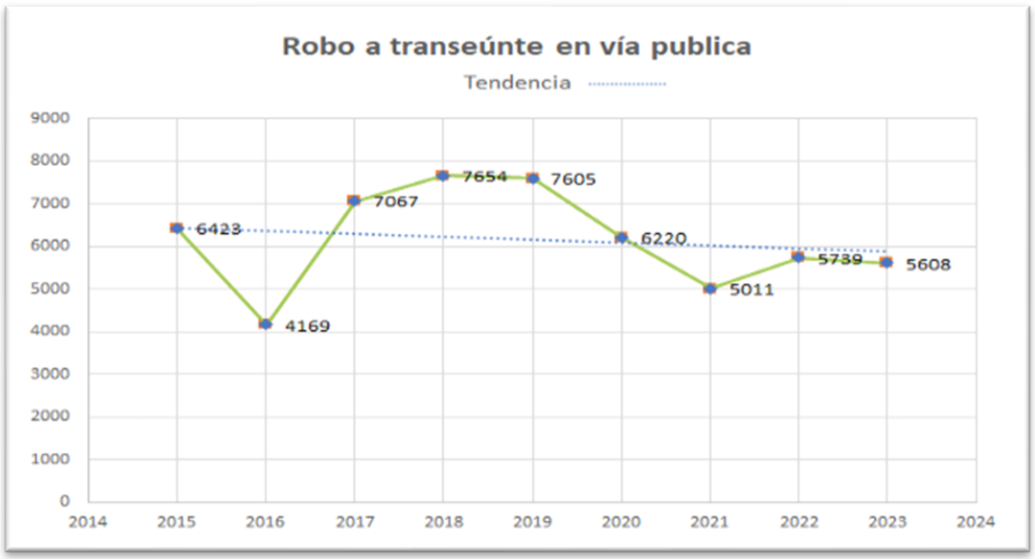
Año	*Robos o asaltos (en millones)*	*Porcentaje de robos de ETM*	*Robos por cada 100 mil habitantes*
2016	8.0	51.5	9,599
2017	9.5	51.2	11,081
2018	9.4	55.5	10,775
2019	8.2	56.0	9,091
2020	6.2	58.5	6,899
2021	6.0	57.4	6,582
2022	5.3	57.2	5,689

Fuente: Elaboración propia con información de ENVIPE, 2022

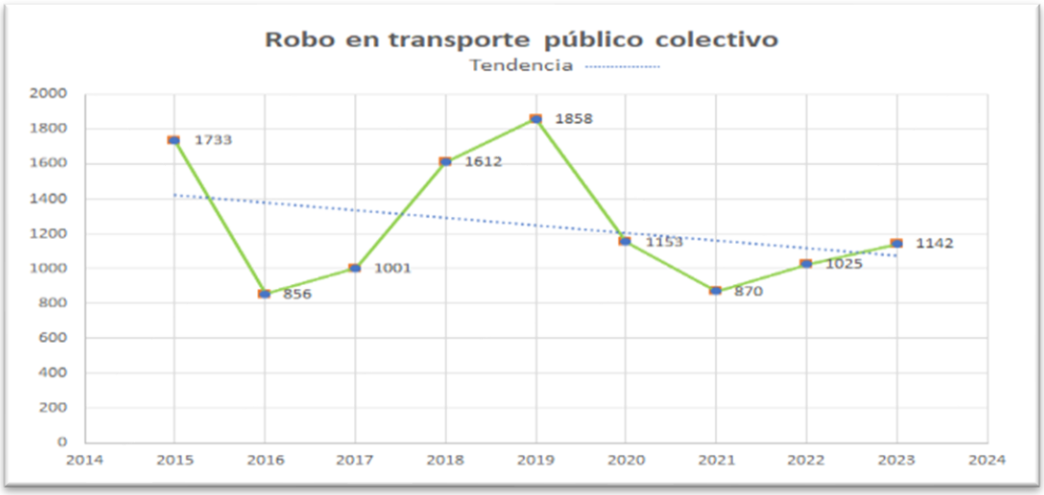
Sin embargo, en el año 2016 del 100% de los robos o asaltos registrados o denunciados en México, 51.5% correspondieron al robo de **ETM**, para 2017 la cifra fue muy parecida, siendo 51.2% el robo, en 2018 esta cifra incremento hasta el 55.5%, para 2019, el mismo fenómeno siguió en aumento situándose en el 56% este robo, para 2020 la tendencia continua al alza llegando hasta el 58.5% del total de los robos en este año, para 2021 y 2022 las cifras se mantienen semejantes, siendo 57.4 y 57.2% respectivamente (ENVIPE, 2022).

De acuerdo a las cifras anteriormente expuestas, se demuestra que el robo de **ETM** por cada 100 mil habitantes ha venido disminuyendo, sin embargo; se observa que del total de robos denunciados, los relativos a **ETM** son los de mayor frecuencia, por lo que el delito continúa siendo de importancia.

Por su parte, el Consejo Ciudadano de Seguridad y Justicia de la Ciudad de México (en lo sucesivo, "*CCSJMX*") en su reporte de incidencia delictiva del mes de febrero de 2023, señaló que en la Ciudad de México (en lo sucesivo, "*CDMX*"), el robo a transeúnte en vía pública disminuyó para el mismo periodo del año anterior, pero el robo a transporte público aumentó para el mismo periodo (CCSJMX, 2023).



Fuente: Elaboración propia con información de *CCSJMX*, 2023



Fuente: Elaboración propia con información de *CCSJMX*, 2023

El robo de los **ETM** en la *CDMX* es uno de los delitos más lucrativos, según estudios del *CCSJMX*, un **ETM** inteligente se vende en cuestión de horas generando altas ganancias en un solo día, si se toma en cuenta que cada 24 horas se roban más de 100 celulares en esa zona (CCSJMX, 2023).

De acuerdo con *ENVIPE*, el delito de ***Robo o asalto en vía pública*** fue el más frecuente en el año 2020 (ENVIPE, 2021).

LUGAR	TOTAL	MUJERES	HOMBRES
1	Robo o asalto en vía pública 22.5 %	Robo o asalto en vía pública 20.7 %	Robo o asalto en vía pública 24.4 %
2	Fraude 19.3 %	Fraude 18.6 %	Fraude 20 %
3	Extorsión 16.9 %	Extorsión 16.3 %	Extorsión 17.5%
4	Robo total o parcial del vehículo 10.6 %	Delitos sexuales 10.8 %	Robo total o parcial del vehículo 11.9 %
5	Amenazas verbales 9.7 %	Amenazas verbales 9.9 %	Amenazas verbales 9.4 %
6	Robo en casa-habitación 6.1 %	Robo total o parcial del vehículo 9.3 %	Otro tipo de robo 5.8 %
7	Delitos sexuales 5.9 %	Robo en casa-habitación 6.6 %	Robo en casa-habitación 5.7 %
8	Otro tipo de robo 5.1 %	Otro tipo de robo 4.3 %	Lesiones 3.8 %
9	Lesiones 3.4 %	Lesiones 2.9 %	Delitos sexuales 0.8 %
10	Otros delitos 0.6 %	Otros delitos 0.6 %	Otros delitos 0.6 %

Fuente: Elaboración propia con información de *ENVIPE*, 2021

En esta sección se analizaron los aspectos relacionados con los antecedentes del robo de **ETM** en México, de lo cual se concluye lo siguiente:

1. **Incremento en la demanda de telefonía móvil:** El crecimiento exponencial de las líneas de telefonía móvil en México refleja la alta demanda y utilidad de estos dispositivos para los usuarios.

2. **Crecimiento sostenido de usuarios de ETM:** A lo largo de los últimos años, se ha tenido en México un aumento constante en el número de usuarios que poseen **ETM**. Este incremento ha ido de la mano con el crecimiento exponencial de las líneas móviles en México.

3. **Reporte de robo de ETM:** De la información obtenida del *ENVIPE* se observa que el robo de **ETM** por cada 100 mil habitantes ha venido disminuyendo, sin embargo; se observa que del total de robos denunciados, los relativos a **ETM** son los de mayor frecuencia.

4. **Delitos relacionados con el robo de ETM:** El robo de **ETM** está asociado con otros delitos, como robos a transeúntes, asaltos en la vía pública, transporte público, locales o centros comerciales, entre otros, lo que indica un panorama más amplio de inseguridad en México.

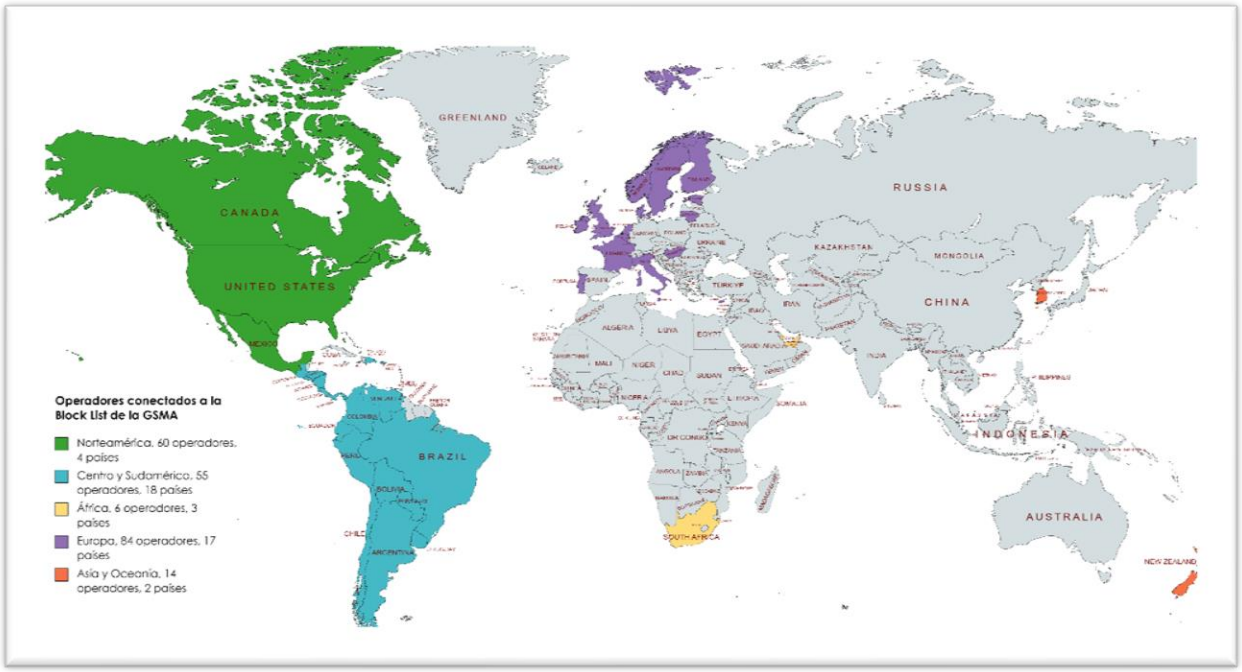
En resumen, el robo de **ETM** en México sigue siendo importante. Aunque los reportes por este fenómeno mostraron una baja, el mismo continúa siendo un problema relevante y el más importante en términos relativos.

b. Uso de la *Block List* o Lista Negra en México

Hoy en día, la mayoría de los países disponen de una *Block List* en la que se registran los *IMEI* de los celulares reportados como robados o extraviados, a fin de que los operadores los bloqueen (y los desbloqueen, una vez que los usuarios los reporten como recuperados).

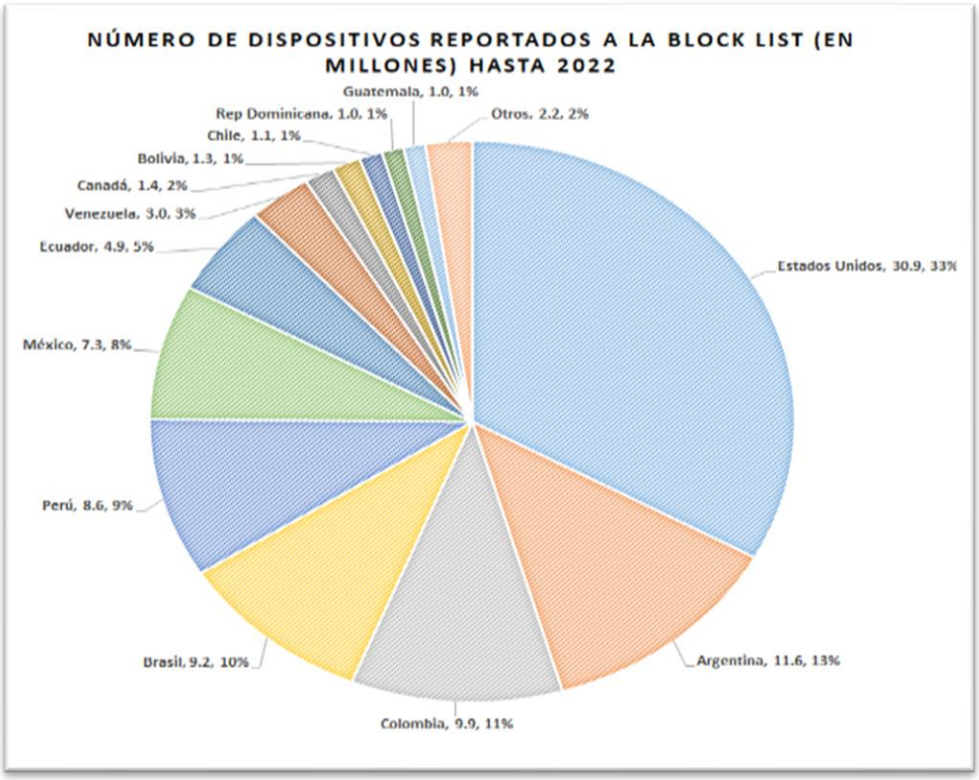
A finales de 2022, la *Lista Negra* de la *GSMA* contaba con más de 106 millones de registros reportados por los diferentes países asociados a la *GSMA*. Esta base de datos ha crecido rápidamente, de la mano de una mayor adopción de esta en la región, al igual el incremento en los robos y la cantidad de equipos móviles en América Latina. A finales de 2015, había poco más de 15 millones de *IMEI* en esta base de datos (con información de la *GSMA*).

Operadores móviles conectados a la *Lista Negra* de la *GSMA* hasta diciembre de 2022



Fuente: Elaboración propia con información de la *GSMA*.

El siguiente gráfico muestra el número de *IMEI* reportados a la *Block List* o *Lista Negra* por los países del continente americano asociados a la *GSMA*. Para 2022, México era el sexto país que más *IMEI* había reportado, con 7.3 millones y un porcentaje del 8% (con información de la GSMA).



Fuente: Elaboración propia con información de la *GSMA*.

Para el año 2022, la cantidad de *IMEI* reportados por México a la *Block List* de la *GSMA* fue de más de 806 mil, es decir, 266 mil *IMEI* menos en relación con los reportados en el año 2019.

Fuente: Elaboración propia con información de la *GSMA*.

En esta sección se revisó la información relacionada con los *IMEI* ingresados a la *Block List* o *Lista Negra* por parte de los países miembros de la *GSMA*, particularmente la información de México.

En resumen, en 2022 México fue el sexto país del continente americano con más ingresos de *IMEI* a la *Block List* de la *GSMA*, de lo que se puede deducir que el robo de ETM no ha cedido a pesar de las medidas implementadas en México para contrarrestar este problema. El número de ingreso de *IMEI* a la *Lista Negra* en 2022 disminuyó 24.8% en comparación con los ingresos de 2019, aun cuando los robos en este segmento se han mantenido constantes, lo que indica que se han dejado de reportar los delitos de esta modalidad, lo que es congruente con lo mencionado en la sección anterior.

c. Políticas y acciones para reducir el robo de ETM en México.

Las políticas públicas son acciones de gobierno con objetivos de interés público que surgen de decisiones sustentadas en un proceso de diagnóstico y análisis de factibilidad, para la atención efectiva de problemas públicos específicos, en donde participa la ciudadanía en la definición de problemas, así como sus soluciones y busca minimizar los estragos en donde ellos son afectados. En este caso, el objeto de estudio en específico: el robo de teléfonos celulares, aquí denominados ETM, afecta al usuario, por ello, se busca reducir este delito en México, así como atenuar sus consecuencias.

En México se hace frente a este problema, mediante acuerdos con la industria, gobiernos locales, federales y usuarios, a fin de generar mecanismos eficientes para reducir este fenómeno delictivo.

En consecuencia, en julio de 2012, con la presencia del entonces presidente de los Estados Unidos Mexicanos y los cuatro principales operadores móviles de México, firmaron el "*Acuerdo para evitar el hurto de celulares a nivel regional"* (GSMA, 2012).

Por otra parte, la Secretaría Ejecutiva del Sistema Nacional de Seguridad Pública a nombre del Gobierno Federal, con la participación de la *ANATEL*, las empresas y la sociedad civil, presentó en noviembre de 2014, la "*Campaña Nacional para el Reporte y Bloqueo a través del IMEI"* de teléfonos celulares robados y extraviados (SEGOB, 2014). Para ello, el Gobierno de la República, en estrecha coordinación con operadores de telefonía móvil, pusieron en

marcha dicha campaña de difusión, a través del código *IMEI*, para el reporte y bloqueo de los teléfonos celulares robados o extraviados.

La intención de esta campaña es hacer conciencia entre la población que haya extraviado su celular o les haya sido robado, para que reporten el hecho a su compañía de servicio, el ETM sea inhabilitado y se impida su uso en la comisión de un delito o en el comercio ilegal de ellos.

A su vez, los operadores móviles comparten las bases de datos de los equipos reportados con sus similares de otros países, a través de la *GSMA*, con la finalidad de evitar su futura reactivación y el eventual mal uso. La *ANATEL*, por su parte, apoya a difundir la campaña a través de su página *Web* y redes sociales, con la finalidad de disminuir el robo de teléfonos celulares y su uso para cometer delitos como la extorsión y el secuestro, realizando diversas colaboraciones con el Gobierno de México, una de ellas fue la iniciativa en noviembre de 2014, relativa a la *"Campaña Nacional para el Reporte y Bloqueo de teléfonos celulares robados o extraviados"*, impulsada con la finalidad de facilitar la consulta del *IMEI* de cada terminal; y así reportar a su proveedor de servicios móviles, si este había sido robado o extraviado, con la finalidad de bloquear su uso y agregarlo a la *Block List* global de la *GSMA* (ANATEL, 2015).

Aunado a ello, en junio de 2015 la *ANATEL* y los operadores de telefonía móvil en México, con el apoyo de la *GSMA*, celebraron la implementación en México del Sistema de Verificación de Dispositivos Robados *Device Check* (GSMA, 2015), el cual permite a los usuarios móviles verificar en tiempo real si el dispositivo móvil a adquirir había sido reportado como robado o extraviado.

A través de su sitio *Web* www.ift.org.mx/IMEI, el Instituto puso en operación la herramienta que permite a los usuarios de telefonía móvil revisar en tiempo real desde cualquier dispositivo (IFT, 2015), si el teléfono celular que se comprará está incluido en la *Block List* de celulares reportados como robados, no solo de México, sino a nivel mundial. La base de datos es actualizada diariamente con reportes de más de 219 operadores globales, incluyendo a 115 operadores de 22 países del continente americano.

Esta iniciativa ha sido realizada en el marco de la campaña "*Nos Importa México*", que fue presentada el 9 de febrero de 2015 por la *ANATEL* y la *GSMA*, como un esfuerzo conjunto de la industria móvil y otras organizaciones nacionales para brindar a los usuarios mexicanos una experiencia móvil más segura y sustentable a través de programas para combatir el robo de

dispositivos móviles, proteger a los niños, facilitar el acceso de las personas con discapacidad y proteger el medio ambiente.

En diciembre de 2015 el Instituto publicó en el Diario Oficial de la Federación (DOF), el *"Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996"*, el cual señala en el Capítulo VII, la suspensión del servicio de los Dispositivos o Equipos o Terminales Móviles reportados como robados o extraviados (DOF, 2015). Además, establecen los mecanismos para que los usuarios y las autoridades competentes soliciten a los concesionarios y autorizados la suspensión de los servicios de los dispositivos robados, así como, para evitar la activación de estos cuando dichos **ETM** hayan sido reportados como robados o extraviados. También establece las disposiciones generales de carácter obligatorio para que los concesionarios y autorizados presenten al Instituto, un procedimiento uniforme que permita que los usuarios reporten los dispositivos o **ETM** que hayan sido robados o extraviados, es decir deberán contar con un procedimiento para que a través de mecanismos, reciban y verifiquen los reportes de duplicación de *IMEI*, el mismo se notifica de manera gratuita vía *SMS*; llevar a cabo la suspensión de los servicios de los **ETM** que hayan sido objeto de un acto ilícito, así se ofrece certeza jurídica a los usuarios de servicios de telefonía móvil, de las acciones tomadas por los operadores, derivadas del aviso de robo o extravío de un dispositivo.

Para que un dispositivo pueda ser homologado, el Instituto deberá otorgar al solicitante, un Certificado de Homologación que será único para cada **ETM**. Por lo anterior, el 27 de abril del 2017, se publicó en el DOF la disposición técnica *"IFT-011-2017: Especificaciones de los equipos terminales móviles que puedan hacer uso del espectro radioeléctrico o ser conectados a redes de telecomunicaciones. Parte 1. Código de identidad de fabricación del equipo (IMEI) y funcionalidad de receptor de radiodifusión sonora en frecuencia modulada (FM)"*, con la finalidad de reforzar el uso del *IMEI*, como único y válido para un **ETM**, lo cual los hace inequívocamente identificados, pudiendo efectuar el bloqueo de estos cuando exista reporte de robo o extravío.

El certificado de Homologación contendrá la siguiente leyenda:

> *"Cada uno de los **ETM** amparados por el presente Certificado de Homologación cuenta con un Código de Identidad de fabricación del equipo (IMEI) conforme a lo establecido en la disposición técnica **IFT-011-2017**."*

Otra de las acciones establecidas en esta disposición, es comprobar que el ETM contenga la información de funcionalidades relativa a su localización geográfica (por ejemplo, localización en línea) y/o protección de contenido (código para desbloquear los equipos) en el caso de robo o extravío.

En julio de 2019, la Procuraduría Federal del Consumidor (en lo sucesivo, "*PROFECO*") se suma a las acciones que llevan a cabo la Asociación Mexicana de Empresas de Servicios Prendarios (*AMESPRE*) junto con las autoridades federales, estatales y municipales, a través de la campaña "*Reporte de Valor*" (PROFECO, 2019), la cual invita a los usuarios a conocer y usar el *IMEI*, esto con el objetivo de desincentivar el robo de teléfonos celulares, siendo esta una manera de promover el consumo seguro, es decir, teniendo certeza de que se adquiere un dispositivo móvil de procedencia legal o no robado.

De acuerdo a lo establecido en la Norma Oficial Mexicana *NOM-184-SCFI-2018 (publicada en el DOF el 8 de marzo de 2019), "Elementos normativos y obligaciones específicas que deben observar los proveedores para la comercialización y/o prestación de los servicios de telecomunicaciones cuando utilicen una red pública de telecomunicaciones"* (cancela a la NOM-184-SCFI-2012), el proveedor de servicios de telecomunicaciones debe informar al consumidor, a través de medios físicos, electrónicos, digitales o de cualquier otra nueva tecnología que lo permita los procedimientos, condiciones y mecanismos expeditos, para que éste pueda solicitar la suspensión y/o cancelación de los servicios de telecomunicaciones contratados, así como el bloqueo de *IMEI* del equipo terminal en caso de robo y/o extravío del mismo, de conformidad con las disposiciones emitidas por el Instituto.

De igual manera, establece que los contratos de adhesión relativos a la prestación de servicio de telecomunicaciones en el esquema de prepago, que sean utilizados por los proveedores de servicios de telecomunicaciones con los consumidores, deben estar registrados ante la *PROFECO* y contener, cuando menos, los medios sin costo a través de los cuales el consumidor podrá reportar el robo o extravío de la línea y/o el equipo terminal de telecomunicaciones así como solicitar la suspensión y/o cancelación de la línea y/o servicios de telecomunicaciones.

Por otra parte, la Secretaría de Seguridad y Protección Ciudadana invita a los usuarios en general a respaldar y proteger la información contenida en sus equipos móviles, se debe tomar en cuenta todos los datos personales y familiares, contactos, sesiones de redes sociales y correo electrónico que quedaron abiertas en un equipo que ha sido extraviado o robado, ya que en muchas de las ocasiones los delincuentes emplean esta información para cometer ilícitos como extorsión telefónica, robo de identidad y acceso a cuentas o bienes (SSPC, 2019).

La entonces jefa de gobierno de la Ciudad de México, lanzó en julio de 2019 la campaña **#bloqueatucel,** a cargo de la Secretarías de Seguridad Ciudadana (SSC) y la Secretaría de Gobierno (SEGOB), para informar a la ciudadanía sobre la importancia de reconocer y reportar el número *IMEI* del celular que haya sido robado o extraviado, ya sea por medio de su compañía operadora, *LOCATEL* o la página de internet https://bloqueatucel.cdmx.gob.mx (CDMX, 2019).

La mandataria, también promovió el veto de la venta de celulares en mercados ambulantes mediante los *"Lineamientos de operación de mercados móviles en la modalidad de tianguis, bazares y complementarios en la Ciudad de México",* publicados en la Gaceta Oficial de la Ciudad de México el 9 de julio de 2019.

El documento establece, entre otros, que la venta de telefonía celular debe ser considerado como falta grave, lo que a su vez ocasionará la cancelación del permiso de todo el tianguis. Por otro lado, se señaló que se podrán hacer operativos especiales en los mercados ambulantes, los cuales deberán ser coordinados por la Secretaría de Seguridad y las alcaldías (CDMX, 2019).

El documento en su artículo 10, señala específicamente lo siguiente:

> *"Queda estrictamente prohibida la venta de teléfonos celulares dentro de los mercados móviles en la modalidad de Tianguis, Bazares y complementarios."*

Fuente: Elaboración propia con información de dependencias y organismos gubernamentales en México.

Para noviembre de 2019, en el Senado de la República se realizó una proposición con punto de acuerdo por el que se exhortaba a las autoridades del Gobierno del Estado de México para adoptar medidas preventivas a fin de evitar la venta de celulares robados en mercados ambulantes y bazares que se instalan en municipios integrantes de la zona metropolitana del Valle de México, emulando lo que ya se había implementado en la Ciudad de México (SENADO, 2019).

En esta sección se revisaron los aspectos relacionados con las políticas y acciones para reducir el robo de **ETM** en México, de lo cual se concluye lo siguiente:

1. **Impacto social y económico:** El robo de **ETM** afecta principalmente al usuario dado que tiene un impacto significativo en su economía y privacidad y principalmente en el usuario, especialmente en áreas urbanas como la Ciudad de México, donde este delito es lucrativo y muy frecuente. La rápida reventa de estos dispositivos genera altas ganancias y contribuye a la incidencia delictiva y por otro lado genera una perdida significativa de patrimonio e información del usuario.

2. **Medidas de seguridad y colaboración:** Los esfuerzos conjuntos entre operadores móviles, reguladores, IFT, organizaciones nacionales e internacionales. autoridades federales, estatales y municipales han buscado fortalecer la seguridad en torno a los robos y principalmente el de los **ETM**, por lo que se han desarrollado e implementado diversas disposiciones, lineamientos y acciones para alcanzar el objetivo de disminuir esta problemática en México.

El robo constante de **ETM** en México ha llevado a la implementación de medidas para contrarrestar este problema, sin embargo, aún persisten desafíos significativos para prevenir este delito, la problemática lejos de disminuir ha ido en constante crecimiento. A pesar de los esfuerzos conjuntos, es necesario evaluar alternativas que puedan resultar más efectivas.

Con base en las conclusiones anteriores, algunas medidas que podrían implementarse para combatir e inhibir el robo de **ETM** en México son:

- **Reportes por robo o extravío:** Los mecanismos o procesos existentes para el reporte por robo o extravío de un **ETM**, deberían ser más sencillos y expeditos, con el fin de que los usuarios hagan cada vez más uso de estos.

- **Campañas informativas y educativas para la población:** Es necesario que la población adquiera mayor conciencia de la importancia de reportar el robo para que el **ETM** sea

inhabilitado, por lo que se considera que se deben reforzar las campañas para concientizar y educar sobre cómo protegerse de este fenómeno.

PUNTOS CLAVE DEL CAPÍTULO IV

- *Las líneas móviles en México han tenido un aumento considerable durante los últimos años.*
- *En 2022, México fue el sexto país del continente americano que más IMEI reportó a la Block List de la GSMA con un total de 7.3 millones de registros.*
- *De acuerdo con la información del ENVIPE, el porcentaje de robos o asaltos de **ETM** se mantuvo constante. Mientras por cada 100 mil habitantes se obtuvo como resultado, una disminución en los robos de **ETM** a partir del año 2019.*
- *Es necesario reforzar el trabajo conjunto entre operadores móviles, reguladores, IFT, organizaciones nacionales e internacionales. autoridades federales, estatales y municipales para encontrar un método más eficiente para la disminución de los **ETM** y fortalecer la seguridad de los usuarios.*

V. Acciones posibles para disminuir el robo de ETM.

La presente investigación, arroja la existencia de diversas prácticas internacionales, así como las necesidades nacionales para la disminución del robo de ETM. A continuación, se presentan las propuestas de algunas acciones posibles a evaluar para disminuir el robo de ETM derivado de la experiencia observada a lo largo del estudio, así como por su innovación:

a. *Kill switch.*

Método que incorpora una función de desconexión total vía remota e impide el funcionamiento del equipo en caso de robo o extravío. Brinda la posibilidad de reactivar el dispositivo, en caso de que el dueño lo recupere y él mismo lo habilite, de lo contrario el equipo quedará totalmente inservible.

Para poder impulsar esta propuesta, el Instituto, derivado de sus atribuciones, podrá evaluar la implementación de regulación que contengan las obligaciones y responsabilidades de los fabricantes, operadores, concesionarios y autorizados, así como las características necesarias para que los equipos que se comercialicen en México implementen esta función, con la finalidad de que los ETM contengan un *software* descargable y actualizable periódicamente, para el bloqueo remoto temporal o permanente del dispositivo móvil en caso de robo o extravío.

Cabe señalar que, de la revisión y modificación de las normas y disposiciones vigentes, se debería considerar un procedimiento no complejo para llevar a cabo la instalación y actualización de los equipos que han sido fabricados y puestos en venta antes de la emisión de la nueva regulación.

b. Listas Blancas.

Otra de las opciones observadas dentro de la investigación son las *Listas Blancas*, que son bases de datos de números *IMEI* registrados por fabricantes, operadores y usuarios para acceder a las redes de los operadores, con ellas se autentifica la propiedad de los ETM. Se registra factura, nombre del usuario, número de teléfono con el que se encuentra asociado el número *IMEI* del dispositivo, entre otros.

Las ventajas de emplear *Listas Blancas* son: tienen acceso a la red de los operadores solo los dispositivos que se encuentren registrados, con su uso también es posible detectar números *IMEI* clonados o alterados e ir restringiendo su acceso a través de la autenticación de la propiedad.

Por otra parte, al utilizar las *Listas Blancas* se generan grandes cantidades de información, la cual debe ser actualizada y administrada por alguien, esto se traduce en cargas de trabajo y altos costos para su operación. También requiere de la cooperación de los usuarios para registrar sus equipos y vincularlos a su línea telefónica, lo cual dependería de su interés. Aunado a ello, limita la capacidad de cambiar fácilmente la tarjeta *SIM* de equipo a otro, debido al registro entre *SIM* y el ETM.

c. Obligaciones de los operadores.

Derivado de las obligaciones de los operadores establecidas en el *"Acuerdo mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996"*, se recomienda reforzar los mecanismos de vigilancia y supervisión referente a los procedimientos presentados por los concesionarios y autorizados, en función de sus obligaciones de robustecer la información de la detección de duplicación de *IMEI* de los ETM, y garantizar la suspensión de los servicios de los ETM que hayan sido objeto de alteración de *IMEI*, dando así certeza jurídica a los usuarios de servicios de telefonía móvil, de las acciones tomadas por los operadores, derivadas del aviso de robo o extravío de un dispositivo.

La importancia del párrafo anterior, es que por medio de los registros en la red los operadores se puede detectar si en su sistema se encuentra repetido una cantidad "N" de veces un número *IMEI*, un ejemplo es que un número *IMEI* usa la red del operador a las 12:00 del día en la Ciudad de México y el mismo número *IMEI* vuelve a emplear la red a las 12:05 del día pero ahora en Tijuana, ahí claramente se tendría un caso de clonación de *IMEI*; también se pueden detectar números *IMEI* que poseen con combinaciones fuera de lo habitual por ejemplo que solo contenga un número (9999999999), ese sería un *IMEI* alterado, los prestadores de servicios tienen acceso a estos registros solo deberían tener bajo vigilancia estos casos.

La desventaja es que se generan costos por la búsqueda de números *IMEI* repetidos, costos por creación de bases internas de los operadores y para una mayor efectividad se debe

hacer un cruce de información, de forma periódica y continua entre operadores, además de que una vez detectada la clonación o alteración de números *IMEI,* se deben tomar acciones para acreditar la propiedad del equipo, una vez acreditada la información se restringe el acceso a las redes de los otros números *IMEI* que no hayan sido acreditados.

d. Responsabilidad de Usuario: Campaña de difusión por parte el Instituto.

Un pilar fundamental del estudio, son las personas usuarias, ya que, dentro de las disposiciones de la Ley Federal de Telecomunicaciones y Radiodifusión, se establece la protección de sus derechos, es así que se considera relevante realizar nuevas campañas de concientización *a través de campañas publicitarias y diversos medios,* enfocadas a impartir información a los usuarios respecto de conocer y conservar el número *IMEI* de sus equipos, así mismo promover el uso de los portales existentes para realizar de manera eficaz y expedita los reportes de sus equipos en caso de robo o extravío.

También es importante reforzar la difusión de información correspondiente a las responsabilidades y derechos adquiridos al ser usuario de un equipo móvil haciendo uso de los servicios de telecomunicaciones exhortándolos a consultar el manual de procedimientos "Atención a Usuarios de Servicios de Telecomunicaciones", "los Derechos de los Usuarios," entre otros instrumentos, los cuales podrán ser consultados en el portal del Instituto. Cabe mencionar, que para que exista eficiencia en la implementación de soluciones reseñadas en este estudio, es necesaria la participación de los usuarios, ya que en muchos casos desconocen sus derechos y responsabilidades.

De las propuestas anteriormente mencionadas, se considera que la implementación de una combinación de estas acciones para disminuir el robo de ETM, como el *Kill switch*, *Listas Negras* y *Listas Blancas*; podría dar mayor resultado para el objetivo que se busca en el presente estudio.

Se observa que, sería conveniente fomentar acciones coordinadas por parte de los operadores y usuarios, así como el fortalecer los mecanismos de difusión de las medidas existentes.

PUNTOS CLAVE DEL CAPÍTULO V

- *Dentro de las acciones sugeridas a implementarse, se considera que el Kill switch podría contribuir en México a una disminución del robo de los ETM, ya que su principal función es dejar inactivo el equipo móvil, por lo que disminuirían los beneficios para la delincuencia.*

- *Otra propuesta es utilizar la Lista Blanca, la cual se refiere a una base de datos de números IMEI registrados por fabricantes, operadores y usuarios para acceder a las redes de los operadores, su principal función es autentificar la propiedad de los **ETM**. Esta acción sería complementaria a la Listas Negra.*

- *Se recomienda reforzar los mecanismos de vigilancia y supervisión en el cumplimiento de las obligaciones de los operadores para robustecer la información de la detección de duplicación de IMEI de los **ETM**, y así garantizar la suspensión de los servicios de los **ETM** que hayan sido objeto de alteración de IMEI, dando así certeza jurídica a los usuarios de las acciones tomadas por los operadores, derivadas del aviso de robo o extravío de un dispositivo móviles.*

- *Asimismo, es necesario reforzar las campañas informativas con la finalidad de que el usuario conozca sus derechos y obligaciones al adquirir y hacer uso de los dispositivos, como lo es conservar el número IMEI y reportar el robo o extravío del **ETM**.*

VI. Conclusión.

Como se ha mencionado a lo largo del estudio, diversos países trabajan dentro de su normativa, para disminuir uno de los actos ilícitos más comunes dentro de la sociedad, el robo de ETM. Para combatir este problema, se ha buscado implementar diversas medidas, como la creación de bases que permiten el bloqueo de equipos y evitan que sean reutilizados; la instalación de programas que funcionan previo reporte por robo o extravío, los cuales permiten una desactivación total o parcial del ETM.

Sin embargo, se ha observado que ningún método ha resultado totalmente efectivo para erradicar este delito, por lo que es un tema relevante en México y a nivel mundial, debido a las afectaciones que genera en aspectos sociales y económicos para los gobiernos, autoridades, operadores móviles y usuarios.

En general, si bien se han realizado esfuerzos significativos para reducir el robo de los ETM en México, aún existen desafíos en la implementación y cumplimiento efectivo de las medidas aplicadas para disuadir esta práctica ilícita.

Para mejor entendimiento de la problemática a lo largo del presente estudio, se llevó a cabo el análisis de fuentes bibliográficas y estadísticas, siendo el capítulo referente al *Contexto general del problema* en donde se reitera la importancia del trabajo conjunto de los usuarios, operadores móviles, fabricantes, gobierno, entes reguladores y organismos de seguridad, para lograr métodos más efectivos para la disminución del robo de los ETM, principalmente reforzar el conocimiento del usuario referente a las consecuencias que conlleva el adquirir un ETM en el mercado ilegal las afectaciones económicas para estos sujetos.

En cuanto al capítulo *Acciones generales a la problemática*, se revisaron diversos métodos para combatir el robo de ETM, evaluando tanto sus ventajas como desventajas al implementarlos. De dicha revisión, destacan herramientas como *Device Check* de la *GSMA*, que se centra en la identificación de dispositivos robados a través del número *IMEI*; además las listas blancas, negras y grises también juegan un papel crucial en este contexto, al registrar los *IMEI* autorizados, reportados como robados y no localizados; asimismo, el *Kill switch* y la vinculación fija del número *IMSI* con el número *IMEI* presentan alternativas efectivas para combatir el robo de ETM. Por su parte, la *UIT* propone medidas para los *IMEI* no válidos, incluyendo el bloqueo de dichos equipos. Estas acciones implementadas ofrecen distintas perspectivas para abordar el desafío en el ámbito de la seguridad de dispositivos móviles.

De la investigación bibliográfica del capítulo *Experiencia Internacional*, se concluye que aún no existe un mecanismo infalible para erradicar el robo de **ETM**, observándose que el más usado por la mayoría de los países es el registro de los equipos reportados como robados o extraviados en las *Listas Negras*, el segundo más utilizado el uso de las *Listas Blancas*, utilizadas como complemento a las *Listas Negras*. Por otra parte, se destaca la experiencia en Estados Unidos de América, en donde los operadores y fabricantes en coordinación con el gobierno, han ido implementando el *Kill switch*, el cual permite la desactivación total de un **ETM** reportado como robado o extraviado. Por otro lado, en ciertos países además de adoptar alguno de los mecanismos anteriores, se establecieron sanciones para los delitos relacionados con el robo de **ETM**.

El siguiente comparativo integra las acciones implementadas en México, compartiendo con los países analizados, las relativas a la *Lista Negra* y del *Servicio de comprobación*.

País	*Lista Negra*	*Lista Blanca*	*Lista Gris*	*Servicios de comprobación*	*Vinculación IMSI-IMEI*	*Kill switch*	*Delito tipificado*
Argentina	✔						
Bolivia	✔	✔		✔			
Colombia	✔	✔		✔			✔
Chile	✔	✔					
Perú	✔	✔		✔	✔		
Paraguay	✔			✔			
Ecuador	✔	✔		✔	✔		
Costa Rica	✔	✔	✔	✔			
USA	✔			✔		✔	✔
Reino Unido							✔
Grecia	✔						
México	✔			✔			
Francia	✔						

Consecuentemente, del análisis realizado, se observa que es recomendable decantarse por la implementación de una combinación de los métodos analizados, para así poder obtener mayor efectividad en el combate al robo de **ETM.**

Respecto a la sección *Situación actual y medidas tomadas en México*, se concluye de la investigación bibliográfica y estadística, que, se observó el aumento creciente y constante de la demanda de servicios móviles en México, situación que se ve reflejada en la demanda de más **ETM**. Los reportes por robo o extravío de **ETM**, aumentaron entre el periodo de 2012 a 2016, mientras que para 2017 y 2018, estos disminuyeron; de igual manera, la información presentada en el *ENVIPE*, arroja cifras del delito por robo de los **ETM** de 2012 a 2018, mostrando que se mantuvo constante, mientras que para el periodo de 2020 a 2022 se pudo observar un cambio estadístico significativo.

Para el año 2022, México fue el sexto país del continente americano que más números *IMEI* reportó a la *Block List* de la *GSMA*, por lo que desde hace varios años operadores móviles, Instituto, organizaciones nacionales e internacionales, autoridades federales, estatales han venido colaborando para encontrar un método más efectivo para la disminución de los **ETM** y fortalecer la seguridad de los usuarios.

Para finalizar, en el capítulo correspondiente a las *Recomendaciones para disminuir el robo de **ETM***, se puntualizan los métodos, mecanismos y acciones que resultan convenientes derivado de la investigación realizada en el presente estudio, entre los cuales se encuentra el *Kill switch*, su principal función es dejar inactivo el **ETM**, por lo que se considera favorable para la disminución de los equipos móviles. Otra propuesta que se mencionó es el uso de las *Listas Blancas*, ya que es una base que contiene los números *IMEI* registrados por fabricantes, operadores y usuarios y permite autentificar la propiedad de los **ETM**.

Dentro de las atribuciones del Instituto, se recomendó reforzar los mecanismos de vigilancia y supervisión del cumplimiento de los operadores conforme a los Lineamientos emitidos por el Instituto; además de reforzar las campañas informativas con la finalidad de que el usuario conozca sus derechos y obligaciones al adquirir un equipo móvil, según sea el caso, considerando que, si se implementan conjuntamente dos o más de las acciones antes citadas, se podría obtener un resultado más eficiente.

De esta forma, se concluye que es necesario un enfoque integral que involucre la cooperación continua para trabajar en una implementación más efectiva y garantizar la protección de los usuarios en el país.

Aunque el bloqueo, el rastreo *GPS* y otras medidas implementadas por medio de *software* en los equipos, pueden ayudar a recuperar los dispositivos o a borrar la información contenida en ellos, aún existen métodos para eludir estas medidas.

Desde otra vertiente, el fortalecimiento de la normativa, así como de la cooperación regional, son elementos clave para abordar este problema, adoptar prácticas adecuadas y seguir con la colaboración entre las autoridades, operadores, asociaciones de telecomunicaciones y usuarios, para obtener un mejor resultado en el combate de robo de ETM.

Se requiere el desarrollo e implementación de normativas administrativas, generales y especializadas que permitan el uso de los métodos inexplorados en el país.

Referencias

ANATEL. (2015). *Nos importa México, Unidos para brindar una experiencia móvil más segura y confiable.* Obtenido de https://www.anatel.org.mx/robo.php

ANATEL. (2020). *Programa de Seguridad.* Obtenido de https://www.anatel.org.mx/programaseguridad.php

ARCEP. (2004). *Décision n° 04-150 de l'Autorité de régulation des télécommunications en date du 24 mars 2004.* Obtenido de https://en.arcep.fr/uploads/tx_gsavis/04-150.pdf

ARCEP. (2004). *Décision n° 04-209 de l'Autorité de régulation des télécommunications en date du 24 mars 2004.* Obtenido de https://en.arcep.fr/uploads/tx_gsavis/04-209.pdf

ARCEP. (2015). *LISTA NEGRA.* Obtenido de www.arcep.com

ARCOTEL. (2017 A). *RESOLUCIÓN 03-03-ARCOTEL-2017.* Obtenido de https://www.arcotel.gob.ec/wp-content/uploads/2019/05/RESOLUCION-03-03-ARCOTEL-2017-Regl-Homologacion-ocr.pdf

ARCOTEL. (2017 B). *Tu Celular Legal.* Obtenido de http://tucelularlegal.arcotel.gob.ec/tucelularlegal/index.aspx

ATT. (2009). *Verificación IMEI.* Obtenido de https://plataformas.att.gob.bo/index.php/verificacion

BIT. (2023). *Servicio Móvil de Telefonía.* Obtenido de https://bit.ift.org.mx/SASVisualAnalyticsViewer/VisualAnalyticsViewer_guest.jsp?reportSBIP=SBIP%3A%2F%2FMETASERVER%2FShared%20Data%2FSAS%20Visual%20Analytics%2FReportes%2FTelefon%C3%ADa%20M%C3%B3vil(Report)&page=vi3205&sso_guest=true&informationEnabled=fa

CCSJMX. (2023). *Incidencia delictiva en la CDMX.* Obtenido de https://consejociudadanomx.org/buscador?consulta=incidencia+delictiva

CDMX, G. (2019). *Lineamientos de operación de mercados móviles en la modalidad de tianguis, bazares y complementarios en la Ciudad de México.* Obtenido de https://data.consejeria.cdmx.gob.mx/portal_old/uploads/gacetas/450fb9f5402b3049c9cb6e2453b41bc7.pdf

Codigo Penal. (2011). *Ley 1453 de 2011.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=43202

Código Penal. (2016). *Ley 1801 de 2016.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=80538

CONATEL. (2008). *RESOLUCIÓN 641-24-CONATEL-2008.* Obtenido de https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/11/2008-CONATEL-GEN-24-641.pdf

CONATEL. (2009). *RESOLUCIÓN 191-07-CONATEL-2009.* Obtenido de https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/191_07_conatel_20091.pdf

CONATEL. (2012). *RESOLUCIÓN TEL-535-18-CONATEL-2012.* Obtenido de https://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/0535_tel_18_conatel_2012.pdf

CONATEL. (2017 A). *RESOLUCIÓN DIRECTORIO N° 647/2017 POR EL CUAL SE APRUEBAN LAS NORMAS COMPLEMENTARIAS DEL DECRETO N.2 6728/17 QUE REGLAMENTA LA LEY N° 5629/16.* Obtenido de https://www.conatel.gov.py/conatel/wp-content/uploads/2019/10/2017-rd-647-cop-1.pdf

CONATEL. (2017 B). *REGISTRO NACIONAL DE EQUIPOS TERMINALES MÓVILES BLOQUEADOS (REMOB).* Obtenido de https://imei.conatel.gov.py/#/imei

Congreso. (2013). *S.1070 - Mobile Device Theft Deterrence Act of 2013.* Obtenido de https://www.congress.gov/bill/113th-congress/senate-bill/1070/text

Congreso. (2014). *H.R.4065 - Smartphone Theft Prevention Act.* Obtenido de https://www.congress.gov/bill/113th-congress/house-bill/4065/text

Congreso. (2016). *Congress.gov.* Obtenido de https://www.congress.gov/bill/114th-congress/house-bill/5834?resultIndex=78

Congreso de la Nación. (2016). *LEY N° 5629 DE OBLIGATORIEDAD A LAS EMPRESAS DE TELEFONÍAS CELULARES A REALIZAR BLOQUEOS DE EQUIPOS TERMINALES MÓVILES CELULARES ROBADOS, HURTADOS, O EXTRAVIADOS A TRAVÉS DE SU SISTEMA INTERNACIONAL PARA LA IDENTIDAD DE EQUIPOS MÓVILES.* Obtenido de https://bacn.gov.py/archivos/5147/20160923093956.pdf

CRC. (2011 A). *RESOLUCIÓN No. 3066 DE 2011.* Obtenido de https://www.crcom.gov.co/sites/default/files/normatividad/00003066_0.pdf

CRC. (2011 B). *RESOLUCIÓN No. 3128 DE 2011.* Obtenido de https://www.crcom.gov.co/sites/default/files/normatividad/00003128_0.pdf

CRC. (2015). *RESOLUCIÓN No. 4813 DE 2015.* Obtenido de https://www.crcom.gov.co/sites/default/files/normatividad/00004813.pdf

CTIA. (2015). *Smartphone Anti-Theft Voluntary Commitment.* Obtenido de https://www.ctia.org/the-wireless-industry/industry-commitments/smartphonea-anti-theft-voluntary-commitment

CTIA. (2017). *STOLEN PHONE CHECKER.* Obtenido de https://stolenphonechecker.org/spc/

Deloitte. (2023). *Deloitte research highlights the dangers of data theft from mobile devices.* Obtenido de https://www2.deloitte.com/ie/en/pages/risk/articles/mobile-devices-security.html

DOF. (2015). *ACUERDO mediante el cual el Pleno del Instituto Federal de Telecomunicaciones expide los Lineamientos de Colaboración en Materia de Seguridad y Justicia y modifica el plan técnico fundamental de numeración, publicado el 21 de junio de 1996.* Obtenido de https://www.dof.gob.mx/nota_detalle.php?codigo=5418339&fecha=02/12/2015#gsc.tab=0

EETT. (2014). *Deactivation of stolen mobile phones through IMEI.* Obtenido de https://www.eett.gr/en/deltia_tipou/eett-deactivation-of-stolen-mobile-phones-through-imei/

ENACOM. (2016). *Resolución N° 2459/2016 (Boletín Oficial N° 33.383, 20/05/2016).* Obtenido de https://www.enacom.gob.ar/multimedia/normativas/2016/Resolucion-2459_16-ENACOM.pdf

ENDUTIH. (2020). *Encuesta Nacional Sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2020.* Obtenido de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2021/OtrTemEcon/ENDUTIH_2020.pdf

ENDUTIH. (2021). *Encuesta Nacional Sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2021.* Obtenido de https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/OtrTemEcon/ENDUTIH_21.pdf

ENVIPE. (2021). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2021.* Obtenido de https://www.inegi.org.mx/contenidos/programas/envipe/2021/doc/envipe2021_presentacion_nacional.pdf

ENVIPE. (2022). *Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública 2022.* Obtenido de https://www.inegi.org.mx/contenidos/programas/envipe/2022/doc/envipe2022_presentacion_nacional.pdf

France Legislation. (2011). *Code des postes et des communications électroniques.* Obtenido de https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000023713267/2011-03-16/

Gaceta Oficial. (2009). *Bolivia: Decreto Supremo Nº 353, 4 de noviembre de 2009.* Obtenido de https://www.lexivox.org/norms/BO-DS-N353.html

GSMA. (2012). *Gobierno de México y operadores firman acuerdo contra el hurto de terminales.* Obtenido de https://www.gsma.com/latinamerica/es/gobierno-de-mexico-y-operadores-firman-acuerdo-contra-el-hurto-de-terminales/

GSMA. (2014). *FAQs – Base de Datos IMEI.* Obtenido de https://www.gsma.com/latinamerica/es/faqs-base-de-datos-imei/

GSMA. (2015). *Anatel y la GSMA celebran la implementación de la herramienta para que los mexicanos puedan verificar que su celular no tenga reporte de robo.* Obtenido de https://www.gsma.com/latinamerica/es/herramienta-mexico-celular-robo/

GSMA. (2015). *GRACIAS.* Obtenido de https://www.inegi.org.mx/progra

GSMA. (2015). *Robo de Celulares en América Latina.* Obtenido de https://www.gsma.com/latinamerica/es/robo-terminales-imei/

GSMA. (2016). *La Economía Móvil América Latina.* Obtenido de https://www.gsma.com/latinamerica/wp-content/uploads/2016/09/ME_LATAM_2016-Spanish-Report-FINAL-Web-Singles-1.pdf-

GSMA. (2017). *Seguridad, privacidad y proteción del sistema móvil.* Obtenido de https://www.gsma.com/latinamerica/wp-content/uploads/2017/06/Seguridad-privacidad-y-proteccio%CC%81n-del-ecosistema-mo%CC%81vil.pdf

GSMA. (2023 A). *Nosotros.* Obtenido de https://www.gsma.com/latinamerica/es/about-us-es/

GSMA. (2023 B). *Device Check.* Obtenido de https://www.gsma.com/services/tac/about-device-check/

ICONECTIV. (2017). *combating mobile crime.* Obtenido de https://iconectiv.com/sites/default/files/2017-04/combating%20mobile%20crime%20public%20policy.pdf

IFT. (2015). *Consulta de IMEI.* Obtenido de https://www.ift.org.mx/IMEI

IFT. (2023). *Datos oportunos del Sector de Telecomunicaciones 2023.* Obtenido de reportedeinformacionoportuna1t2023_1.pdf (ift.org.mx)

Inetum. (2011). *SRTM Sistema de Registro de Terminal Móvil.* Obtenido de https://www.imeicolombia.com.co/

IPE. (2022). *Instituto Peruano de Economía.* Obtenido de https://www.ipe.org.pe/portal/cuanto-nos-cuesta-el-robo-de-un-celular-por-nicolas-zevallos/

Judicial, O. d. (2019). *7879-SUTEL-SCS-2020*. Obtenido de https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=92402&nValor3=122330&strTipM=TC

Karachi, U. d. (2015). *Economic Review and Street crime Analysis Using Cell Phone Snatching and Theft.* Obtenido de

https://www.researchgate.net/publication/306017525_Economic_Review_and_Street_crime_Analysis_Using_Cell_Phone_Snatching_and_Theft

MTT. (2011). *DECRETO 157 ESTABLECE EL PROCEDIMIENTO QUE REGULA EL BLOQUEO DE EQUIPOS TERMINALES ROBADOS, HURTADOS Y EXTRAVIADOS.* Obtenido de https://www.bcn.cl/leychile/navegar?idNorma=1027905&idVersion=2011-09-19

MTT. (2013). *RESOLUCIÓN 1068 EXENTA RESOLUCIÓN QUE REGULA EL BLOQUEO DE EQUIPOS TERMINALES MÓVILES DE SERVICIOS DE TELECOMUNICACIONES EN SITUACIONES ESPECIALES.* Obtenido de https://www.bcn.cl/leychile/navegar?idNorma=1049952&idParte=9342212&idVersion=2023-01-27

MTT. (2016). *RESOLUCIÓN 1463 EXENTA FIJA NORMA TÉCNICA QUE REGULA LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS QUE DEBERÁN CUMPLIR LOS EQUIPOS TERMINALES UTILIZADOS EN LAS REDES MÓVILES.* Obtenido de https://www.bcn.cl/leychile/navegar?idNorma=1091663

OSIPTEL. (2016). *DECRETO LEGISLATIVO 1338 QUE CREA EL REGISTRO NACIONAL DE EQUIPOS TERMINALES MÓVILES PARA LA SEGURIDAD, ORIENTADO A LA PREVENCIÓN Y COMBATE DEL COMERCIO ILEGAL DE EQUIPOS TERMINALES MÓVILES Y AL FORTALECIMIENTO DE LA SEGURIDAD CIUDADANA.* Obtenido de https://www.osiptel.gob.pe/media/bxajt1n3/dl1338-registro-terminales-moviles.pdf

OSIPTEL. (2017). *NORMAS COMPLEMENTARIAS PARA LA IMPLEMENTACIÓN DEL REGISTRO NACIONAL DE EQUIPOS TERMINALES MÓVILES PARA LA SEGURIDAD.* Obtenido de https://www.osiptel.gob.pe/media/vvsp2tf0/res081-2017-cd_normascomplementarias.pdf

OSIPTEL. (2019). *CONSULTA DE EQUIPOS CELULARES ROBADOS, PERDIDOS O RECUPERADOS.* Obtenido de https://www.osiptel.gob.pe/sistemas/sigem.html

PROFECO. (2019). *Profeco y Amespre buscan combatir el robo de telefonía móvil.* Obtenido de https://www.gob.mx/profeco/prensa/profeco-y-amespre-buscan-combatir-el-robo-de-telefonia-movil?idiom=es-MX

QUALCOMM. (2018). *With DIRBS, Qualcomm Technologies is helping governments and OEMs combat the counterfeit, illegal, and stolen device market.* Obtenido de https://www.qualcomm.com/news/onq/2018/09/dirbs-qualcomm-technologies-helping-governments-and-oems-combat-counterfeit

SEGOB. (2014). *Campaña Nacional para el Reporte y Bloqueo a través del IMEI.* Obtenido de https://www.gob.mx/segob/prensa/conferencia-de-sesnsp-carlos-hurtado-el-subsecretario-de-normatividad-de-medios-andres-chao-y-otros?idiom=es-MX

SENADO. (2019). *Dictamen de la Comisión de Seguridad Pública por el que se aprueba proposición con punto de acuerdo por el que se exhorta respetuosamente a las autoridades del Gobierno del Estado de México.* Obtenido de https://infosen.senado.gob.mx/sgsp/gaceta/64/2/2019-12-10-1/assets/documentos/Dict_Com_Seguridad_Publica_Venta_Celulares_Zona_Metropolitana.pdf

SSPC. (2019). *¿Extraviaste tu celular?... ¡no seas víctima de extorsión!* Obtenido de https://www.gob.mx/sspc/articulos/extraviaste-tu-celular-no-seas-victima-de-extorsion

SUTEL. (2020). *RCS-234-2020 "SOBRE DISPOSICIONES Y ASPECTOS OPERATIVOS PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE TERMINALES MÓVILES" EXPEDIENTE: GCO-NRE-REL-00123-2020.* Obtenido de https://www.sutel.go.cr/sites/default/files/rcs-234-2020_disposiciones_y_aspectos_operativos_sistema_terminales_moviles.pdf

SUTEL. (2022). *Plataforma de Validación de Celulares (PVC).* Obtenido de https://www.sutel.go.cr/pagina/plataforma-de-validacion-de-celulares-pvc

TMG. (2018). *Hurto de equipos móviles en América Latina: Políticas e iniciativas actuales.* Obtenido de https://www.tmgtelecom.com/wp-content/uploads/2018/12/TMG-Hurto-de-equipos-m%C3%B3viles-en-Am%C3%A9rica-Latina.pdf

Trustonic. (2019). *Smartphone Crime Is Growing – How Do We Turn the Tide?* Obtenido de https://www.trustonic.com/opinion/smartphone-crime-turning-the-tide/

UIT. (2017 A). *The Economic Cost Of IPR Infringement In The Smartphones Sector.* Obtenido de https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/research-and-studies/ip_infringement/study11/smartphone_sector_en.pdf.

UIT. (2017 B). *Requisitos de seguridad y arquitecturas funcionales para las medidas de lucha contra el robo de teléfonos móviles.* Obtenido de https://www.itu.int/rec/T-REC-X.1127/es

UIT. (2019). *Solución marco para contrarrestar la falsificación de dispositivos TIC.* Obtenido de https://www.itu.int/rec/T-REC-Q.5050/es

UIT. (2020). *Marco para luchar contra la utilización de dispositivos móviles robados.* Obtenido de https://www.itu.int/rec/T-REC-Q.5051/en

UK Legislation. (2002). *Mobile Telephones (Re-programming) Act 2002.* Obtenido de https://www.legislation.gov.uk/ukpga/2002/31

Velasco Chaves, L. F. (2021). *PROYECTO DE LEY POR LA CUAL SE DICTAN DISPOSICIONES PARA REDUCIR EL HURTO DE DISPOSITIVOS MÓVILES EN EL TERRITORIO NACIONAL.* Obtenido de https://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2020%20-%202021/PL%20412-21%20Robo%20de%20Celulares.pdf

Victimización, E. N. (2017). *Perdidas Patrimoniales por Victimización en Argentina*. Obtenido de https://www.seguridadciudadana.org.ar/recursos/articulos/perdidas-patrimoniales-por-victimizacion-en-argentina

COLABORADORES QUE PARTICIPARON EN LA ELABORACIÓN DE ESTE ESTUDIO.

Vanegas Soriano José Pablo

Dirección General de Regulación de Interconexión y Reventa de Servicios Mayoristas

Zambrano Vargas Vanessa

Dirección de Resolución de Desacuerdos de Interconexión

Alonso Cruz Mario

Subdirección de Resolución de Desacuerdos de Servicios de Interconexión 1

Guerra Durán Natalia Marcela

Subdirección de Resolución de Desacuerdos de Servicios de Interconexión 2

Caballero Bartolo Marco Antonio

Subdirección de Resolución de Desacuerdos de Servicios de Interconexión 3

Ortiz Moncada Hassid Abraham

Analista de Resolución de Desacuerdos de Interconexión

INSTITUTO FEDERAL DE TELECOMUNICACIONES

Insurgentes Sur 1143, Col. Nochebuena,

Demarcación Territorial Benito Juárez, C.P. 03720

Ciudad de México, Tel: 55 5015 4000 / 800 2000 120

www.ift.org.mx