Nº 00015-DAPU/2024

A	**:**	SERGIO ENRIQUE CIFUENTES CASTAÑEDA **GERENTE GENERAL**
ASUNTO	**:**	INFORME QUE PROPONE EL PROCEDIMIENTO PARA ATENDER LOS CUESTIONAMIENTOS DE BLOQUEO DE EQUIPOS POR IMEI CLONADOS O DUPLICADOS
FECHA	**:**	**1 de marzo de 2024**
REFERENCIA	**:**	RESOLUCIÓN DE CONSEJO DIRECTIVO N° 228-2023-CD/OSIPTEL

		CARGO	**NOMBRE**
ELABORADO POR	:	ANALISTA ECONÓMICO	LUIS PALACIOS SÁNCHEZ
		ESPECIALISTA PRINCIPAL EN ANALISIS ECONÓMICO	YOEL RIOS ARROYO
		COORDINADORA LEGAL	MATILDE JUDITH GONZALEZ VILLANUEVA
REVISADO Y APROBADO POR	:	DIRECTORA DE ATENCIÓN Y PROTECCION DEL USUARIO (E)	HAYINE GUSUKUMA LOZANO

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

ÍNDICE

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOSS
OSIPTEL DAPU M.GONZALEZ

1. OBJETIVO

El presente documento tiene por objeto sustentar el procedimiento para evaluar los cuestionamientos por bloqueo de equipo terminal móvil con IMEI clonado o duplicado.

Adicional a ello, se propone actualizar algunos artículos contenidos en la Norma de Condiciones de Uso de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones en virtud a las Normas Complementarias para la Implementación del RENTESEG, considerando la última modificación del Decreto Legislativo N° 1338.

2. DECLARACIÓN DE MEJORA REGULATORIA

En aplicación de lo dispuesto por la Resolución N° 030-2024-CD/OSIPTEL[1], se declara que el presente Informe, que sustenta el proyecto normativo que modifica la "Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones" y las "Normas Complementarias para la implementación del Registro Nacional de Equipos Terminales Móviles para la Seguridad", cumple con los Lineamientos de Mejora Regulatoria del Osiptel.

3. ANTECEDENTES

Mediante el Decreto Legislativo N° 1338[2], se creó el Registro Nacional de Equipos Terminales Móviles para la Seguridad y encargó su implementación y administración al OSIPTEL. Asimismo, mediante el Decreto Supremo N° 007-2019-IN[3], se aprobó el reglamento vigente de este Decreto Legislativo[4], el cual, entre otros aspectos, dispone que el OSIPTEL apruebe el régimen de infracciones y sanciones del citado marco legal.

Posteriormente, el OSIPTEL, mediante la Resolución N° 07-2020-CD-OSIPTEL aprobó las Normas Complementarias para la Implementación del Registro Nacional de Equipos Terminales Móviles para la Seguridad (en adelante, Normas Complementarias del RENTESEG), las cuales detallan la información que debe ser entregada al RENTESEG por los concesionarios del servicio público móvil, los importadores, ensambladores y fabricantes de equipos terminales móviles del país.

Asimismo, se debe señalar que en el capítulo II de las Normas Complementarias del RENTESEG, el OSIPTEL estableció los criterios para el procedimiento de detección de los IMEI duplicados o clonados que los concesionarios móviles deben aplicar para la identificación en su propia red. Específicamente, en el artículo 23 se establece que para realizar la referida detección se deben aplicar los criterios de (i) simultaneidad de las comunicaciones y ii) conflicto tiempo-distancia[5].

Por otra parte, a pesar de que en aplicación del marco normativo vigente se ha logrado bloquear 14 548 457[6] de equipos terminales móviles asociados a códigos IMEI inválidos desde el 2018; todavía se observa que esta problemática no se ha controlado plenamente. En efecto, en los últimos años, se tiene que las organizaciones criminales optarían por adoptar una nueva modalidad conocida como la clonación del código IMEI, con el objetivo de reducir la probabilidad de detección de un IMEI alterado y así habilitar los equipos terminales móviles bloqueados por robo para, posteriormente, ser comercializados en el mercado negro. Ante esta situación y considerando que la Tercera Fase del RENTESEG prevé el bloqueo de equipos terminales móviles duplicados o clonados, resulta necesario

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

[1] Publicada en el Diario Oficial El Peruano el 12 de febrero de 2024.
[2] Publicado en el diario oficial El Peruano el 6 de enero de 2017.
[3] Publicado en el diario oficial El Peruano el 4 de abril de 2019.
[4] Inicialmente, el Decreto Supremo N° 13138 fue reglamentado mediante el Decreto Supremo N° 009-2017-IN.
[5] Las empresas operadoras pueden proponer criterios distintos y el OSIPTEL podría determinar nuevos criterios.
[6] Cantidad de IMEI inválidos bloqueados durante el periodo septiembre 2018 - noviembre 2023.

plantear el procedimiento mediante el cual se evaluarán los cuestionamientos de bloqueo de equipo terminal por IMEI clonado o duplicado.

Del mismo modo, se debe indicar que considerando la última modificación del Decreto Legislativo N° 1338 referido al RENTESEG, resulta necesario actualizar algunos artículos contenidos en la Norma de Condiciones de Uso y en las Normas Complementarias del RENTESEG.

En la misma línea, se propone eliminar el procedimiento de cuestionamiento de titularidad del servicio móvil prepago a fin de evitar que ante del desconocimiento de este tipo de servicio, se siga haciendo uso de un servicio respecto del cual no se tiene identificado quién es el titular. Al aplicarse el procedimiento de reclamo por contratación no solicitada, a la fecha de presentación del reclamo la empresa debe suspender el servicio, salvo se ingrese por medios distintos al telefónico y presencial, en cuyo caso se ejecuta en 1 día hábil. Adicionalmente, se propone establecer precisiones sobre la contraseña única con la finalidad de facilitar su adecuada implementación y masificación.

Cabe indicar que, este proyecto normativo fue aprobado para comentarios mediante la Resolución N° 00228-2023-CD/OSIPTEL, publicado el 2 de agosto de 2023. En la referida resolución se estableció un plazo de quince (15) días hábiles para que los agentes interesados presenten sus comentarios. Durante este período se recibieron los comentarios de Viettel Perú S.A.C. (en adelante, Viettel), Entel Perú S.A. (en adelante, Entel), Flash Servicios Perú S.R.L. (en adelante, Flash), América Móvil Perú S.A.C. (en adelante, América Móvil) y Telefónica del Perú (en adelante, Telefónica).

Considerando los comentarios recibidos, en este informe se sustenta el proyecto normativo final que atiende la problemática de la clonación de equipos móviles, el problema de la desactualización de los contratos de servicios y otros problemas relacionados con la norma de Condiciones de Uso.

4. PROBLEMÁTICA DE SEGURIDAD EN EL SERVICIO PÚBLICO MÓVIL

4.1. Antecedentes

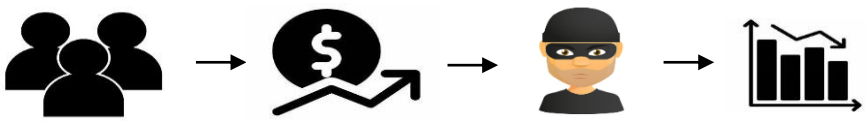
La regulación en la seguridad de los servicios públicos móviles consiste en el establecimiento de políticas que permitan brindar a los usuarios una experiencia móvil segura y garantizar, al mismo tiempo, las obligaciones de proteger la seguridad pública. De esta forma, en la medida que se desarrollan servicios móviles más avanzados y complejos, también se incrementa la lista de posibles amenazas y el alcance de los daños que pueden causar a los usuarios. Esto último implica la sustracción y comercialización de dispositivos robados y venta de uso de dispositivos falsificados, fraude y seguridad de los dispositivos móviles, ciberacoso y otras actividades ilegales que se realizan tanto a través de redes móviles como de servicios digitales (GSMA, 2018). Tal es así, que el OSIPTEL en los últimos años ha establecido una serie de medidas en el mercado con la finalidad de implementar mejoras en la seguridad de los usuarios tales como: desincentivar la incidencia de robos de equipos terminales móviles, proteger a los usuarios en los procesos de contratación del servicio y reposición de chips, entre otras.

Al respecto, según el reporte de la empresa de ciberseguridad Trustonic[7], para finales de 2020, la cantidad de usuarios de equipos terminales móviles en todo el mundo alcanzó los 3 500 millones, ascendiendo a un valor de mercado total de 1.46 trillones de dólares. Esto ha llevado a que la industria de las telecomunicaciones se convierta en una de las más susceptibles al fraude y al robo, de tal manera que expertos de la industria han estimado una pérdida de aproximadamente $17 mil millones al año debido a este tipo de

[7] Fuente: Trustonic. Disponible en: https://www.trustonic.com/opinion/healing-the-smartphone-theft-epidemic/

delitos. Ello implica una alarmante preocupación no solo para los usuarios y concesionarios del servicio móvil, sino también para los fabricantes y distribuidores que se ven afectados por conductas negativas ocasionadas por las organizaciones criminales.

FIGURA N° 1: IMPACTO DEL FRAUDE Y ROBO EN EL SECTOR DE TELECOMUNICACIONES



Fuente: Trustonic (2020)

Con relación a la escala de esta problemática, es preciso señalar que el robo de equipos terminales móviles surge en varias etapas de la cadena de oferta, la cual está conformada por los fabricantes, distribuidores, comercializadores y consumidores. Tal es así que, se procura mejorar los niveles de seguridad en cada uno de ellos, debido a que según lo reportado por Trustonic (2020), el robo de dispositivos móviles puede ocurrir en la etapa de fabricación, durante los envíos o en la tienda minorista. Al respecto, de acuerdo a las cifras presentadas por la referida empresa, entre el 5% y el 25% del robo de equipos móviles se comete durante los envíos de los terminales. Aunado a lo anterior, según Verizon, el número de robos a tiendas presentó un incremento interanual de 200% en el 2017, denotando una situación alarmante en las etapas de distribución y comercialización de los dispositivos móviles.

En tal contexto, las repercusiones irían desde la incapacidad de ofrecer nuevos equipos móviles a clientes potenciales y, en consecuencia, la pérdida de ingresos, hasta el aumento de las primas de seguros debido al robo del equipo móvil. La problemática se agrava en América del Sur, donde se ha evidenciado un rápido incremento en el número de delitos relacionados con los dispositivos móviles. De acuerdo con el referido artículo publicado por Trustonic (2020), se estima que en Brasil se roban hasta 15 000 dispositivos móviles al día, seguido de 6 000 en Perú y 5 000 en Argentina.

Ampliando el análisis a nivel internacional, según Trustonic (2020), se estima que cada día se denuncian más de 1000 dispositivos robados en el Reino Unido. Además, según la Oficina de Estadísticas Nacionales del referido país, más de 48 millones de consumidores han denunciado el robo de un dispositivo en los últimos 10 años, pero esta cifra se considera infravalorada y podría llegar a ser el doble. De manera similar, en Sudáfrica, la última encuesta de víctimas de delitos encontró que casi el 70% de los robos de propiedad personal están relacionados con equipos móviles.

En ese sentido, Trustonic (2020) recomienda que, en la etapa de fabricación, durante el transporte o en los puntos de venta, los operadores móviles deben poder rastrear, identificar y controlar el ciclo de vida del equipo terminal móvil para preservar los servicios de los usuarios y reducir los incentivos para el robo. Esto les permitirá proteger (e incrementar) sus ingresos y prevenir perdidas, así como reducir la participación de los equipos terminales móviles en el mercado negro.

Por último, se debe precisar que entre los factores que intervienen en el incremento de robos de equipos terminales móviles se tienen (i) el uso de equipos móviles de alto valor (smartphones) en las calles por parte de los usuarios, de manera que son objetivo rentable para los delincuentes y/o asaltantes de la calle, (ii) el tamaño de los equipos y la forma de uso en la vía pública (recibir llamadas, revisar internet) tornándose un blanco fácil para los ladrones, (iii) las familias que entregan equipos de valor a miembros con alta vulnerabilidad de ser asaltados (niños, adolescentes y adultos mayores), (iv) crecimiento de la informalidad y la pobreza que incrementa la demanda por equipos móviles usados

probablemente robados, (v) los usuarios que encuentran la posibilidad de satisfacer su necesidad de contar con equipos caros de alta gama a través de los equipos robados, y (vi) equipos móviles que son sustraídos para obtener la información personal.

Respecto a la clonación y duplicación de SIM card

En la actualidad, los equipos terminales bloqueados por sustracción (robo o hurto) pueden ser alterados para ser usados ilícitamente mediante la reprogramación del IMEI, de manera que se registre un IMEI inválido o se clone o duplique un IMEI que sí es válido. En el caso de equipos terminales con IMEI inválidos, el marco normativo vigente ha identificado un procedimiento efectivo para su identificación, dado que estos no cumplen con los estándares definidos por la industria, por lo que son fáciles de identificar y bloquear. Es así que, en el caso de los equipos terminales móviles con IMEI inválidos, estos pueden ser identificados contrastando el TAC (los dígitos que identifican la marca y el modelo del dispositivo), permitiendo la ejecución del bloqueo del equipo móvil.

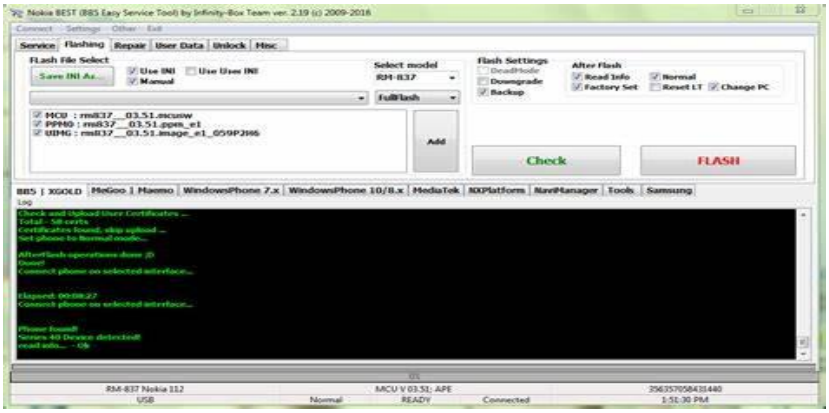
No obstante, en el caso de los IMEI clonados o duplicados, la técnica de identificación es más sofisticada y menos segura, debido a que los delincuentes replican directamente códigos IMEI de equipos terminales móviles con IMEI original, sin el conocimiento del titular del IMEI original y de incluso equipos terminales móviles que aún no han sido utilizados en las redes móviles, resultando difícil distinguir entre el titular verdadero y el que usa el IMEI clonado.

Al respecto, se debe señalar que la clonación se efectúa mediante el cambio y manipulación del IMEI con la ayuda de herramientas de software y flashes de hardware disponibles en diversos sitios *web* (Kumar et al., 2015). De acuerdo con la Unión Internacional de Telecomunicaciones (UIT, 2020b), estos métodos de clonación se pueden efectuar a través de tres tipos de técnicas:

- Mediante hardware: reemplazando el *chipset* en un dispositivo móvil con uno que pueda funcionar en el dispositivo objetivo.
- Mediante software: para cambiar el IMEI de los dispositivos móviles a través del *flasheo* o instalación de programas.
- Intermitentes: son una combinación de software y hardware que, originalmente se diseñaron con fines de reparación, pero pueden usarse ilegalmente para cambiar el IMEI en algunos dispositivos móviles.

Particularmente, se debe mencionar que, en los últimos años, se ha evidenciado el surgimiento del mercado negro de herramientas intermitentes, las cuales tienen como función principal la reparación del dispositivo móvil; sin embargo, actualmente, son utilizadas por parte de las organizaciones criminales con el propósito de alterar el IMEI de un dispositivo móvil sustraído o robado. Dentro de estos instrumentos se encuentran las denominadas cajas de intermitentes o cajas de liberación (*Box Infinity*) que permiten conectar un equipo bloqueado robado, y detectar la lista completa de IMEI de equipos terminales por marca, con la finalidad de seleccionar cualquier IMEI para replicarlo e instalarlo en un equipo terminal bloqueado (Kumar et al., 2015). En la figura N° 2 se puede apreciar el interfaz de una caja de liberación.

FIGURA N° 2: INTERFAZ DE LA CAJA DE LIBERACIÓN (BOX INFINITY)



Fuente: GSM-Forum

En el mercado negro existen diversas variedades de cajas intermitentes que cubren una amplia variedad de dispositivos móviles. A continuación, se presentan las dos categorías principales de cajas intermitentes (Unión Internacional de Telecomunicaciones - UIT, 2020b):

- Cajas de marca
    - Son más caros que sus equivalentes genéricos, tienen nombres y números de modelo conocidos y tienen números de serie únicos.
    - Algunas cajas necesitan activación.
    - Se proporciona software, actualizaciones y soporte para estas cajas.
    - No requieren una fuente de alimentación externa para funcionar.
    - Se basan en la interfaz USB como fuente de alimentación
    - Son ampliamente utilizados por los técnicos de servicio.
    - Los venden proveedores reconocidos y, a menudo, se encuentra una "lista de proveedores aprobados" en el sitio web del fabricante.
    - Por lo tanto, es más fácil obtener soporte para ellos en foros y en otros sitios web.
- Cajas sin marca
    - Estos son mucho más baratos que las cajas de marca y, a veces, coinciden con las cajas intermitentes originales en términos de componentes y funcionalidad.
    - A veces combinan la funcionalidad y el soporte de dispositivos de más de una caja intermitente de marca, al admitir la adición de una tarjeta inteligente de cajas intermitentes de marca.
    - No vienen con ningún software o controlador que haga que el comprador tenga la responsabilidad de crear el software de otras fuentes de Internet.
    - Algunos requieren una fuente de alimentación externa que generalmente no se proporciona con la compra.

Adicionalmente, existe otra técnica específica para la clonación de IMEI en equipos terminales con sistema operativo Android, consistente en descargar e instalar un emulador de terminal en el equipo e introducir una serie de comandos con el objetivo de insertar e

implantar un código IMEI válido en el equipo terminal. Asimismo, también se han detectado casos de clonación de IMEI de equipos iPhone de Apple, con sistema operativo iOS, mediante herramientas como Ziphone (Kumar et al., 2015).

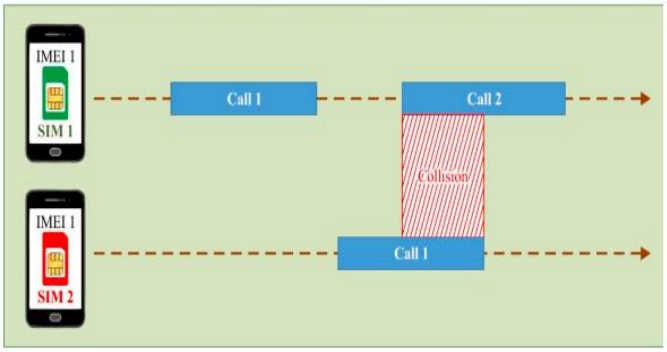
En general, resulta evidente que las organizaciones criminales han ido innovando en lo que respecta a métodos o técnicas de clonación de IMEI, sin limitarse a la marca, el modelo o sistema operativo que pueda contar el equipo terminal móvil. Cabe señalar que estas herramientas, técnicas y equipos para la clonación tienen un alto grado de accesibilidad para la delincuencia, dado que existen tutoriales en redes sociales.

En la relación con la problemática de la clonación de IMEI, la Unión Internacional de Telecomunicaciones (UIT) ha propuesto la implementación de mecanismos técnicos de identificación de IMEI clonados mediante el análisis de las condiciones de tiempo y distancia para la validación de la tarjeta SIM del equipo terminal. Específicamente, se ejecuta la metodología CDR (Registro de Detalles de Llamadas), la cual incorpora verificar los siguientes aspectos:

- **Conflicto de simultaneidad de comunicaciones**

  Consiste en revisar los CDR e identificar si existen IMEI utilizados simultáneamente en llamadas de equipos distintos, o si registran envíos de SMS o datos en otros equipos (ver figura N° 3).

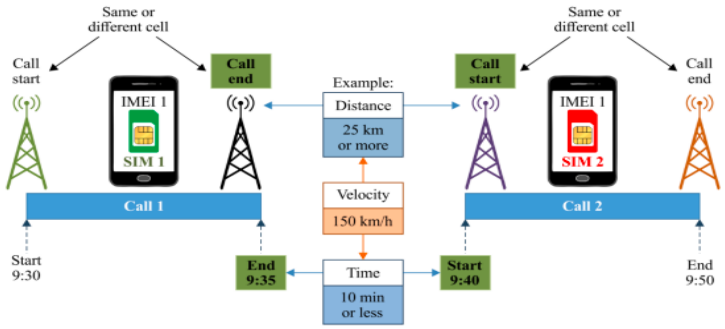
FIGURA N° 3: CONFLICTO DE SIMULTANEIDAD DE COMUNICACIONES



Fuente: Documento - ITU-T Q.5052 (UIT 2020c)

- **Conflicto de tiempo y distancia**
  Se revisan los CDR en los cuales se pueda observar dos servicios móviles vinculados a un mismo IMEI, en un período menor o igual a treinta (30) minutos y dentro 70 kilómetros de distancia (ver figura N° 4).

FIGURA N° 4: CONFLICTO DE TIEMPO Y DISTANCIA



Fuente: Documento - ITU-T Q.5052

En el marco de la Resolución de Consejo Directivo Nº 101-2020-CD/OSIPTEL[8], se requirió a los operadores su propuesta de identificación de IMEI clonados o duplicados. Asimismo, mediante la Resolución de Gerencia General N° 00329-2020-GG/OSIPTEL[9], se determinó el procedimiento para la identificación, verificación y compartición de IMEI duplicados o clonados intra-red. Cabe señalar que, el proveedor INETUM viene culminando un procedimiento de detección de IMEI clonados o duplicados inter-red.

4.2. Planteamiento del problema

De acuerdo con las cifras proporcionadas por el RENTESEG, durante el 2022, se registraron 1 709 770 reportes por sustracción de equipos terminales móviles en la lista negra. Esto implicaría que se reportaron diariamente 4 684 equipos móviles sustraídos. Asimismo, en el 2023 se reportaron 1 707 014 reportes de sustracción y en promedio 4677 reportes diarios de sustracción de equipo.

Adicionalmente, se debe señalar que la dimensión del problema de sustracción de equipos terminales móviles es mucho mayor, si se considera que los usuarios cuentan con una alta tasa de no denuncia. En efecto, según la ENAPRES[10], el 40% de las víctimas de hechos delictivos no denuncia porque considera que sería una pérdida de tiempo; mientras que según el Estudio de Satisfacción 2023, se observa que, en el servicio de telefonía móvil aproximadamente el 35% de usuarios que experimentan un problema no presentan un reclamo, el 46% ni siquiera comunica su problema a la empresa operadora. Ello implica que, probablemente existan muchos equipos robados o perdidos que siguen siendo comercializados ilegalmente, debido a que sus propietarios no han cumplido con reportarlo a los concesionarios móviles.

Asimismo, los delincuentes, con la finalidad de mantener un mercado negro de equipos sustraídos y robados, no solo reemplazan el IMEI lógico del equipo y le asignan un número de IMEI que no cumple con estándares internacionales, sino también duplican o clonan equipos con IMEI original. Esta situación ha motivado que de septiembre de 2018 a noviembre de 2023 se ejecute el bloqueo de 14 548 457 IMEI inválidos.

En ese contexto, las organizaciones criminales han optado por innovar en el comercio ilegal de equipos terminales móviles, mediante la implementación de técnicas de clonación de IMEI genuino u original de los equipos terminales móviles, a fin de replicar un IMEI que no se encuentre en lista negra. Como resultado de esta alteración, el IMEI

[8] Publicado el 26 de agosto de 2020.
[9] Publicado el 28 de diciembre de 2020.
[10] Informe Técnico de Estadísticas de Seguridad Ciudadana (Marzo-Agosto 2023). Disponible en: https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_estadisticas_de_seguridad_ciudadana.pdf

previamente clonado o duplicado permitirá habilitar el servicio móvil para un terminal móvil sustraído o robado.

En octubre del 2023, el OSIPTEL aplicó las metodologías de (i) conflicto de simultaneidad de comunicaciones y (ii) conflicto tiempo y distancia con la finalidad de identificar la cantidad de IMEI clonados o duplicados en las redes de Telefónica del Perú S.A.A. (en adelante, Telefónica), América Móvil Perú S.A.C (en adelante, América Móvil), Entel Perú S.A. (en adelante, Entel) y Viettel Perú S.A.C[11] (en adelante, Viettel). De esta evaluación se detectaron 344 622 IMEI originales que han sido clonados intra-red, una cantidad mayor a lo detectado en marzo del 2022, donde se obtuvo solo 177 848[12].

Asimismo, se detectó que los IMEI identificados como clonados se encuentran asociados a 881 236 líneas móviles, esto implica que, en promedio, un IMEI original o genuino ha sido clonado 1.6 veces dentro de la propia red móvil[13]. Comparando con lo observado en marzo del 2022, donde se identificaron 471 660 líneas asociadas[14] a IMEI originales, se ha encontrado que la cantidad de clonaciones se ha mantenido en 1.7 veces. Cabe señalar que el 95.6% de los IMEI con líneas asociadas clonadas ha sido clonada entre 2 y 4 veces, el 4.1% entre 5 y 20 veces y el 0.3% más de 20 veces. Particularmente, en el caso de los que han sido clonados más de 20 veces, en esta última evaluación se han encontrado 964 IMEI y 42 802 líneas asociadas; lo cual significa un incremento significativo respecto a lo observado en marzo del 2022, donde solo se identificaron 434 IMEI y 15 128 líneas asociadas[15].

Por otra parte, la tasa de incidencia de líneas móviles asociadas a un IMEI clonado o duplicado respecto al total de líneas móviles (Telefónica, Entel, América Móvil y Viettel) alcanzó un 2.2% en la evaluación de octubre del 2023. Este nivel de incidencia es superior a lo observado en marzo del 2022, donde se obtuvo 1.5%.

En el mismo período, el porcentaje de IMEI detectados como clonados respecto al total de IMEI identificados como sustraídos, perdidos, inválidos y clonados es del 66%, es decir, corresponde a más de la mitad del total de equipos móviles con IMEI en situación irregular. Este porcentaje es mucho mayor a lo observado en marzo del 2022, donde los clonados o duplicados representaban el 49%. Ampliando el análisis, se identificó que, entre el 2017 y marzo del 2023, la concesionaria móvil con mayor crecimiento anual promedio[16] de líneas asociadas a IMEI clonados fue Telefónica con 55.1%, seguido de América Móvil con 24.2% y Viettel con 19.2%[17].

Por lo tanto, se debe señalar que la falta de control sobre los equipos terminales con IMEI clonados o duplicados reduce significativamente la efectividad de la política de bloqueo de equipos terminales que circulan en el mercado negro, dado que estos podrían seguir siendo comprados y utilizados mediante un IMEI clonado o duplicado, cuando el objetivo es que estos equipos terminales sustraídos se inhabiliten de forma permanente. En efecto,

[11] No se ha realizado la evaluación en la red de Entel debido a que su plataforma de detección recién estará operativa en julio del 2022.
[12] En la evaluación del 2022 no participó Entel, por ello se estima que en el marzo del 2022 debió haber 228205 IMEI originales clonados.
[13] La cantidad de clonaciones por IMEI original se obtiene dividiendo la cantidad de líneas con IMEI clonado no original (881 236 menos 344 622) entre el total de IMEI originales (344 622).
[14] En marzo del 2022 no se evaluó a Entel, por ello se estima que en ese período debió haber habido 605 209 líneas asociadas a IMEI originales. Esto implica que la cantidad de líneas asociadas se ha incrementado en casi 19%.
[15] El incremento en número de IMEI y líneas asociadas con más de 20 clonaciones con respecto a marzo del 2022 no se explica por la inclusión de Entel en la evaluación de marzo del 2023, sino porque otra empresa operadora es la que registrado una mayor incidencia.
[16] Se considera una tasa de crecimiento promedio geométrico.
[17] No se dispone de información de Entel como para poder determinar cuál es su tasa de crecimiento anual.

al inhabilitar el equipo terminal móvil sustraído se elimina la posibilidad de venderlos, y se reduce el incentivo de realizar hechos delictivos contra la propiedad.

De manera similar, en el caso de los equipos terminales móviles contratados por la modalidad prepago, los cuestionamientos de titularidad han mantenido una tendencia creciente, llegando a más de 30 mil casos entre las principales cuatro empresas competidoras de enero a noviembre del 2023, lo cual es un incremento significativo dado que en el 2022 llegó a cerca de 10 mil casos. Este incremento de los cuestionamientos de titularidad prepago se podría deber en parte a que la suspensión de la línea cuestionada recién se ejecuta a los 15 días de recibida la solicitud.

Cabe señalar que, el procedimiento de cuestionamiento de titularidad prepago es un proceso que permite al usuario obtener la desvinculación con una línea en un plazo de 2 días hábiles, sin requerir una verificación biométrica. En este caso, la empresa operadora no requiere presentar evidencias de la contratación realizada, por lo que fácilmente un delincuente podría adquirir una línea prepago para cometer actos ilícitos y, posteriormente desvincularse sin mayor trámite.

Asimismo, para la suspensión de una línea prepago cuestionada, la normativa actual establece que se debe esperar 15 días calendario, con la finalidad de brindar a los usuarios que usan esa línea cuestionada la oportunidad de regularizar. Sin embargo, respecto a este punto se ha identificado que no se está haciendo uso de esa facilidad.

Por otra parte, se ha identificado que la entrega de la contraseña única se viene realizando de manera discrecional por parte de las empresas operadoras, lo cual genera diversos riesgos de seguridad y en algunos casos que los usuarios no accedan a la contraseña única de manera oportuna.

Asimismo, se debe señalar que, bajo el anterior marco normativo, se consideraban tres supuestos de excepción a la verificación biométrica (i) discapacidad o huella desgastada, (ii) fallas de conectividad con la base de datos de la RENIEC y (iii) el solicitante es extranjero. En el caso de los supuestos (i) y (ii), el solicitante debe presentar una declaración jurada con campos de información obligatorios, la declaración jurada no es exigible si la empresa operadora conserva la huella digital del solicitante. En cambio, en el caso del supuesto (iii), los extranjeros solo debían presentar el documento de identidad.

Al respecto, se ha identificado que estas reglas han generado una brecha de seguridad, dado que se han identificado varios registros inconsistentes en las listas de abonados, los cuales probablemente se hayan realizado mediante la contratación del servicio durante los períodos en los que la conectividad con la RENIEC falla o declarando falsamente que el usuario es discapacitado o extranjero.

Cabe señalar que, la consecuencia inmediata de estos registros inconsistentes radica en que los pedidos de información relacionada al titular de un servicio móvil o IMEI implicado en algún acto delictivo, formulados por el Ministerio Público, el Ministerio del Interior y la Policía Nacional, no podrían ser atendidos con una información útil. De este modo, la detección de registros inválidos de titulares de líneas dificultaría la investigación de las entidades en cuestión.

4.3. Agentes involucrados

Los agentes directamente involucrados son: (i) las empresas operadoras de servicios públicos de telecomunicaciones, (ii) los abonados de estos servicios, (iii) la entidad encargada de la regulación y supervisión (OSIPTEL).

4.4. Evidencias

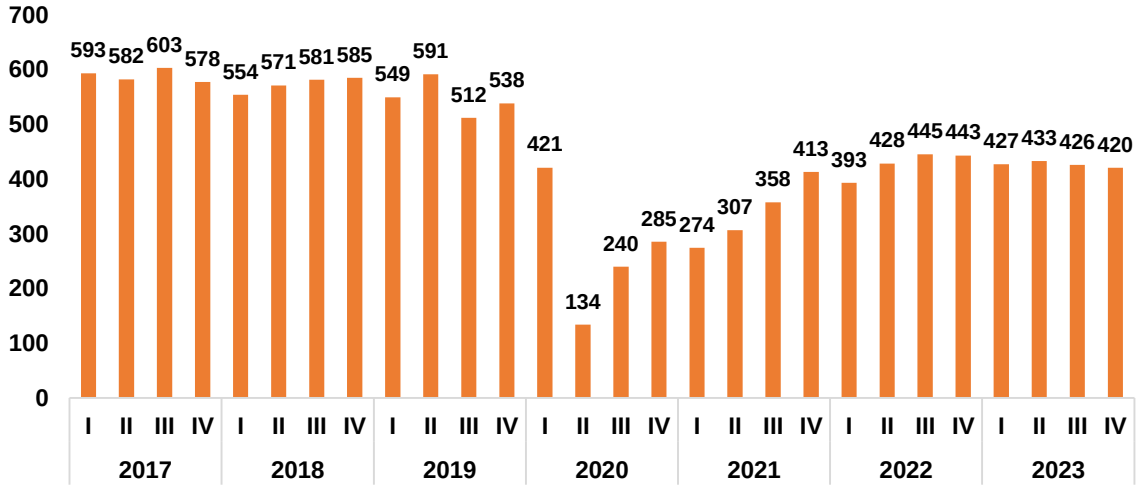
En esta subsección se presentan, con mayor detalle, las evidencias del problema planteado previamente.

4.4.1. Evolución de la cantidad de equipos terminales móviles sustraídos o robados

Según el RENTESEG, de enero de 2017 a diciembre de 2023, se han reportado 12.7 millones de equipos terminales móviles por sustracción, lo que revela la necesidad de continuar fortaleciendo medidas para combatir este mercado negro.

Así, en el siguiente gráfico se observa que la cantidad de equipos terminales móviles reportados por sustracción se ha mantenido constante durante el período 2017 – 2019, y durante el 2020 y parte del 2021 hubo un descenso explicado por el período de confinamiento obligatorio. En cambio, desde el tercer trimestre del 2021 se aprecia un incremento constante, el cual sin embargo se ha estabilizado en el 2023 a un promedio trimestral de 427 mil equipos.

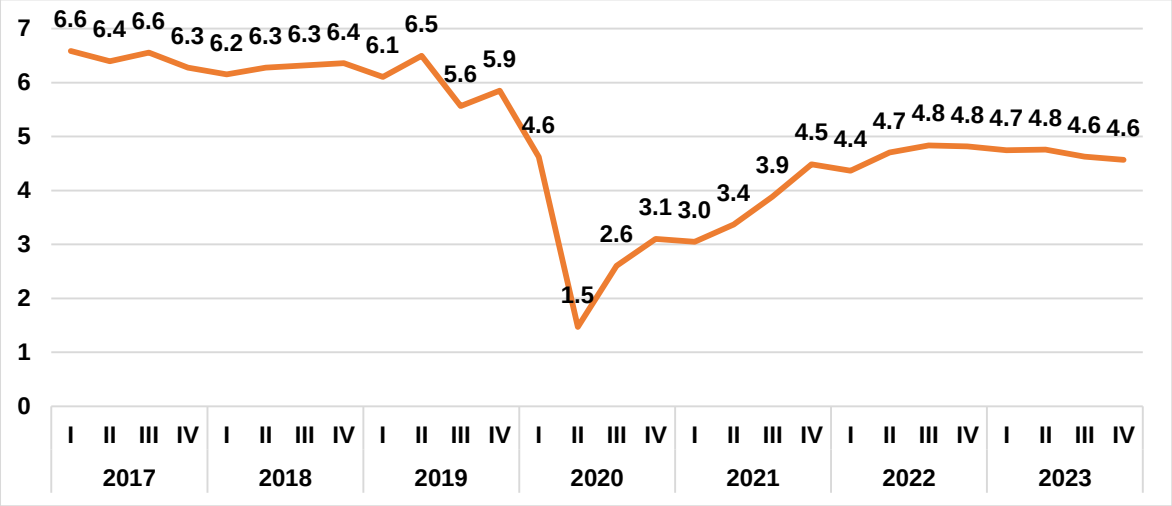
GRÁFICO N° 1: CANTIDAD DE EQUIPOS TERMINALES MÓVILES SUSTRAÍDOS (En miles)



Fuente: RENTESEG - PUNKU
Elaboración: OSIPTEL.

En el siguiente gráfico se observa que el promedio diario de equipos terminales móviles sustraídos se ha mantenido constante entre el 2017 y 2019, y solo ha experimentado una reducción durante el período de confinamiento obligatorio entre el 2020 y parte del 2021. A partir del segundo trimestre del 2021 se aprecia un crecimiento sostenido del promedio diario de sustracciones, aunque todavía no ha llegado a los niveles prepandemia.

GRÁFICO N° 2: PROMEDIO DIARIO DE EQUIPOS TERMINALES MOVILES SUSTRAÍDOS (En miles)



Fuente: RENTESEG - PUNKU
Elaboración: OSIPTEL

Sobre lo anterior, gran parte de los equipos terminales sustraídos son ofertados en el mercado de equipos usados, también denominados equipos de segunda mano. Estos lugares de comercialización se encontrarían bajo la fachada de servicios técnicos y venta de accesorios para dispositivos móviles, y estarían ubicados en mercados, centros comerciales y galerías de distritos como Cercado de Lima[18], Ate Vitarte[19], Carabayllo[20], Puente Piedra[21], entre otros. Cabe señalar que el mercado ilegal de equipos móviles usados también ofrece sus productos a través del canal virtual, por lo que actualmente se pueden adquirir estos equipos a través de sitios web.[22]

FIGURA N° 5: INCAUTACIÓN DE EQUIPOS SUSTRAÍDOS EN ATE VITARTE

Fuente: Ministerio del Interior (2022)

En paralelo, la demanda del mercado de equipos terminales móviles de segunda mano continúa existiendo dado que las personas, posiblemente de escasos recursos o bajo nivel socioeconómico, prefieren adquirir un equipo terminal móvil usado a menor precio en comparación a un nuevo equipo terminal móvil. Al respecto, en noviembre de 2021, el

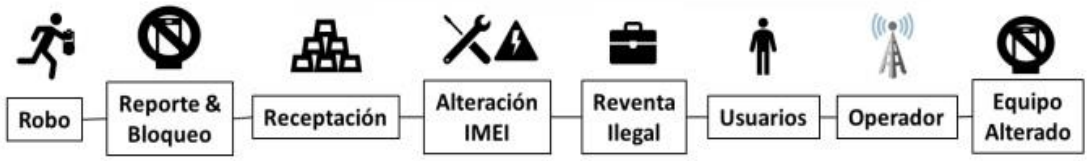
[18] Fuente: APNoticias. Disponible en: https://www.apnoticias.pe/peru/willax/pnp-realiza-campana-de-concientizacion-contra-la-venta-de-celulares-robados-video-640204
[19] Fuente: Ministerio del Interior. Disponible en: https://www.gob.pe/institucion/mininter/noticias/612113-policia-nacional-incauta-mas-de-4-mil-celulares-de-dudosa-procedencia-en-galerias-de-ate-vitarte
[20] Fuente: RPP Noticas. Disponible en: https://rpp.pe/lima/actualidad/carabayllo-pnp-intervino-galeria-donde-se-vendian-celulares-robados-video-noticia-1380797?ref=rpp
[21] Fuente: ATV Noticias. Disponible en: https://www.youtube.com/watch?v=Vt-NS7dx4b0
[22] Fuente: Venta de celulares. Disponible en: https://www.venta-de.com.pe/celulares-gama-alta

precio de un equipo terminal móvil de gama alta fluctuaba entre S/ 800 y S/ 850 en el mercado negro, siendo que su precio en tiendas autorizadas se ubicaba entre los S/ 2000 y S/ 2500 soles. En el caso de equipos terminales móviles de gama media, estos se ofertaban en el mercado negro a un precio no mayor a S/ 500, mientras que su valor original rondaba entre S/ 1 000 y S/ 1 500[23]. Esto evidencia que, para muchos usuarios de bajos niveles económicos, todavía les resulta atractivo adquirir equipos terminales móviles de procedencia dudosa, lo cual incentiva el robo y la delincuencia.

De esta manera, se manifiesta la cadena de valor de equipos terminales móviles sustraídos que tiene como punto de partida el robo del equipo al usuario, el cual se ejecuta mediante modalidades de hurto o robo a mano armada; luego de materializada la sustracción, la victima realiza el reporte al concesionario móvil para el bloqueo del equipo. Una vez obtenido el equipo terminal móvil, el delincuente vende el dispositivo sustraído y el comprador se encarga de la restauración de fábrica del equipo, la alteración del IMEI y, según sea el caso, la sustitución de las partes defectuosas; permitiendo que el equipo terminal móvil se encuentre en condiciones para su comercialización.

Tan pronto como los equipos terminales móviles se encuentren listos para su venta en el mercado ilegal, son distribuidos a todos los establecimientos, galerías o centros comerciales para su comercialización al público. Así, el usuario final adquiere el equipo terminal móvil a un precio menor que en establecimientos autorizados. Esta dinámica ilícita requiere ser detenida no solo con el bloqueo de IMEI inválidos, sino también con el bloqueo de IMEI duplicados o clonados.

FIGURA N° 6: CADENA DE VALOR DE EQUIPOS TERMINALES MÓVILES SUSTRAÍDOS



Fuente: CRC (2019)

4.4.2. Reducción de la cantidad de IMEI inválidos bloqueados

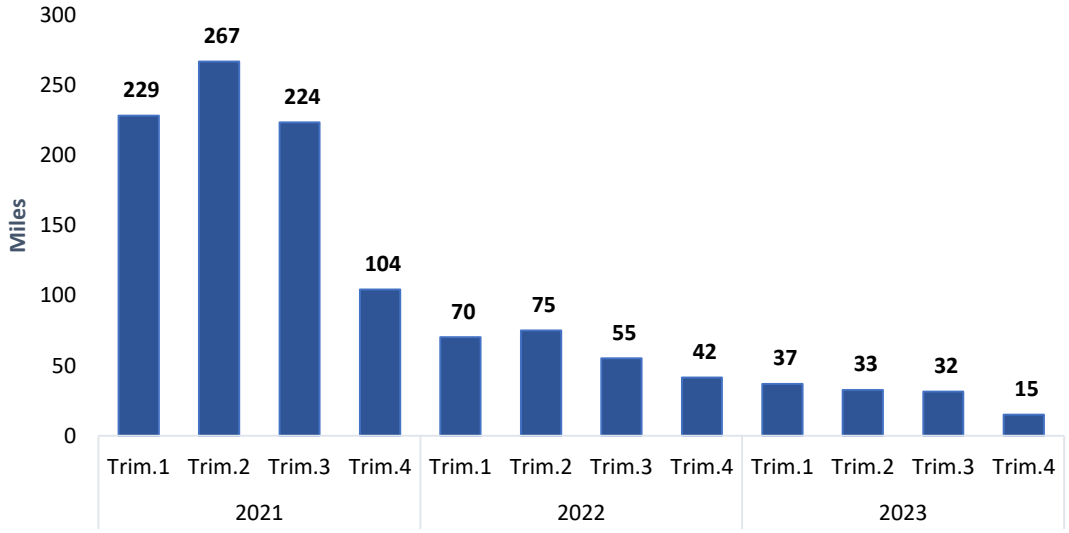
En setiembre de 2018, se inició con la identificación de IMEI inválidos que operan en el Perú, y se implementó el primer bloqueo de 250 000 IMEI inválidos. Mediante la referida medida, el OSIPTEL busca desincentivar la compra de equipos terminales móviles en comercios ilegales. Al respecto, se han registrado un total de 14 548 457 IMEI inválidos bloqueados a noviembre 2023.

Conforme a lo esperado, la mayor cantidad de bloqueos de IMEI inválidos se han realizado durante el 2021, específicamente se bloquearon 823 683 líneas. Como se puede apreciar en el gráfico siguiente, la cantidad de bloqueos en el 2022 y 2021 es notoriamente menor, ello debido a que probablemente la tasa de detección de IMEI inválidos es mayor que la tasa de generación de nuevos casos, lo cual demuestra que este mecanismo de control es eficiente.

Por lo tanto, se evidencia que la medida ha impactado de forma esperada, permitiendo mitigar la cantidad de equipos móviles terminales con IMEI inválido; no obstante, ello ha obligado a que las organizaciones criminales empleen otras técnicas delictivas tales como la clonación de IMEI para poder continuar con la comercialización ilegal de equipos móviles.

[23] Fuente: El Comercio. Disponible en: https://elcomercio.pe/lima/policiales/robo-de-celulares-cada-20-segundos-delincuentes-arrebatan-equipos-moviles-en-las-calles-las-malvinas-noticia/

GRÁFICO N°3: EQUIPOS TERMINALES MÓVILES CON IMEI INVÁLIDOS BLOQUEADOS (en miles)

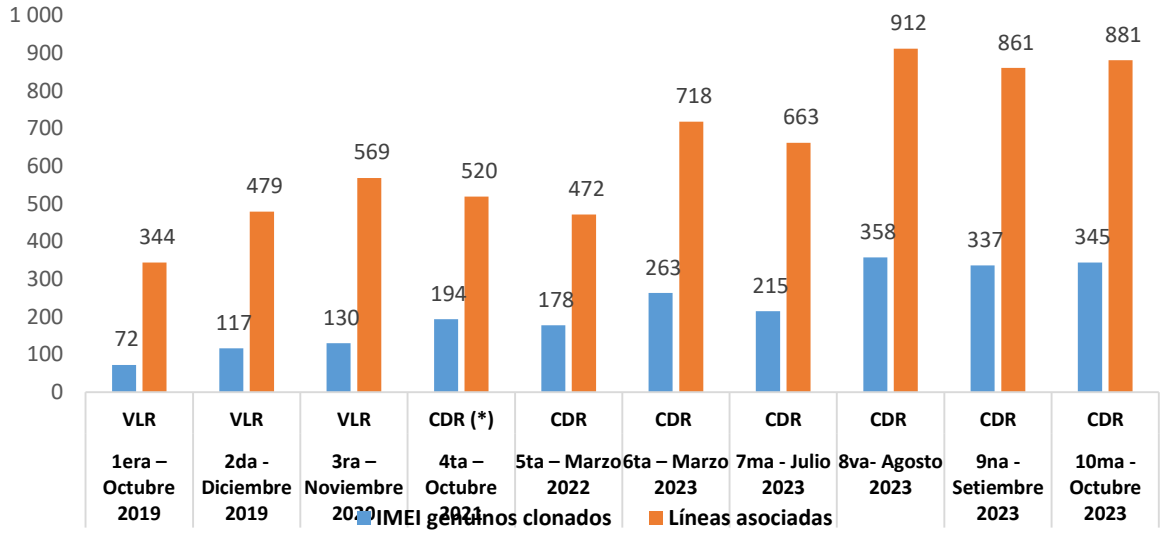


Fuente: RENTESEG
Elaboración: OSIPTEL

4.4.3. IMEI duplicados o clonados detectados intra-red en redes de los concesionarios

Desde octubre 2019 se han ejecutado seis evaluaciones para la detección de IMEI originales o genuinos que han sido clonados intra-red y la cantidad de líneas móviles asociadas a estos IMEI alterados. En el siguiente gráfico, se observa que las tres primeras evaluaciones se realizaron a través de la metodología de Registro de Localización de Visitantes (VLR) que utiliza la información sobre abonados en itinerancia dentro del área de ubicación de un centro de computación móvil; mientras que desde octubre 2021 se viene ejecutando la metodología actual CDR. De esta forma, se evidencia que la cantidad de IMEI identificados como duplicados o clonados en octubre 2023 se ha incrementado en 376% desde la primera evaluación (octubre 2019). Asimismo, la cantidad de líneas asociadas a un IMEI clonado intra-red aumentó en 156% durante el mismo período de análisis.

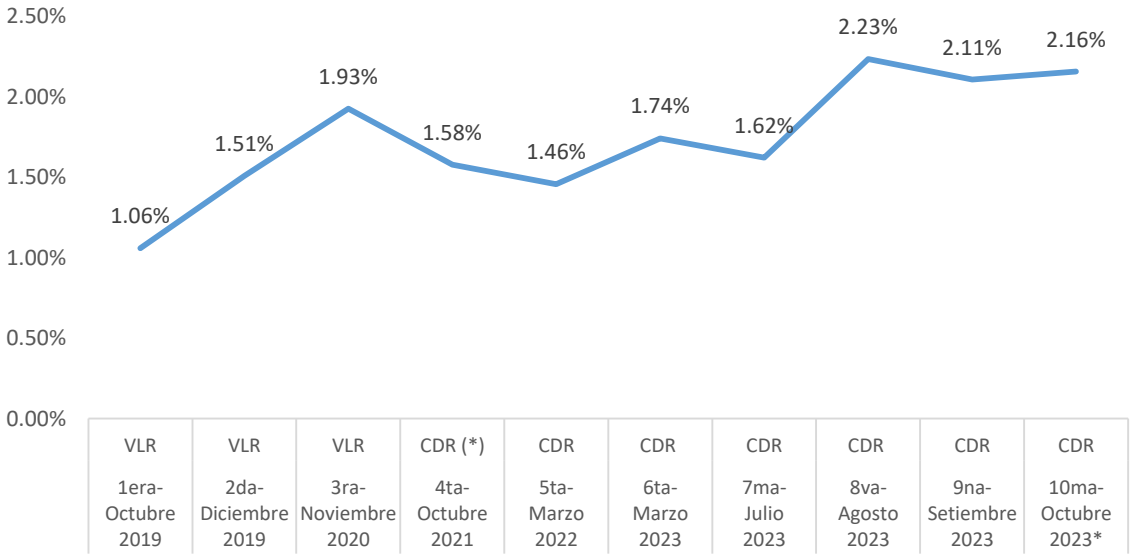
GRÁFICO N° 4: CANTIDAD DE IMEI GENUINOS CLONADOS INTRA-RED Y LINEAS MÓVILES ASOCIADAS (En miles)



Fuente: RENTESEG
Elaboración: OSIPTEL

Ampliando el análisis, en el siguiente gráfico se aprecia la tasa de incidencia de la cantidad de líneas móviles asociadas a un IMEI clonado intra-red respecto a la cantidad total de líneas móviles. Como se puede apreciar en el gráfico N° 4, entre el 2019 y 2023, la tasa de incidencia se mantiene en promedio en 1.7%, aunque se observa un incremento entre el 2022 y 2023, lo cual indicaría que el problema de los IMEI clonados o duplicados se estaría agravando.

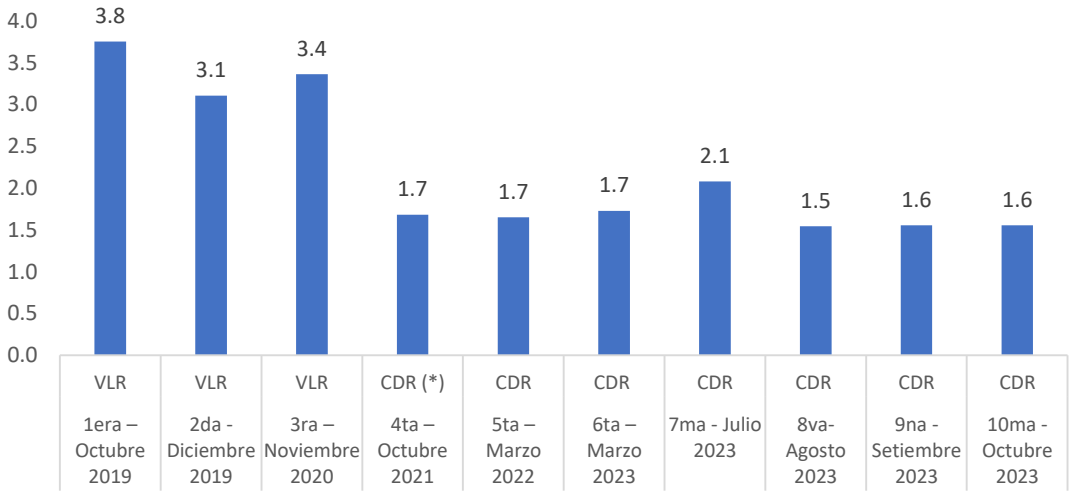
GRÁFICO N° 5: TASA DE INCIDENCIA DE LA CANTIDAD DE LINEAS MÓVILES ASOCIADAS A UN IMEI CLONADO RESPECTO AL TOTAL DE LINEAS MOVILES



Nota: Para el cálculo de la tasa del mes de octubre se considera la cantidad de líneas del último mes disponible (Setiembre 2023).
Fuente: RENTESEG y PUNKU
Elaboración: OSIPTEL

Por otra parte, a partir de la cantidad de IMEI que han sido clonados y la cantidad de líneas asociadas, se estima que un IMEI en promedio puede ser duplicado hasta en 1.6 veces. No obstante, se debe señalar que cerca del 0.3% de estos casos han sido clonados en más de 20 veces, pudiendo generar serios perjuicios a los afectados.

GRÁFICO N° 6: CANTIDAD DE VECES QUE UN IMEI ORIGINAL SE CLONA



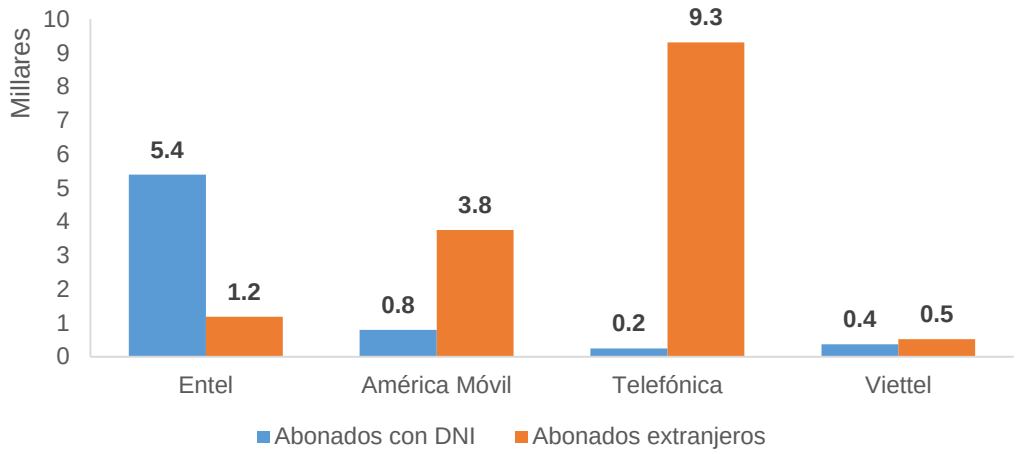
Fuente: RENTESEG
Elaboración: OSIPTEL

4.4.4. Registros inconsistentes de usuarios extranjeros

Durante el último año (julio 2022 a mayo 2023) se identificaron diversos tipos de inconsistencias tales como titulares con nombre y apellidos ininteligibles, con la misma fecha de activación, fechas de activación incongruentes, número de documento legal que incluye caracteres alfabéticos no habituales, etc. Específicamente, se realizó un cotejo entre el Registro de Abonados y la base de datos de la RENIEC y Migraciones, se ha identificado un total de 21 567 registros irregulares, de los cuales 8002 registros corresponden al período noviembre del 2022 a mayo del 2023.

Asimismo, se encontró que del total detectado entre julio del 2022 y mayo del 2023, el 31.5% corresponde a supuestos abonados nacionales y 68.5% a abonados de origen extranjeros. Particularmente, se ha encontrado que los solicitantes podrían presentarse como extranjeros con la finalidad de evitar la verificación biométrica y el contraste con la base de datos de la RENIEC. Cabe señalar que, según el marco normativo vigente, los extranjeros que no puedan pasar la verificación biométrica pueden contratar el servicio público móvil exhibiendo su documento de identidad, no se les requiere dejar una copia física del documento, lo cual impide su posterior identificación.

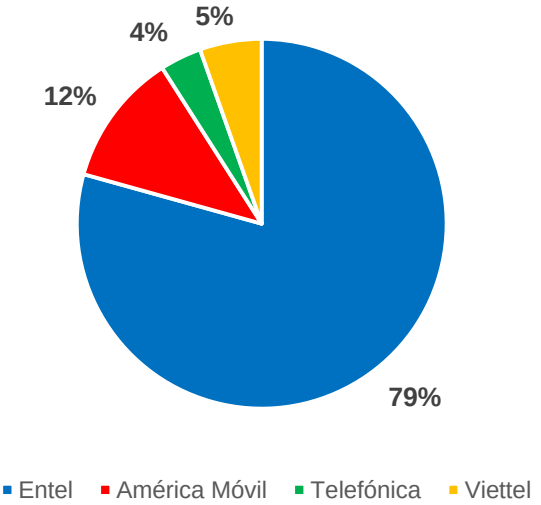
GRÁFICO N° 7: CANTIDAD DE ABONADOS NACIONALES Y EXTRANJEROS QUE PRESENTAN REGISTROS INCONSISTENTES, JULIO 2022 A MAYO 2023(En miles)



Fuente: RENTESEG
Elaboración: OSIPTEL

Ampliando el análisis y considerando los resultados obtenidos a partir de la información remitida por los cuatro concesionarios móviles, se observa que, el 79% del total inconsistencias detectadas en los registros de abonados nacionales corresponde a la empresa Entel, el 12% corresponde a América Móvil, seguido de Telefónica y Viettel con 4% y 5%, respectivamente.

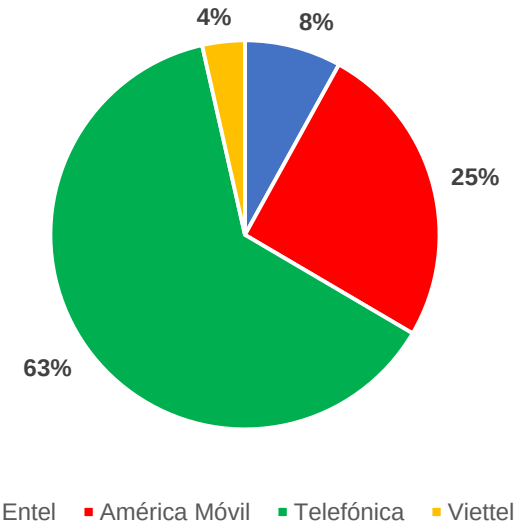
GRÁFICO N° 8: CANTIDAD DE ABONADOS NACIONALES QUE PRESENTAN REGISTROS INCONSISTENTES POR EMPRESA OPERADORA



Fuente: RENTESEG
Elaboración: OSIPTEL

En paralelo, se evidencia que el 63% de la cantidad total de registros de abonados extranjeros detectados como inconsistentes corresponden a la concesionaria móvil Telefónica, seguida de América Móvil con 25%; mientras que las dos empresas operadoras restantes (Entel y Viettel) cuentan el 8% y 4% del total de registros inconsistentes asociados a abonados extranjeros respectivamente.

GRÁFICO N° 9: CANTIDAD DE ABONADOS EXTRANJEROS QUE PRESENTAN REGISTROS INCONSISTENTES POR EMPRESA OPERADORA

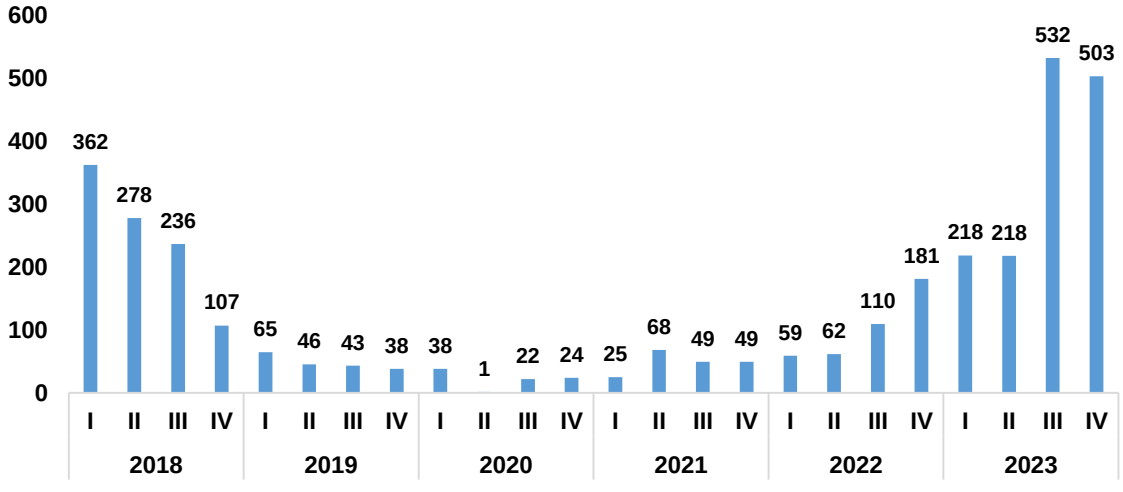


Fuente: RENTESEG
Elaboración: OSIPTEL

4.4.5. Cuestionamientos de titularidad prepago

Como puede observarse, a raíz de las medidas adoptadas para fortalecer las fiscalizaciones por parte del OSIPTEL, la cantidad de cuestionamientos de titularidad presenta una caída en la incidencia trimestral de casos por cada 1 millón de líneas, sin embargo, esta tendencia ha empezado a revertirse y crecer por segundo año consecutivo, sobre todo en un escenario en el cual las suspensiones de las líneas cuestionadas se hacen efectivas en un periodo de 15 días calendario en el cual los delincuentes pueden seguir operando.

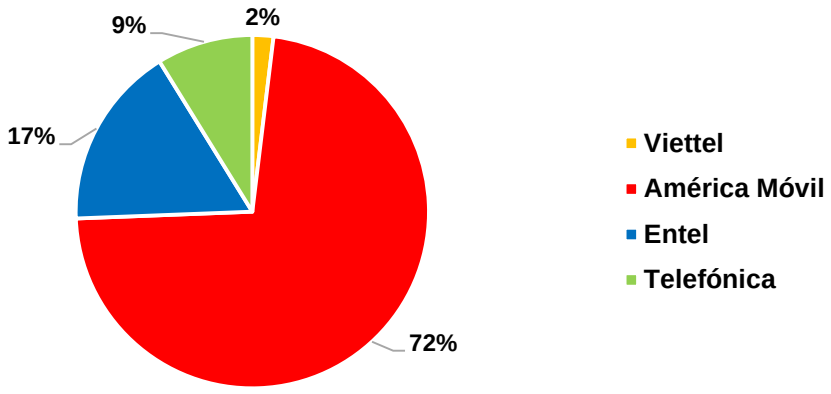
GRÁFICO N° 10: INCIDENCIA TRIMESTRAL DE CUESTIONAMIENTO DE TITULARIDAD PREPAGO (Cada 1 millón líneas)



Fuente: RENTESEG
Elaboración: OSIPTEL

Respecto a la distribución de los casos, se observa que América Móvil es la empresa que cuenta con la mayor cantidad de cuestionamientos de titularidad prepago (72%), seguido de Entel con el 17%, Telefónica con el 9% y Viettel con el 2%.

GRÁFICO N° 11: DISTRIBUCIÓN DE LOS CUESTIONAMIENTOS DE TITULARIDAD PREPAGO, POR EMPRESA (2017- 2023)



Nota: La información 2023 se encuentra a noviembre.
Fuente: RENTESEG
Elaboración: OSIPTEL

4.5. Causas del problema

En esta sección se analizan las causas que explican las problemáticas de los equipos terminales móviles que contengan un código IMEI clonado y las inconsistencias en el registro. Específicamente, se han identificado las siguientes causas: (a) facilidad de acceso a las técnicas de clonación por comercializadores, (b) preferencia por equipos móviles en el mercado negro, (c) vulnerabilidad de las bases de datos de IMEI válidos, (d) dificultades para identificar al abonado con el IMEI original, (e) incremento en la cantidad de abonados de origen extranjero y (g) falta de integración entre los procesos de verificación, contratación, registro y conservación de contratos.

4.5.1. Facilidad de acceso a las técnicas de clonación por comercializadores

Los comercializadores cuentan con fácil acceso a las diversas técnicas de clonación, esto se debe a que existen sitios web[24], videos[25], blog, tutoriales y aplicaciones específicas con información necesaria para obtener un IMEI original válido y replicarlo en otro equipo terminal móvil (Kumar, et al., 2015).

Cabe indicar que, estos métodos de clonación de libre acceso asumen costos reducidos, a diferencia del costo de adquirir un nuevo equipo terminal móvil de forma lícita (Kumar, et al., 2015), por lo que algunas personas prefieren utilizar estas herramientas a fin de ahorrarse un determinado monto de dinero. Al respecto, se evidencia que las herramientas de clonación de IMEI con mayor oferta en el mercado son las cajas de liberación, dado que estas son comercializadas a través de sitios web donde se detallan características, funciones y precio de los dispositivos[26].

[24] Foro sobre clonación de IMEI: clonación de | de IMEI Foros de XDA (xda-developers.com)
[25] Enlace de video sobre cómo cambiar de IMEI. (How to Change IMEI Number on Android Mobile 100% Verified - Mobile imei number Changer). Disponible en: https://www.youtube.com/watch?v=r9YTFnFglrQ
[26] Disponible en: https://deviceservices.org/

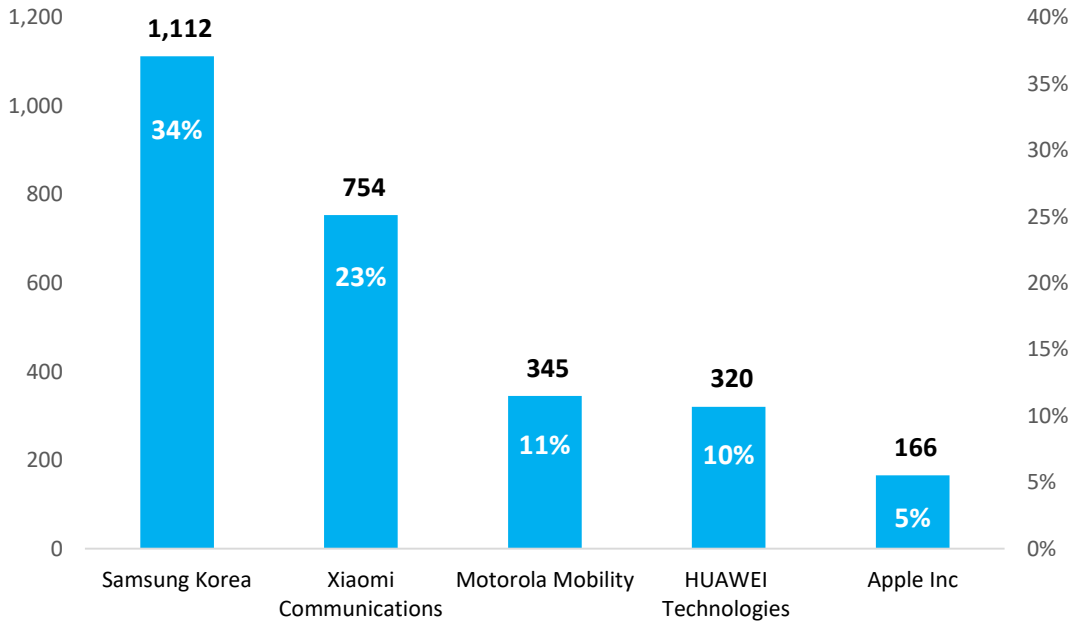
4.5.2. Preferencia por equipos móviles en el mercado negro

Según el estudio realizado por Dominio Consultores, durante el primer semestre de 2022, Samsung, Xiaomi y Motorola fueron las marcas con mayor participación de mercado alcanzando cuotas de 36.8%, 29.5% y 9.6%, respectivamente[27]. En ese sentido, al contar con una mayor cuota de mercado, estas marcas tenderían a ser más demandadas por las organizaciones criminales.

En paralelo, el mercado negro de equipos móviles ofrece la comercialización de cajas de liberación de las principales marcas de fabricantes tales como Samsung, LG, Alcatel, Huawei, Motorola, etc.[28], situación que facilitaría la clonación de códigos IMEI específicos para cada tipo de dispositivo. De esta forma, las organizaciones criminales tendrían mayores facilidades para satisfacer la demanda por equipos terminales móviles en el mercado negro.

En ese sentido, de acuerdo a las estadísticas del RENTESEG, del total de equipos terminales móviles reportados como sustraídos a noviembre del 2023, el 34% corresponde al fabricante Samsung, seguido de Xiaomi con el 23%, Motorola con el 11%, Huawei y Apple con 10% y 5%, respectivamente.

GRÁFICO N° 12: PRINCIPALES MARCAS DE FABRICANTE DE EQUIPOS REPORTADOS COMO SUSTRAÍDOS A NOVIEMBRE 2023 (En miles)



Fuente: RENTESEG
Elaboración: OSIPTEL

4.5.3. Vulnerabilidad de las bases datos conteniendo IMEI válidos

En el mercado ilegal de equipos móviles se ofrecen herramientas como las cajas de liberación que incorporan un listado de IMEI válidos que puede ser replicados en cualquier equipo terminal. Esto implicaría que, en la realidad, existe un mercado negro de

[27] Disponible en: https://rpp.pe/tecnologia/moviles/el-mercado-de-celulares-en-el-peru-se-contrae-y-samsung-sigue-siendo-el-lider-noticia-1423932#:~:text=Tanto%20Samsung%20como%20Xiaomi%20importaron,36.8%25%20de%20participaci%C3%B3n%20del%20mercado.
[28] Disponible en: https://all-spares.com/es/gsm/boxes-and-dongles/

información en el cual se intercambian bases datos de IMEI válidos[29], obtenidos mediante la sustracción ilegal de datos[30] o establecimientos de venta de equipos terminales móviles.

De esta manera, se observa la posible deficiencia en la seguridad y confidencialidad de las bases de IMEI; generando un mayor grado de desprotección en los abonados que cuentan un equipo terminal móvil con IMEI válido.

4.5.4. Dificultades para identificar al abonado con el IMEI original

A diferencia del bloqueo de los equipos terminales móviles reportados como sustraídos o los equipos terminales móviles con IMEI inválidos, en el caso de los IMEI clonados no basta con identificar qué IMEI han sido bloqueados, sino que se requiere identificar cuál es el abonado del IMEI original. En efecto, ante la identificación de un IMEI clonado, la empresa operadora tendría ante sí a 2 o más abonados de líneas móviles que podrían ser el abonado del IMEI original y, por tanto, tendría que determinar cuál de ellos es el original, antes de bloquearlos.

En este contexto, las empresas operadoras podrían enfrentar considerables dificultades, debido a que muchos abonados no conservan los comprobantes de pago por adquisición de equipos o no recuerdan su número IMEI. Incluso, la dificultad se podría incrementar si se considera que los IMEI clonados no necesariamente corresponden a equipos con fecha de fabricación reciente, por lo que podría dificultar que el abonado del IMEI original no pueda demostrar que es el legítimo propietario del IMEI.

En línea con lo anterior, los equipos terminales móviles con IMEI clonados o duplicados representan un desafío para las agencias de seguridad y entes reguladores, dado que es complejo identificar y rastrear de manera única los dispositivos específicos que pueden ser ofrecidos en el mercado afectando a abonados incautos o que fueron adquiridos por abonados malintencionados.

Esto último, incentivaría el robo o hurto de equipos terminales móviles por parte de organizaciones criminales debido a que los valores de reventa de los dispositivos móviles robados serían lucrativos, ya que la clonación del número IMEI tiene el potencial de hacer que los dispositivos robados sean difíciles de rastrear y que funcionen libremente en las redes móviles.

4.5.5. Incremento en la cantidad de abonados de origen extranjero y la falta de validación adecuada

Según datos reportados por Naciones Unidas[31], para el 2021, se estimó que en el Perú residían 1 347 893 migrantes internacionales en territorio nacional, lo que representa el 4% del total de la población peruana[32]. Cabe señalar que el 86.8% de los migrantes internacionales son venezolanos, el 3.3% colombianos y 1.1% ecuatorianos.

En ese contexto, se debe resaltar el aumento de migrantes que ingresaron a través de forma ilegal y que, probablemente, no se encuentren registrados en las bases de datos de la Superintendencia Nacional de Migraciones.

[29] Página web que ofrece códigos IMEI válidos. Disponible en: https://www.clangsm.com/forum/index.php?showtopic=497145

[30] Robo de datos privados, IMEI y el PIN de clientes de T-Mobile https://www.adslzone.net/noticias/seguridad/robo-datos-privados-t-mobile-agosto-2021/

[31] INEI (2022). PERÚ: Estadísticas de la emigración internacional de peruanos e inmigración de extranjeros 1990-2021.

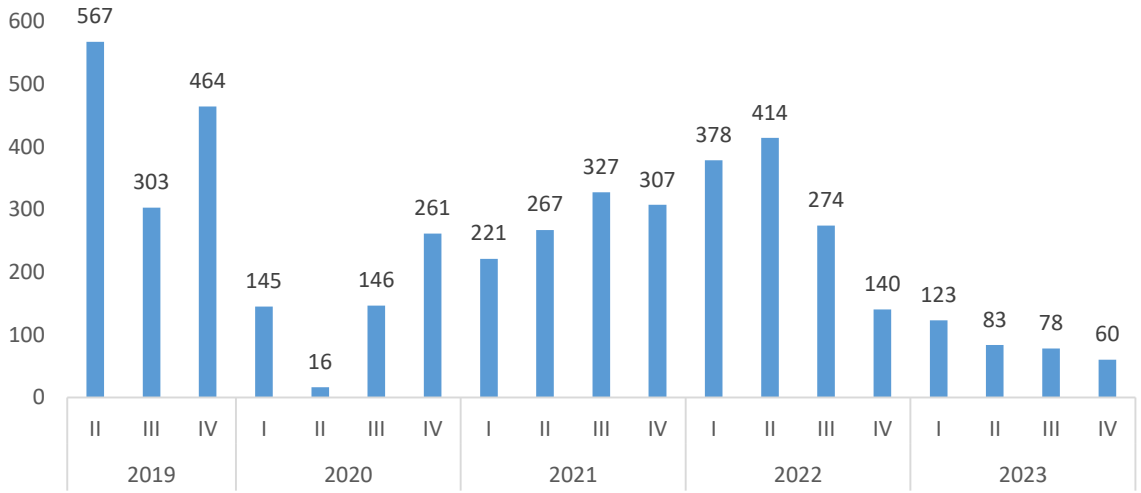
[32] Según las estimaciones y proyecciones del INEI, para el 2022, el Perú tiene una población de 33 396 698 habitantes. Disponible en: https://www.gob.pe/institucion/inei/informes-publicaciones/3464927-peru-proyecciones-de-poblacion-total-segun-departamento-provincia-y-distrito-2018-2022

De igual modo, el aumento en la cantidad de migrantes internacionales en el país se ha visto reflejado en el incremento de abonados registrados de origen extranjero. Así, en el siguiente gráfico se observa un crecimiento sostenido en el número de abonados extranjeros desde el segundo trimestre del 2020, período donde se estableció la emergencia sanitaria debido a la propagación del Covid-19. Se debe precisar que entre el segundo trimestre del 2021 y 2022, el número de abonados extranjeros se incrementó en 55%.

No obstante, el número de abonados de origen extranjero reportados por las concesionarias móviles implicaría un aumento en el número de registros inconsistentes o erróneos. Esto se debería a que, durante el procedimiento de validación de la identidad del abonado extranjero, usualmente, no era posible realizar una validación con la autoridad competente de Migraciones. Por tal motivo, el proceso de registro de los datos personales no era el óptimo, lo que generaba el surgimiento de titulares con un número de documento legal (pasaporte o carne de extranjería) incorrecto o inclusive falsificado.

En línea con lo anterior, se debe mencionar que esto generaba incentivos para que abonados nacionales se hicieran pasar por extranjeros con la finalidad de evitar la verificación biométrica y así poder adquirir un servicio móvil de manera rápida e irregular. Esta técnica podría haber sido aprovechada por individuos que forman parte de organizaciones criminales, para obtener una línea móvil sin ser plenamente identificados y así ejecutar conductas delictivas tales como la extorsión mediante llamadas telefónicas[33].

GRÁFICO N° 13: CANTIDAD DE ABONADOS DE ORIGEN EXTRANJERO REPORTADOS EN EL REGISTRO DE ABONADOS (En miles)



Fuente: RENTESEG
Elaboración: OSIPTEL

4.5.6. Falta de integración o mejora en los procesos de verificación, contratación, registro y conservación de contratos

Otra casuística que se manifiesta sería la falta de integración o mejora entre los procesos de verificación, contratación, registro y conservación de la información registrada en el Registro de Abonados de las empresas operadoras.

Con relación al proceso de verificación de la identidad del abonado, podrían existir interrupciones en el sistema de verificación que impide la correcta identificación del

[33] Fuente: La República. Disponible en: https://larepublica.pe/sociedad/2022/07/07/arequipa-18-denuncias-de-extorsion-se-presentaron-en-solo-48-horas-lrsd

abonado, así como el incentivo para que individuos malintencionados que pretenden adquirir un servicio móvil puedan hacerlo de forma rápida y sin restricciones.

En lo que concierne al registro de información, es necesario que las empresas operadoras cuenten con el personal responsable de captar los datos de los abonados y que sea oportunamente capacitado para el procedimiento de recopilación de datos, de tal forma que la probabilidad de error en los datos sea nula o mínima.

Por último, las empresas operadoras enfrentan la necesidad de mejorar sus sistemas de seguridad de datos personales de los abonados, dado que, actualmente, existen altos riesgos de ser víctimas de robo o manipulación de información por parte de los *hackers* con el objetivo de realizar fraudes utilizando el servicio móvil del abonado[34].

Respecto a este punto, se debe señalar que, las reglas de excepción de la verificación biométrica serían una brecha de seguridad, dado que permitiría que los ciudadanos extranjeros puedan obtener una línea móvil sin identificarse. Asimismo, se ha encontrado que las empresas operadoras están realizando la entrega de la contraseña única mediante procesos sin parámetros mínimos, lo cual implica un riesgo para los usuarios.

4.6. Permanencia del problema en caso de no intervención

De permanecer la situación actual de la problemática de IMEI duplicados o clonados, la cantidad de equipos terminales móviles sustraídos continuaría en aumento, debido a que los delincuentes emplearían las mencionadas técnicas de alteración para ejecutar la implantación de un número IMEI válido que permita la habilitación del equipo terminal móvil, previamente sustraído o perdido, en la red móvil. Incluso, considerando que el acceso a las técnicas de clonación no es prohibitivo ni costoso, es posible que la cantidad de IMEI clonados aumente, y con ello se dificulte lograr el objetivo de frenar el robo o sustracción de equipos terminales móviles.

En tal contexto, al no implementarse el procedimiento de bloqueo de equipos terminales móviles por IMEI clonado o duplicado, y no establecerse el proceso de cuestionamiento de bloqueo respectivo; la cantidad de equipos terminales móviles conteniendo un código IMEI duplicado o clonado se incrementaría en gran medida.

En consecuencia, se generaría un mayor nivel de desprotección a los abonados que adquirieron el equipo terminal móvil de forma licita, así como también una afectación a aquellos abonados propietarios de equipos terminales móviles con el IMEI original que han sido víctimas de clonación, debido a que podrían estar relacionados a algún tipo de acto delictivo realizado a través de un equipo terminal móvil asociado al mismo IMEI.

Adicionalmente, se producirían retrasos o errores en las respuestas a los requerimientos de información solicitados por las entidades públicas como el Poder Judicial, Ministerio del Interior y la Policía Nacional; dado que, frecuentemente, se requiere la validación de la titularidad de un IMEI o servicio móvil mediante la aplicación del principio de verdad material.

Considerando lo anteriormente expuesto, la afectación al abonado se manifestaría a través de un mayor tiempo de bloqueo del equipo terminal móvil, debido a que su solicitud de cuestionamiento no cuenta con la respuesta del OSIPTEL en un plazo razonable. Asimismo, los abonados que no presenten datos correctamente registrados podrían ser, erróneamente, objeto de investigación o acusación por parte de alguna entidad.

[34] Fuente: https://urgente24.com/omni/nuevo-tipo-ciberataque-el-sim-swapping-y-como-evitarlo-1540445

5. OBJETIVO DE LA INTERVENCIÓN Y BASE LEGAL

5.1. Objetivo general de la intervención

Mejorar los niveles de seguridad para los abonados en la adquisición y uso de equipos terminales móviles, así como reducir la problemática de información asimétrica en la contratación y corregir la rigidez del mercado respecto a las barreras de salida que enfrentan los abonados y usuarios.

5.1.1. Objetivos específicos

- Objetivo 1: Desincentivar el uso y la adquisición de equipos terminales móviles de origen dudoso y que probablemente hayan sido duplicados o clonados.
- Objetivo 2: Mejorar los niveles de idoneidad y autenticidad de la información reportada por las empresas operadoras en el registro de abonados.
- Objetivo 3: Facilitar la entrega de la contraseña única a través de un proceso seguro y confiable.
- Objetivo 4: Reducir los escenarios en los que la delincuencia puede utilizar una línea prepago contratada a nombre de otra persona.

5.2. Base legal

La base legal para la intervención del OSIPTEL respecto de la problemática analizada está dada por los siguientes artículos:

- Artículo 3 de la Ley N° 27332 - Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos – modificada por las Leyes Nº 27631 y Nº 28337, el cual establece que el OSIPTEL tiene asignada, entre otras, la función normativa, que comprende la facultad de dictar, en el ámbito y en materia de sus respectivas competencias, los reglamentos, normas que regulen los procedimientos a su cargo, otras de carácter general y mandatos u otras normas de carácter particular referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de sus usuarios, así como la facultad de tipificar las infracciones por incumplimiento de obligaciones.
- Artículo 18 del Reglamento General del OSIPTEL, aprobado por Decreto Supremo N° 008-2001-PCM y modificatorias, el cual indica que este Organismo tiene la facultad de regular y normar el comportamiento de las empresas operadoras en sus relaciones con los usuarios.
- Artículo 24 del Reglamento General, el cual señala que el Consejo Directivo del OSIPTEL es el órgano competente para ejercer de manera exclusiva la función normativa y conforme al inciso b) del artículo 75 del citado Reglamento dispone que es función del Consejo Directivo del OSIPTEL, el expedir normas y resoluciones de carácter general o particular, en materia de su competencia.
- Quinta Disposición Complementaria Final del Decreto Legislativo N° 1338, Decreto Legislativo 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” el cual establece que el OSIPTEL, el Ministerio del Interior y la Policía Nacional del Perú, en el marco de sus competencias, dictan las normas complementarias que resulten necesarias para la implementación de las disposiciones establecidas en el dicho decreto legislativo y su reglamento.

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

- Artículo 4 del Reglamento del Decreto Legislativo N° 1338, el cual indica que los procedimientos necesarios que permitan la operatividad de la Lista Blanca y la Lista Negra son establecidos por el OSIPTEL y son de cumplimiento obligatorio.
- Numeral 1.3 del Anexo 5 de la Norma de Condiciones de Uso, el cual establece que la empresa operadora tiene la obligación de suministrar al abonado y al OSIPTEL, cuando le sea requerido, la información que acredite la solicitud y/o aceptación de los actos señalados en el punto 1.1. del citado anexo.
- Numeral 2.7 del Anexo 5 de la Norma de Condiciones de Uso, el cual establece que la empresa operadora debe llevar un registro actualizado de los abonados que hubieran contratado servicios bajo la modalidad prepago, control y/o pospago.

6. ANÁLISIS DE LAS ALTERNATIVAS

En esta sección se detalla las alternativas de solución a la problemática descrita y su respectiva evaluación para poder seleccionar la que mayor beneficio otorgue a la sociedad.

6.1. Descripción de las alternativas

Considerando la problemática expuesta y los objetivos definidos previamente, en esta sección se propone evaluar las siguientes alternativas:

6.1.1. Alternativa 1: Mantener el esquema regulatorio vigente

Respecto a la problemática expuesta, el marco normativo vigente ha establecido las siguientes obligaciones:

- Existe un procedimiento técnico para la identificación de IMEI duplicados o clonados; sin embargo, no se dispone de un procedimiento para su bloqueo. Esto implica que para reducir la incidencia de IMEI duplicados o clonados, la única opción disponible es el desarrollo de campañas informativas con el objetivo de concientizar a los abonados acerca de los riesgos de adquirir equipos terminales móviles usados.
- Se establece los supuestos de excepción a la verificación biométrica. En el caso del solicitante del servicio nacional con discapacidad física o falla de conectividad de RENIEC debe presentar una declaración jurada con campos de información obligatorios, lo cual no es exigible si en los casos de falla de conectividad la empresa operadora conserva la huella digital del solicitante para una posterior validación.
- La entrega de la contraseña única se encuentra regulada de forma general.
- En caso de cuestionamiento de titularidad prepago, el usuario solicita la desvinculación con la línea y la empresa operadora tiene 2 días hábiles para ejecutar la solicitud. Sin embargo, el servicio móvil se mantiene activo por 15 días hábiles a fin de que el usuario pueda regularizar la titularidad de la línea, en caso contrario se ejecuta la suspensión del servicio cuestionado.

Ventajas:

- No hay riesgo de bloquear el IMEI del abonado original.
- No genera costos de cuestionamientos de bloqueo de equipo a los abonados, ni pérdida de ingresos a las empresas operadoras.
- Cada empresa operadora puede diseñar el proceso de entrega de contraseña única en función de sus características tecnológicas y disponibilidad de recursos.

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

- El procedimiento para las personas que no pueden pasar la verificación biométrica, o cuando no está disponible la conectividad con la RENIEC es accesible y no es demasiado restrictivo respecto al derecho de acceso a los servicios públicos de telecomunicaciones.
- El usuario obtiene la desvinculación de la línea cuestionada en un plazo de 2 días hábiles.
- Se brinda a los usuarios, cuya titularidad de línea ha sido cuestionada, un período de 15 días hábiles para que regularice.

Desventajas

- Los IMEI duplicados o clonados van permanecer activos y probablemente la cantidad de IMEI duplicados o clonados seguirían incrementándose.
- La clonación de IMEI va continuar estimulando la incidencia de robo de equipos, sustracción de datos personales, extorsiones y fraudes bancarios.
- No hay garantía de que los abonados voluntariamente eviten adquirir equipos con IMEI duplicados o clonados.
- No existen garantías que las reglas que definen las empresas operadoras para la entrega de la contraseña única no generen mayores riesgos de seguridad a los usuarios o limiten su acceso hacia todos los usuarios.
- La delincuencia podría aprovechar las reglas excepcionales de verificación de identidad, y se seguiría observando registros inconsistentes en la lista de abonados.
- Los delincuentes pueden hacer uso de líneas prepago para cometer delitos y luego, desvincularse a través del procedimiento de cuestionamiento prepago.

6.1.2. Alternativa 2: Bloqueo de IMEI.

Considerando el análisis de la problemática y sus causas, se ha formulado la siguiente alternativa de solución:

CUADRO N° 1: DESCRIPCIÓN DE LA ALTERNATIVA 2

Objetivo	Alternativa de solución	Ventajas	Desventajas
Objetivo 1: Desincentivar el uso y la adquisición de equipos terminales móviles de origen dudoso y que probablemente hayan sido clonados.	Para este objetivo se han identificado dos alternativas de solución distintas a la alternativa 1:		
	Alternativa 2.1: Bloqueo de IMEI duplicado o clonado sin procedimiento previo de identificación	• El proceso de depuración de IMEI duplicados o clonados es más rápido, y solamente se van a desbloquear aquellos equipos terminales móviles en los que los abonados tienen como demostrar que son los titulares originales. En ese sentido, el procedimiento de cuestionamiento permite corregir solo aquellos casos en los que el bloqueo afectó al abonado que sí era propietario de ese número de IMEI. • El cuestionamiento es un proceso conocido por los abonados y las empresas operadoras, por lo que no debería requerir de un gran período de implementación o adecuación. • El bloqueo inmediato de IMEI duplicados o clonados podría desincentivar a los abonados a seguir comprando equipos de origen dudoso o ilícito, dado que podrían quedarse con equipos bloqueados e inservibles.	• Los propietarios originales del IMEI no van a poder hacer uso del servicio público móvil mientras dure el bloqueo. • Se debería esperar un incremento en la tasa de cuestionamientos exitosos, lo cual también puede suponer una mayor carga de trabajo para las áreas encargadas de esa evaluación dentro de las empresas operadoras y en el regulador. • La obligación de presentar el cuestionamiento de manera presencial podría generar costos de viaje y de espera a los abonados.
	Alternativa 2.2: Bloqueo de IMEI duplicado o clonado con procedimiento previo de identificación	• Se brinda a los propietarios originales del número IMEI la oportunidad de evitar la suspensión del servicio y el bloqueo del equipo terminal. • Se procura que la cantidad de cuestionamientos sea menor, dado que los que no se acogieron a la verificación previa probablemente tampoco realicen el cuestionamiento.	• Considerando que los abonados van a poder solicitar la verificación previa y el cuestionamiento, es probable que se incrementen los costos administrativos. • La obligación de presentar el cuestionamiento de manera presencial podría generar costos de viaje y de espera a los abonados.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Objetivo 2: Mejorar los niveles de idoneidad y autenticidad de la información reportada por las empresas operadoras en el registro de abonados.	Para los tres supuestos en los que aplican las reglas de excepción de la verificación biométrica, se propone añadir la obligación de conservar una copia del documento legal del solicitante.	• Eleva las medidas de seguridad en el caso de las de las excepciones a la verificación biométrica. • Mejora la capacidad del OSIPTEL para evitar que existan registros inconsistentes en la lista de abonados.	• Genera costos de almacenamiento de copias de documentos de identidad.
Objetivo 3: Facilitar la entrega de la contraseña única a través de un proceso seguro y confiable.	Se establece un procedimiento de entrega de contraseña única	• Brinda predictibilidad sobre el proceso de entrega de la contraseña única, reduciendo los riesgos de los usuarios en el proceso de activación de la referida contraseña.	• En un escenario de cambio tecnológico, el procedimiento de entrega de contraseña única podría desfasarse; y las empresas operadoras no podría adaptarse debido a que se encuentra a nivel de norma.
Objetivo 4: Reducir los escenarios en los que la delincuencia puede utilizar una línea ago contratada a bre de otra ona	Se elimina el procedimiento de cuestionamiento prepago para que este tipo de problema se atienda como un reclamo.	• Simplificación procedimental. • Serán atendidos como reclamos por contratación no solicitada.	• El reclamo por contratación se resuelve en un plazo mayor al del cuestionamiento prepago. • Se evita el uso de las líneas prepago para delinquir, dado que ya no podrán desvincularse del equipo rápidamente.

oración: OSIPTEL.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

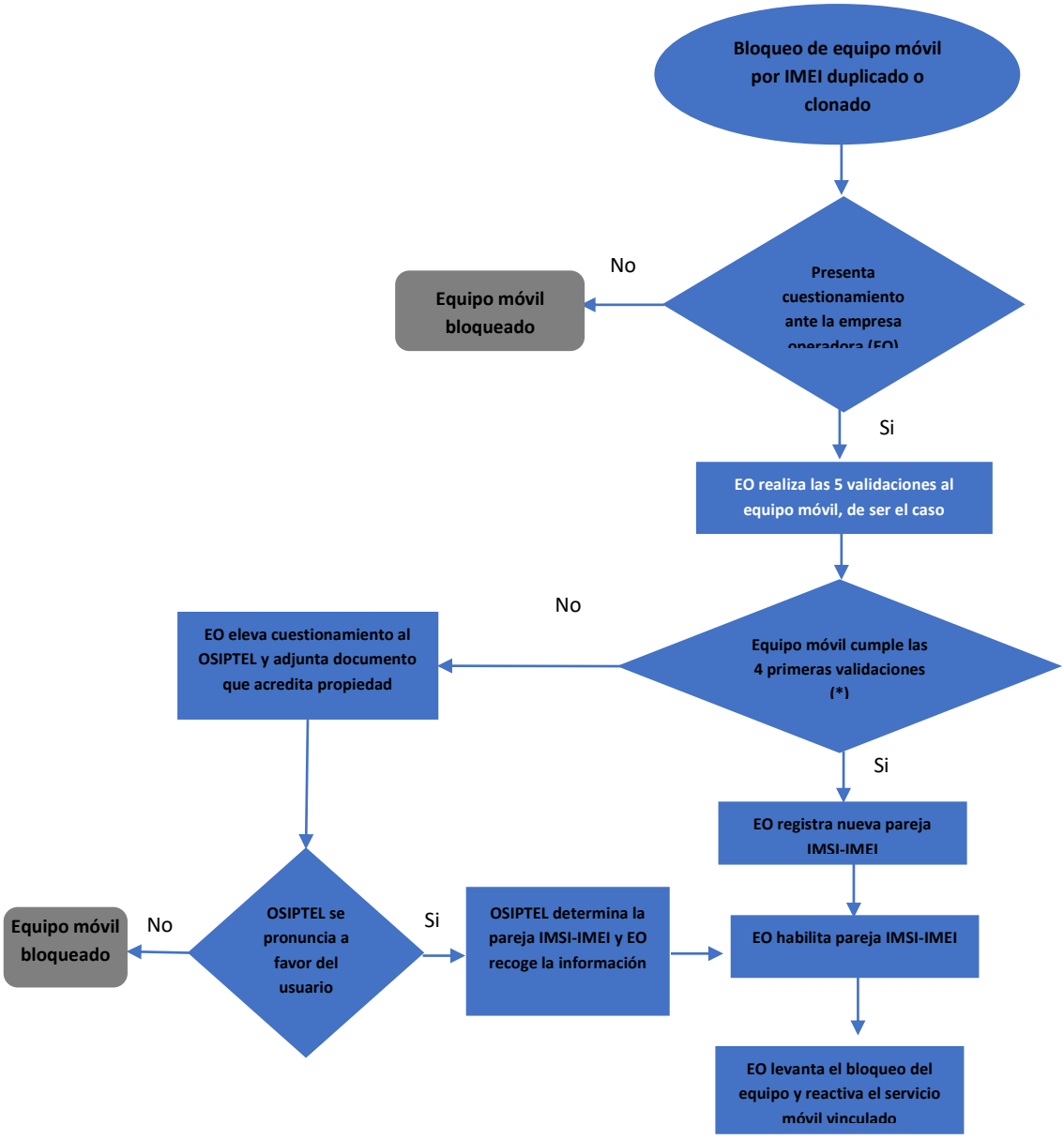
OSIPTEL DAPU M.GONZALEZ

A continuación, se brinda mayor detalle sobre las principales alternativas:

a) Alternativa 2.1: Bloqueo de IMEI duplicado o clonado sin procedimiento previo de identificación

En esta alternativa, se establece un procedimiento ex post de evaluación de cuestionamiento al bloqueo por IMEI duplicado o clonado, no se brinda al usuario una opción previa de evitar el bloqueo. Este procedimiento se detalla en el siguiente diagrama:

FIGURA N° 7: ALTERNATIVA 2.1: BLOQUEO DE IMEI CLONADO O DUPLICADO SIN PROCEDIMIENTO DE IDENTIFICACIÓN PREVIA



(*) i) identidad del abonado del servicio móvil, (ii) coincidencia del IMEI físico y lógico, (iii) SIM Card del servicio móvil de abonado corresponda a un servicio registrado bajo su titularidad y que este se encuentre vinculado al equipo terminal y (iv) coincidencia del TAC (marca y modelo) del equipo terminal móvil con sus respectivas características físicas.
Elaboración: OSIPTEL

Asimismo, las empresas operadoras deben evaluar el cuestionamiento mediante diversas validaciones[35], y adicionalmente validar la adquisición del equipo terminal en sus sistemas comerciales, de ser el caso. Cabe señalar que, en caso el abonado no esté conforme con la decisión de la empresa operadora, este podría elevar el cuestionamiento al OSIPTEL, solicitándole al abonado el comprobante de pago que acredite la adquisición de su equipo previamente para remitirlo. Los principales cambios en el procedimiento de cuestionamiento de bloqueo de equipos son los siguientes:

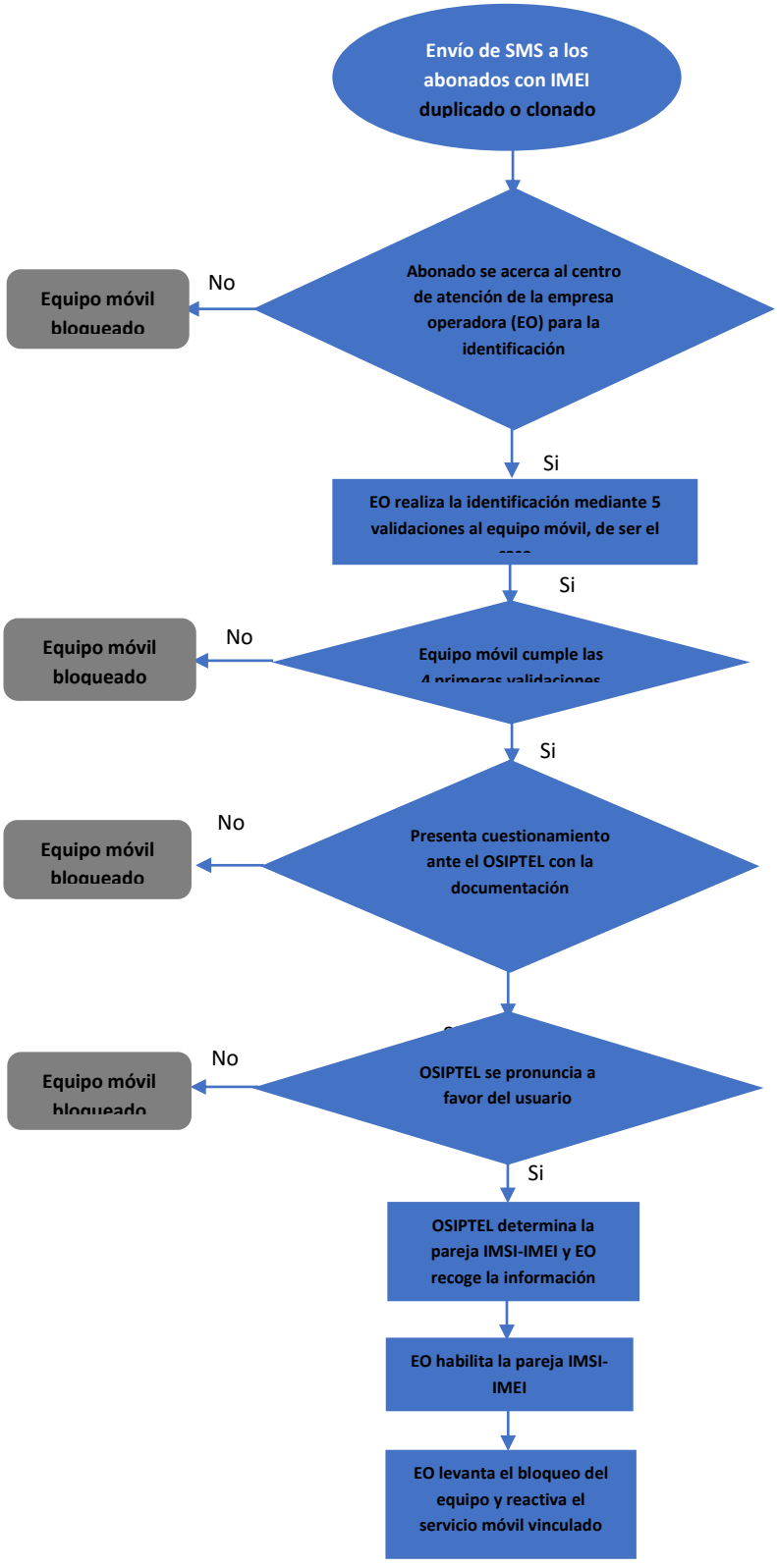
- Validar identidad mediante verificación biométrica o contraseña única.
- Cotejar coincidencia TAC (marca / modelo) con características físicas.
- Verificar en el sistema comercial que el equipo fue adquirido por el abonado.
- Los 4 criterios de validación no aplican cuando (i) no está la lista blanca, (ii) está en la lista negra y (iii) disposiciones para equipo extranjero.
- Si el bloqueo se realizó por tener un IMEI clonado/duplicado, el equipo se habilita solo con el servicio que tiene vinculado a la fecha.
- Concesionario reporta el IMEI-IMSI a la lista de excepción del OSIPTEL.
- Entrega de constancia de procedencia o no del cuestionamiento.
- En el caso de la elevación de cuestionamiento, el concesionario debe brindar constancia de cuestionamiento.
- 2 días para que la empresa operadora remita la documentación. Previamente, la empresa operadora solicita comprobantes de pago del equipo.
- El OSIPTEL se pronuncia sobre el cuestionamiento en un plazo de 10 días.

b) Alternativa 2.2: Bloqueo de IMEI duplicado o clonado con procedimiento previo de identificación

En esta alternativa, las empresas operadoras deben remitir un SMS a los abonados, indicando que tienen 30 días calendario para acercase a una oficina para regularizar el registro del número IMEI, y si no lo hace en ese plazo, se procederá al bloqueo del equipo. En caso el abonado se acerque para regularizar, la empresa debe realizar las mismas validaciones que se aplican en los cuestionamientos, y adicionalmente de ser el caso validar la adquisición del equipo terminal móvil en sus sistemas comerciales. Luego del bloqueo, el abonado todavía tiene el derecho de presentar el cuestionamiento, e incluso que este sea evaluado por el OSIPTEL cuando la respuesta de la empresa no resulte satisfactoria para él. En el siguiente gráfico se detalla el proceso en un diagrama procedimental.

[35] (i) verificar identidad del abonado del servicio móvil, (ii) verificar la coincidencia del IMEI físico y lógico, (iii) verificar que el SIM Card del servicio móvil de abonado corresponda a un servicio registrado bajo su titularidad y que este se encuentre vinculado al equipo terminal y (iv) verificar la coincidencia del TAC (marca y modelo) del equipo terminal móvil con sus respectivas características físicas.

FIGURA N° 8: ALTERNATIVA 2.2. BLOQUEO DE IMEI CLONADOS CON PROCEDIMIENTO DE IDENTIFICACIÓN PREVIA



Elaboración: OSIPTEL

c) Procedimiento de entrega de contraseña única:

- Entrega de la contraseña única al momento de la contratación u otro trámite, o a requerimiento expreso.
- En servicios móviles se valida mediante verificación biométrica y se puede aplicar el procedimiento de excepción de verificación biométrica. En servicios fijos se valida la identidad de la misma forma como se contrata: exhibición de documento legal de identidad. La operadora puede emplear otro mecanismo de validación de identidad previa aprobación del Osiptel (Vg. biométrica facial)
- Procedimiento de entrega de contraseña única: remisión de código provisional el cual debe modificarse en su primer uso, enlace personalizado que derive a un sitio para la generación de la contraseña y/o ingreso directo de una clave secreta por parte del abonado.
- Vigencia de código provisional de 7 días calendario.
- La contraseña única se puede cambiar las veces que desee el usuario.
- Representante legal o abonado designado debe proporcionar la contraseña única.
- Obligación de implementar formas de entrega de contraseña única para todos sus abonados incluyendo aquellos que no cuentan con acceso a Internet.
- Obligación de envío de mensaje de texto de alerta al momento de la generación de la contraseña única.

6.2. Análisis Beneficio-Costo

En esta sección se realiza la evaluación de las alternativas 2.1 y 2.2 mediante un análisis Costo-Beneficio, con el objetivo de cuantificar si estas propuestas generan una mejora en los niveles de bienestar y cuál de ellas es la más recomendable en comparación con la alternativa 1. Es de recalcar que el ámbito de aplicación de esta metodología es para la propuesta normativa relacionada a los IMEI clonados.

6.2.1. Estimación de los beneficios

Una de las principales razones por las que se busca bloquear los IMEI clonados intra-red es disuadir el robo de equipos terminales, y que estos ya no puedan ser comercializados en el mercado negro. Esto implica que la implementación de la alternativa 2.1 o la alternativa 2.2 debería tener un impacto en la cantidad anual de nuevos IMEI clonados intra-red. Es decir, si bien no se espera que el bloqueo IMEI disuada al 100% a los clonadores, sí debería evidenciarse una menor incidencia por efecto de la norma.

Al respecto, en el Anexo 1 se realizó la proyección de la cantidad acumulada de IMEI clonados al 2023 y los nuevos IMEI clonados que se detectarían entre el 2024 y el 2029. Cabe señalar que, respecto a las alternativas 2.1 y 2.2, se prevé una disminución progresiva a partir de la implementación de la política.

Por otra parte, se considera que dentro del total de los equipos con IMEI duplicado o clonados se encuentran 3 grupos de abonados: (i) los propietarios originales del IMEI, (ii) abonados estafados que adquirieron el equipo sin conocer que el IMEI es clonado o duplicado y (iii) los “abonados” que deliberadamente tienen un equipo con IMEI clonado o duplicado con el objetivo de cometer actos delictivos.

A partir de la información obtenida por la Dirección de Fiscalización (DFI), en aplicación de la metodología de detección de IMEI clonados intra-red, se identificó a noviembre del

2023 un total de 944 624 equipos con IMEI clonados o duplicados, de los cuales 370 027 corresponde a abonados originales.

Por otra parte, respecto a las alternativas 2.1 y 2.2, se estima la cantidad de IMEI clonados o duplicados a cierre del 2023 en 962 488. Asimismo, en el cuadro N° 2 se reportan la cantidad de IMEI originales afectados por la clonación, la tasa de originales, la estimación de abonados estafados con un IMEI clonado y el total de cuestionamientos. Cabe señalar que para el cálculo de los abonados estafados se está asumiendo una probabilidad de estafa de 50% que se aplica sobre los IMEI clonados no originales.

CUADRO N° 2: ESTIMACIÓN DE LA CANTIDAD INICIAL DE CUESTIONAMIENTOS PARA LAS DOS ALTERNATIVAS

Empresa	IMEI duplicados o clonados	IMEI originales (víctimas)	Tasa de originales	Abonados estafados (IMEI clonados -IMEI originales)*0.50	Total cuestionamientos o verificaciones (IMEI originales + abonados estafados)
Operador A	235 538	94 198	0.40	70 670	164 868
Operador B	131 403	48 134	0.37	41 634	89 769
Operador C	94 440	34 153	0.36	30 143	64 296
Operador D	501 108	209 709	0.33	145 699	355 408
Total	962 488	386 195		288 147	674 341

Nota: (a) Se asume que el 50% de los IMEI no originales lo tiene un abonado estafado. (c) La tasa de originales resulta de dividir la cantidad de IMEI genuinos originales entre el total de IMEI clonados, y (d) se considera a los abonados con IMEI genuino u original que presentarían el respectivo cuestionamiento ante la empresa operadora.
Fuente: RENTESEG
Elaboración: OSIPTEL

En relación con beneficios incrementales de las alternativas 2.1 y 2.2, se debe señalar que se espera una reducción de los robos de equipos por lo menos de gama media y gama baja[36], lo cual implica un menor gasto en reponer los equipos sustraídos, menor tiempo sin servicio debido a un robo y una reducción de los costos de denuncia. Adicionalmente, se debe señalar que el bloqueo de equipos con IMEI duplicados o clonados tiene un beneficio inmediato en la reducción de la criminalidad, dado que los equipos con IMEI clonados puede estar siendo usados para realizar delitos, tales como la extorsión o fraude. Al respecto, se debe considerar que, el escenario de la alternativa 2.1 incorpora el supuesto de un mes en relación al tiempo que un individuo utilizaría el equipo duplicado o clonado para fines delictivos, dado que se produciría el bloqueo inmediato a la identificación del IMEI clonado; mientras que, para la alternativa 2.2 el tiempo sería de 2 meses, tomando en cuenta que existe un periodo de identificación previa, por lo que se añadiría al menos un mes adicional al tiempo de uso del equipo terminal con IMEI clonado o duplicado para fines criminales.

En el cuadro siguiente se brinda detalles de los supuestos y parámetros utilizados para el cálculo de los beneficios incrementales, y los resultados obtenidos en este ejercicio[37].

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

[36] Se está asumiendo que los equipos de gama media se roban para obtener IMEI y clonarlos, mientras que los equipos de gama alta se roban para insertar un IMEI clonado y comercializarlo.
[37] Los beneficios estimados están a valor presente, calculados con una tasa, para un período de 5 años

CUADRO N° 3: BENEFICIOS ESTIMADOS A VALOR PRESENTE (En soles)

Fuentes de afectación	Supuestos	Escenario base	Alternativa 2.1		Alternativa 2.2	
			Afectación	Beneficio incremental	Afectación	Beneficio incremental
B1. Robo de equipo de gama media para obtener IMEI	- Aplica sobre total de IMEI originales - Costo del equipo nuevo: S/ 500[38] - Pérdida de valor del equipo por uso: 54%[39]	229 405 168	158 183 079	71 222 089	160 687 572	68 717 596
B2. Costo del abonado para reponer equipo de gama media	- Aplica sobre total de IMEI originales - Se asume que compra un nuevo equipo 44% más barato del original[40]	188 470 417	129 957 102	58 513 315	132 014 697	56 455 721
B3. Robo de equipo de gama alta para venta con IMEI clonado	- Aplica sobre total de abonados estafados - Costo del equipo nuevo: S/ 1660[41] - Pérdida de valor del equipo por uso: 54%	568 179 824	391 780 337	176 399 487	397 983 345	170 196 479
B4. Costo del abonado para reponer equipo de gama alta	- Aplica sobre total de abonados estafados - Se asume que compra un nuevo equipo 44% más barato del original	466 794 576	321 871 578	144 922 998	326 967 730	139 826 847
B5. Tiempo sin servicio por robo	- Aplica sobre total de IMEI originales y abonados estafados - Se asume en 5 días y se valora en función del ARPU	2 288 678	1 578 125	710 553	1 603 112	685 566
B6. Costo de denuncia	- Aplica sobre total de IMEI originales - Costo de denuncia policial: S/ 7,6 en el 2021[42].	6 481 336	4 469 113	2 012 223	4 539 872	1 941 464
37. Uso delictivo de líneas con MEI clonado	- Aplica sobre la cantidad residual de IMEI clonados luego de quitar a originales y estafados. - S/ 100 por extorsión, 6 meses (escenario base), 1 mes (alternativa 2), 2 meses (alternativa 3) y 2 víctimas	763 552 877	87 749 509	675 803 368	178 277 672	585 275 205
TOTAL DE BENEFICIOS ESTIMADOS			**1 129 584 032**		**1 023 098 878**	

Nota: Debido a que los precios unitarios son del 2022, se aplica una tasa de inflación de 5.69% para el 2023, 2.4% para el 2024 y 2.02% en adelante.
Elaboración: OSIPTEL.

[38] Disponible en: https://gestion.pe/economia/movil-celulares-equipos-entel-ahora-peruanos-apuntan-a-celulares-de-gama-media-cuyo-precio-promedio-oscila-en-s-500-noticia/
[39] Se consideró el valor correspondiente al equipo de marca Samsung Galaxy con sistema Android, el cual presenta la mayor devaluación de equipo con el 53,8%. Disponible en: https://rpp.pe/tecnologia/mas-tecnologia/celulares-android-gama-alta-pierde-50-de-valor-en-meses-noticia-1405538
[40] Se consideró el valor correspondiente al equipo de marca Samsung Galaxy con sistema Android, el cual presenta la mayor devaluación de precio de equipo con el 44,2%. Disponible en: https://rpp.pe/tecnologia/mas-tecnologia/celulares-android-gama-alta-pierde-50-de-valor-en-meses-noticia-1405538
[41] Se consideró el equipo móvil de gama alta con menor valor, dado que es el más accesible para los usuarios. En ese sentido, se tomó el precio del Apple IPhone SE (2022) que asciende US$429,99 y el tipo de cambio del 2021 (S/ 3,86) según lo proyectado en el Marco Macroeconómico Multianual 2022-2025. Precio del equipo móvil disponible en: https://elcomercio.pe/tecnologia/moviles/seis-celulares-que-reunen-la-potencia-de-la-gama-alta-por-menos-de-800-dolares-samsung-apple-iphone-google-xiaomi-oneplus-noticia/?ref=ecr
[42] Valor obtenido del TUPA de la Policía Nacional del Perú. Disponible en: https://www.bn.com.pe/tramites-entidades-publicas/tupa/policia-nacional.pdf

6.2.2. Estimación de los costos

Al respecto, se esperaría un comportamiento diferenciado por parte de los abonados frente a la alternativa 2.1 o la alternativa 2.2. En la alternativa 2.1, en la cual no hay período de verificación previa y se aplica un bloqueo inmediato a todos los equipos con IMEI clonados o duplicados, se debería esperar que todos los propietarios de los IMEI originales o genuinos y los abonados estafados que desconocen que su IMEI está duplicado o clonado presenten, de manera masiva, el cuestionamiento del bloqueo. En cambio, en la alternativa 2.2, dado que se realizará una comunicación previa a través de un SMS, se esperaría que soliciten la verificación previa los abonados que tienen la capacidad de sustentar que ese IMEI les pertenece, así como los abonados estafados que desconocen que su IMEI fue clonado o duplicado. Cabe señalar además que en la alternativa 2.2, se asume, por simplicidad, que no se realizarán cuestionamientos, debido a que los que podían demostrar ser propietarios del IMEI ya hicieron la verificación previa, mientras que los abonados estafados son conscientes que probablemente el cuestionamiento no tendrá una respuesta favorable. Adicionalmente, la alternativa 2.1 presenta un mayor periodo sin contar con el servicio móvil que la alternativa 2.2, debido a que, en la primera se ejecuta un bloqueo inmediato mientras que la segunda, otorga un periodo adicional para la verificación antes de ejecutar el bloqueo del equipo.

Por otra parte, para estimar los costos de las alternativas 2.1 y 2.2 se han identificado 7 fuentes de costos:

- C1 Costo de la atención presencial por cuestionamientos
- C2 Costo de atender cuestionamientos
- C3 Costo de no contar con el servicio debido al bloqueo por IMEI clonado (*)
- C4 Costo de baja de servicio para las empresas operadoras (*)
- C5 Costo de envío de SMS
- C6 Costo de la atención presencial por verificación previa
- C7 Costo de atender la verificación previa

Nota: (*) Peor escenario en el cual el abonado no reemplaza o adquiere otro equipo.

Al respecto, el cálculo de estos costos se realizó en función de las siguientes pautas:

- C1 y C2 se calculan respecto a la cantidad estimada de cuestionamientos, la cual a su vez se calcula en función de la cantidad de IMEI originales y la cantidad estimada de abonados estafados con un IMEI duplicado o clonado.
- C3 se estima respecto al total de IMEI originales y los abonados estafados, los cuales representan el total de abonados afectados con el bloqueo.
- C4 se calcula respecto a los abonados estafados, dado que se asume que las empresas operadoras solo perderían a este tipo de abonados.
- C5 aplica solo en la alternativa 2.2 y se calcula respecto a la totalidad de IMEI clonados o duplicados.
- C6 y C7 aplica solo en la alternativa 2.2 y se calcula respecto a la totalidad de IMEI originales y los abonados estafados, debido que asistirían presencialmente a la empresa operadora a fin de sustentar la propiedad de su equipo terminal móvil.
- Los parámetros y valores unitarios que se emplearon para calcular todos estos costos se reportan en el Anexo 2.

De esta manera, proyectando para un periodo de 6 años (2023 – 2029), con una tasa de descuento social de 8.5%[43] se estima que la alternativa 2.1 y 2.2 tienen un costo a valor presente de S/ 200.4 millones y S/ 200.8 millones. En el siguiente cuadro se reportan estos cálculos por tipo de costo.

CUADRO N° 4: COSTOS ESTIMADOS A VALOR PRESENTE DE LAS ALTERNATIVAS 2.1 Y 2.2 (Soles)

	Alternativa 2.1	Alternativa 2.2
C1. Costo de la atención presencial por cuestionamiento	624 322	0
C2. Costo de atender cuestionamientos	41 814 535	0
C3. Costo de no contar con el servicio debido al bloqueo por IMEI duplicado o clonado	66 116 363	51 957 023
C4. Costo de baja de servicio para las empresas operadoras	91 873 736	93 328 361
C5. Costo de envío de SMS	0	8 792
C6. Costo de la atención presencial por verificación previa	0	2 652 839
C7. Costo de atender la verificación previa	0	52 879 657
COSTO TOTAL	**200 428 956**	**200 826 672**

Nota: Se aplica la tasa de descuento del MEF de 8,5%.
Elaboración: OSIPTEL.
Fuente: OSIPTEL

6.2.3. Ratio Beneficio-Costo

Los beneficios y costos que finalmente fueron estimados no son todos los que un paquete de medidas puede generar, pero constituyen una aproximación razonable a ellos, en la medida que no solamente existen costos sin estimar, sino que también una serie de beneficios vinculados a las medidas propuestas.

CUADRO N° 5 RESULTADOS DEL ANÁLISIS BENEFICIO – COSTO (soles)

Valores	Alternativa 2.1	Alternativa 2.2
Beneficios	1 129 584 032	1 023 098 878
Costos	200 428 956	200 826 672
Beneficio Neto	929 155 075	822 272 205
Ratio Costo - Beneficio	**5.64**	**5.09**

Elaboración: OSIPTEL.
Fuente: OSIPTEL

En virtud a ello, se ha planteado el análisis beneficio-costo con la información disponible, donde se debe considerar que un ratio mayor a 1 indicaría que las medidas son costo-efectivas (beneficios mayores a los costos) y brindan un aporte favorable al bienestar social, mientras que un valor menor a 1 denota que los costos son mayores que los beneficios.

Para ello, se calculó el valor presente de los costos y beneficios[44] para ambas alternativas. En el caso de la alternativa 2.1, los costos ascenderían a S/ 200.4 millones y los beneficios a S/ 1129.6 millones, así, los beneficios netos de ejecutar la propuesta normativa ascenderían a S/ 929 millones, resultando un ratio beneficio-costo de 5.64. En cambio, para la alternativa 2.2, los costos ascenderían a S/ 200.8 millones y los beneficios a S/ 1023 millones; obteniendo un ratio beneficio-costo de 5.09.

[43] Tasa social de descuento anual (MEF). Disponible en: https://www.mef.gob.pe/contenidos/inv_publica/docs/parametros_evaluacion_social/Tasa_Social_Descuento.pdf

[44] Se consideró una tasa social de descuento de 8,5%.

6.3. Análisis Multicriterio (AMC) de otras normas de protección del consumidor

En el caso de las propuestas asociadas a los objetivos 2, 3 y 4, referidas a la propuesta relacionada con la problemática asociada con la información reportada en el Registro de Abonados, la contraseña única y el cuestionamiento de titularidad prepago, se ha realizado un análisis multicriterio, dado que se trata de propuestas normativas complementarias o que no implican costos significativos de implementación. A continuación, se presentan las propuestas normativas que serán evaluadas a través del análisis multicriterio:

CUADRO N° 6 ANÁLISIS DEL NIVEL DE IMPACTO DE LAS ALTERNATIVAS

Objetivo	Alternativa 2	Análisis
Objetivo 2: Mejorar los niveles de idoneidad y autenticidad de la información reportada por las empresas operadoras en el registro de abonados.	Para los tres supuestos en los que aplican las reglas de excepción de la verificación biométrica, se propone añadir la obligación de conservar una copia del documento legal del solicitante.	Esta obligación solo afecta a los usuarios de origen extranjero que se encuentran indocumentados. No obstante, su aplicación no genera que no puedan acceder al servicio, sino que solo busca dejar una trazabilidad al proceso de contratación.
Objetivo 3: Facilitar la entrega de la contraseña única a través de un proceso seguro y confiable.	Se establece un procedimiento de entrega de contraseña única.	Si bien esta propuesta afecta potencialmente a todos los usuarios del servicio público móvil; no obstante, en la actualidad ya existen este tipo de procedimientos, por lo que la norma, en su mayoría, está recogiendo la práctica, a fin de garantizar que la entrega de la contraseña única se realice de forma segura y a todos los usuarios, digitalizados o no.
Objetivo 4: Reducir los escenarios en los que la delincuencia puede utilizar una línea prepago contratada a nombre de otra persona	Eliminación de procedimiento de cuestionamiento prepago	Con la eliminación del procedimiento de cuestionamiento prepago los usuarios no pierden el derecho a rechazar una contratación no realizada, dado que ello mismo lo pueden seguir haciendo a través de un reclamo por contratación no solicitada.

En atención a estos argumentos se ha valorado que estas 3 medidas regulatorias no requieren de un análisis Costo-Beneficio y, que pueden ser evaluada de manera más flexible con un análisis multicriterio.

6.3.1. Atributos o criterios de evaluación

Para esta propuesta normativa, se propone la evaluación de los siguientes criterios o atributos asociados a impactos positivos:

CUADRO N° 7*:* PONDERACIÓN DE LOS CRITERIOS

Atributos	Criterio
	• Mejora la capacidad de presentar reclamos

1. Mejora de la atención de reclamos (15%)	• Reduce la probabilidad de ocurrencia de problemas
	• Mejora la capacidad de verificar incumplimientos
2. Mejora de decisiones de consumo (15%)	• Mejora el conocimiento de la información tarifaria y de cobertura
	• Facilita el cambio de operador
	• Limita la contratación de servicios
3. Reducción de riesgos (15%)	• Incidencia de delitos y riesgos
	• Contrataciones seguras
4. Trazabilidad de la información (10%)	• Identificación del solicitante
	• Trazabilidad del proceso
	• Oportunidad de la información
5. Dificultad para la implementación (25%)	• Niveles de inversión
	• Incidencia de escenario de difícil implementación
6. Efecto en la competencia (20%)	• Retención de clientes
	• Limitaciones para captar clientes
	• Diferenciación entre empresas operadoras

Elaboración: OSIPTEL.

La evaluación de los atributos y los criterios se realiza en una escala del -1 al 1, donde -1 es el escenario más desventajoso, 1 más ventajoso para los agentes de mercado y 0 un escenario en el cual la propuesta no genera cambios ni positivos ni negativos.

6.3.2. Resultados del AMC

En el AMC que se ha implementado para evaluar a las alternativas relacionadas con los objetivos 2, 3 y 4, se ha demostrado que cada componente de la propuesta normativa tiene un impacto positivo en el mercado comparado con la alternativa de mantener el marco normativo vigente.

Los atributos elegidos y los pesos otorgados garantizan que esta AMC evalúe de manera equilibrada los diversos aspectos que el mercado y los usuarios valoran. En tal sentido, los resultados obtenidos permiten identificar la alternativa más recomendable o la que va a generar un mayor impacto en el bienestar social. Como se puede apreciar en el siguiente cuadro, en promedio el escenario base tiene una calificación de -0.10 y la alternativa 2, una calificación de 0.13.

Por lo tanto, en atención a los resultados obtenidos en este AMC, se recomienda la implementación de la alternativa 2. Cabe señalar que, en el anexo 6 se encuentra el análisis de robustez de los resultados realizado mediante una simulación Monte Carlo, de manera que se cumple con lo establecido en los Lineamientos de Calidad Regulatoria del Osiptel.

CUADRO N° 8: RESULTADO DEL ANÁLISIS MULTICRITERIO (AMC)

Objetivo	Escenario base	Alternativa 2
CALIFICACIÓN PROMEDIO	**-0.10**	**0.13**
Objetivo 2: Mejorar los niveles de idoneidad y autenticidad de la información reportada por las empresas operadoras en el registro de abonados.	0.02	0.08
Objetivo 3: Facilitar la entrega de la contraseña única a través de un proceso seguro y confiable.	-0.09	0.14
Objetivo 4: Reducir los escenarios en los que se puede utilizar una línea prepago para cometer delitos	-0.23	0.17

7. APLICACIÓN DE LA SOLUCIÓN SELECCIONADA

7.1. Análisis de legalidad

Para el referido análisis, es pertinente considerar el marco normativo que contempla las facultades y atribuciones conferidas por ley al OSIPTEL, tanto para emitir normas de carácter general, como la facultad para imponer sanciones y medidas cautelares; así como aquellas disposiciones que regulan la contratación de servicios públicos móviles.

En ese sentido, se tiene que mediante el Decreto Legislativo N° 702[45], cuyo texto y modificatorias fueron recopilados en el Texto Único Ordenado de la Ley de Telecomunicaciones, aprobado mediante el Decreto Supremo N° 013-93-TCC (en adelante, Ley de Telecomunicaciones), se creó al OSIPTEL, atribuyéndole el rol de regular el comportamiento de las empresas operadoras de servicios públicos de telecomunicaciones, a través de resoluciones expedidas por su Consejo Directivo, conforme a lo siguiente:

> ***"Artículo 76.-*** *La Comisión Reguladora de Tarifas de Comunicaciones será sustituida por el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL), que se encargará de regular el comportamiento de las empresas operadoras, así como las relaciones de dichas empresas entre sí, de garantizar la calidad y eficiencias del servicio brindado al usuario y de regular el equilibrio de las tarifas."*
>
> ***"Artículo 77.-*** *El poder regulatorio que esta Ley concede a OSIPTEL en relación a materias de su competencia será ejercido a través de resoluciones expedidas por su Consejo Directivo. (Subrayado agregado)"*

Posteriormente, la Ley N° 27332, Ley Marco de Organismos Reguladores de Servicios Públicos, así como su modificatoria, sistematizó las diversas funciones de los organismos reguladores; estableciendo respecto de las funciones normativa, supervisora y fiscalizadora, lo siguiente:

> ***"Artículo 3.- Funciones***
> *3.1 Dentro de sus respectivos ámbitos de competencia, los Organismos Reguladores ejercen las siguientes funciones:*
> *(…)*
> ***a) Función supervisora****: comprende la facultad de verificar el cumplimiento de las*
> *obligaciones legales, contractuales o técnicas por parte de las entidades o actividades supervisadas, así como la facultad de verificar el cumplimiento de cualquier mandato o resolución emitida por el Organismo Regulador o de cualquier otra obligación que se encuentre a cargo de la entidad o actividad supervisada; (…)*
> ***c) Función Normativa****: comprende la facultad de dictar en el ámbito y en materia de sus respectivas competencias, los reglamentos, normas que regulen los procedimientos a su cargo, otras de carácter general y mandatos u otras normas de carácter particular referidas a intereses,*

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

[45] Que aprobó las Normas que regulan la Promoción de Inversión Privada en Telecomunicaciones.

obligaciones o derechos de las entidades o actividades supervisadas o de sus usuarios;

***d) Función fiscalizadora y sancionadora**: comprende la facultad de imponer sanciones dentro de su ámbito de competencia por el incumplimiento de obligaciones derivadas de normas legales o técnicas, así como las obligaciones contraídas por los concesionarios en los respectivos contratos de concesión; (…)".*

Más recientemente, la Ley N° 29158, Ley Orgánica del Poder Ejecutivo estableció las siguientes reglas, respecto de los organismos reguladores:

*"**Artículo 32.- Organismos Reguladores***

Los Organismos Reguladores:

1. *Se crean para actuar en ámbitos especializados de regulación de mercados o para garantizar el adecuado funcionamiento de mercados no regulados, asegurando cobertura de atención en todo el territorio nacional. (…)*
3. *Dentro de sus respectivos ámbitos de competencia, tienen funciones supervisoras, reguladoras, normativas, fiscalizadoras y sancionadoras; y de solución de controversias y reclamos, en los términos previstos por la Ley de la materia.*

   (…)

7. *Defienden el interés de los usuarios con arreglo a la Constitución Política del Perú y la ley.*

(…)".

De lo anterior, se desprende que este Organismo Regulador se encuentra facultado para dictar de manera exclusiva y dentro del ámbito de su competencia, reglamentos y normas de carácter general, aplicables a todos los administrados que se encuentren en las mismas condiciones. Asimismo, se indica que tales reglamentos pueden definir los derechos y obligaciones entre las empresas operadoras y de estas con los usuarios.

De la misma manera, se faculta al OSIPTEL a supervisar y fiscalizar el cumplimiento de las disposiciones normativas en el marco de su competencia; así como a sancionar el incumplimiento de estas por parte de los agentes del mercado, de ser el caso.

Por otro lado, el 6 de enero de 2017, en el diario oficial El Peruano, se publicó el Decreto Legislativo N° 1338, Decreto Legislativo 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.

Conforme se establece en su artículo 1, la finalidad del referido Decreto Legislativo es el fortalecimiento de la seguridad ciudadana garantizando la contratación de los servicios públicos móviles de telecomunicaciones[46].

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

[46] *"**Artículo 1. Objeto y finalidad***
1.1 El presente decreto legislativo tiene por objeto la creación del Registro Nacional de Equipos Terminales Móviles para la Seguridad – RENTESEG, con la finalidad de prevenir y combatir el hurto, robo y comercio ilegal de equipos

El Decreto Legislativo N° 1338 y su Reglamento establecen que el OSIPTEL puede establecer las normas complementarias que resulten necesarias para la implementación de las disposiciones, tal como se indica a continuación:

Decreto Legislativo N° 1338	**QUINTA. Normativa complementaria** El OSIPTEL, el Ministerio del Interior y la Policía Nacional del Perú, en el marco de sus competencias, dictan las normas complementarias que resulten necesarias para la implementación de las disposiciones establecidas en el presente decreto legislativo y su reglamento.
Decreto Supremo N° 009-2017-IN (derogado)	**Artículo 30.- Obligaciones de las empresas operadoras** Son obligaciones de las empresas operadoras: (…) o) Otras obligaciones que establezca el presente Reglamento y la normativa complementaria aprobada por el OSIPTEL.
Decreto Supremo N° 007-2019-IN (vigente)	**Artículo 32.- Obligaciones de las empresas operadoras** Son obligaciones de las empresas operadoras: (…) o) Otras obligaciones que establezca el presente Reglamento y la normativa complementaria aprobada por el OSIPTEL.

Precisamente, a través del Decreto Legislativo N° 1338 se faculta al OSIPTEL a establecer la normativa necesaria que coadyuve al cumplimiento de la finalidad de la seguridad ciudadana relacionada a la contratación del servicio público móvil y la operatividad del RENTESEG.

7.2. Razonabilidad y proporcionalidad

A manera de síntesis, en esta sección se retoman los argumentos y evidencias presentados a lo largo de todo el informe, a fin de demostrar que las medidas propuestas por el OSIPTEL cumplen con los criterios de razonabilidad y proporcionalidad.

7.2.1. Justificación de la intervención

Sobre la justificación de la intervención, la regulación es razonable en la medida que existen fallas de mercado tales como asimetrías de información que estarían generando una afectación al interés público: mercado negro de equipos terminales móviles sustraídos que son, posteriormente, manipulados mediante técnicas de duplicación o clonación de IMEI; lo que generaría una alta afectación a los abonados que hayan adquirido estos dispositivos. Además, se debe remarcar el alto nivel de informalidad en el país lo cual acrecienta los riesgos de seguridad para los abonados, puesto que permite la continuidad de la comercialización de equipos móviles de dudosa procedencia.

Además, el Estado debe velar y contribuir a proteger a los abonados que están expuestos o son víctimas de clonación del equipo terminal móvil. En atención a ello, dado que el regulador no puede asegurar la procedencia de los equipos terminales móviles ofrecidos en el mercado por las características descritas anteriormente, se considera necesario establecer un procedimiento que permita identificar el IMEI original en los cuestionamientos de bloqueo de equipo terminal por IMEI clonado o duplicado.

En ese sentido, es de mencionar que la protección de los referidos intereses públicos, impactan en otros bienes jurídicos tutelados como el de seguridad ciudadana. Sobre el particular, es de considerar que la seguridad ciudadana es un bien jurídico que el Estado busca cautelar desde diferentes ámbitos. Por tal motivo, a través del Decreto Legislativo N° 1338 se creó el RENTESEG, con la finalidad de prevenir y combatir el hurto, robo y

terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; garantizando la contratación de los servicios públicos móviles de telecomunicaciones. (…)

comercio ilegal de equipos terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; así como a fin de garantizar la contratación de los servicios públicos de telecomunicaciones.

En este contexto normativo, se desprende que el OSIPTEL tiene una función normativa con relación a los derechos de los usuarios y abonados del servicio público de telecomunicaciones, a efectos de resguardar a los abonados se enmarquen en un ámbito de seguridad. Asimismo, dicha función normativa se extiende para aquellas transacciones y/o solicitudes que involucren la comercialización de equipos terminales móviles.

7.2.2. Proporcionalidad de la medida

La proporcionalidad de las medidas propuestas ha sido evaluada a partir del análisis costo beneficio. Se debe destacar que en el referido análisis costo-beneficio se cuantificaron los siguientes beneficios: (i) afectación por robo de equipo de gama media para obtener IMEI, (ii) afectación por reposición de equipo robado gama media, (iii) afectación por venta de equipos con IMEI clonado, (iv) afectación por reposición de equipo robado gama alta, (v) afectación por el tiempo sin servicio, (vi) afectación por trámite de denuncia y (vii) afectación por extorsión y/o fraude. Asimismo, los costos que se cuantificaron estuvieron relacionados con (i) costo de atención presencial por cuestionamiento, (ii) costo de atender cuestionamientos para la empresa operadora, (iii) costo de no contar con el servicio debido al bloqueo por IMEI duplicado o clonado, (iv) costo de baja de servicio para las empresas operadoras, (v) costo de envío de SMS, (vi) costo de la atención presencial por verificación previa y (vii) costo de atender la verificación previa.

Como resultado de este análisis, se ha obtenido que esta propuesta regulatoria tiene, a valor presente, un costo de S/ 200.4 millones y un beneficio de S/ 1129.6 millones, resultando un ratio beneficio-costo de 5.64.

7.2.3. Existencia de otras medidas menos gravosas

Respecto a la existencia de medidas menos gravosas para la mejorar los niveles de seguridad para los abonados en la adquisición y uso de equipos terminales móviles frente a las técnicas de clonación de IMEI, se debe considerar las medidas para abordar el problema de asimetría de información (por ejemplo, campañas de sensibilización de los abonados). En ese sentido, es necesario la participación de las concesionarias móviles, así como también de las entidades públicas como el Ministerio del Interior y la Policía Nacional a fin de impulsar una campaña pública de información sobre las medidas adoptadas, los beneficios y las acciones que los abonados deben realizar si pierden sus teléfonos o se los sustraen, o si adquieren dispositivos cuyos IMEI hayan sido objeto de clonación.

Asimismo, se han encontrado experiencias internacionales y recomendaciones de organismos como la Unión Internacional de Telecomunicaciones (UIT) que van en línea con las medidas propuestas por OSIPTEL, como la solución del bloqueo de las redes móviles que impidan la utilización de dispositivos con IMEI clonados y que sean capaces de distinguir los dispositivos auténticos de los clonados.

7.3. Propuesta normativa

Mediante Decreto Supremo N° 007-2019-IN se modificó el Reglamento del Decreto Legislativo N° 1338, por lo que corresponde que la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones y las Normas Complementarias para la Implementación del RENTESEG adecúen sus disposiciones al citado reglamento.

Del mismo modo, recientemente, mediante Decreto Legislativo N° 1596 se modificó el Decreto Legislativo N° 1338, el cual –entre otros- elimina la figura del intercambio seguro.

Asimismo, considerando los próximos bloqueos de equipos terminales con IMEI duplicado o clonado se requiere establecer las disposiciones para la realización de tales bloqueos y la atención de los cuestionamientos que puedan presentar los abonados.

En ese sentido, luego de la revisión realizada se ha considerado necesario establecer algunas precisiones y modificaciones a la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones y a las Normas Complementarias para la Implementación del RENTESEG.

Se propone modificar el artículo 65 de la Norma de las Condiciones de Uso, así como de los artículos 25 y 27-H de las Normas Complementarias para la Implementación del RENTESEG, relacionados al procedimiento de cuestionamiento de bloqueo de equipos terminales con IMEI clonado o duplicado.

Del mismo modo, se propone eliminar el numeral 4. del Anexo 4, a fin de que el cuestionamiento de titularidad del servicio público móvil prepago sea abordado mediante un procedimiento de reclamo. Con la finalidad de establecer un procedimiento detallado sobre la contraseña única se propone modificar el numerales 3.3 del Anexo 5 de la Norma de las Condiciones de Uso. Se propone incluir los artículos 61-A y 65-A referidos al desbloqueo por regularización de equipo terminal en el Renteseg, así como el boqueo del equipo terminal móvil en los casos de contratación o portabilidad no solicitada. Con relación al régimen sancionador se propone incluirlo como parte de los artículos de la norma (art. 77) y derogar su inclusión en el Anexo 9.

De otro lado, conforme a lo establecido en el Decreto Supremo N° 007-2019-IN que aprueba el Reglamento del Decreto Legislativo N° 1338, se propone la actualización de los artículos 60, 61, Anexo 1 y numeral 3.4. del Anexo 5 de la Norma de las Condiciones de Uso.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

7.3.1. Sobre el procedimiento de cuestionamiento de bloqueo de equipo terminal móvil cuyo IMEI original ha sido clonado o duplicado

Se propone modificar el artículo 65 de Normas de las Condiciones de Uso, así como los artículos 25 y 27-H de Normas Complementarias para la Implementación del RENTESEG, relacionados al procedimiento de cuestionamiento de bloqueo de equipos terminales con IMEI clonado o duplicado, conforme al siguiente detalle:

Normas de las Condiciones de Uso	
Artículo que se propone modificar	**Fundamento**
"Artículo 65.- Cuestionamiento al bloqueo del equipo terminal y suspensión del servicio *En caso de existir cuestionamiento respecto al bloqueo del equipo terminal y/o suspensión del servicio por alguna de las causales previstas en el presente Título, esta situación debe ser comunicada personalmente por el abonado, en cualquiera de las oficinas o centros de atención de la empresa operadora* ***que le presta el servicio****. Para tal efecto, el abonado debe acercarse conjuntamente con el equipo terminal bloqueado y el SIM Card o Chip correspondiente****, así como, de ser posible, con el documento físico o virtual que acredite la propiedad del equipo****.* *Al respecto, rigen las disposiciones establecidas en las Normas Complementarias del RENTESEG."*	Considerándose que para atender los cuestionamientos al bloqueo de los equipos terminales móviles de los abonados, en ocasiones el OSIPTEL debe validar la adquisición del equipo terminal móvil ante las empresas operadoras, resulta necesario abordar esta situación con la finalidad de simplificar y brindar celeridad al procedimiento de atención, así como de brindar mayor seguridad del pronunciamiento respecto de la procedencia o no del desbloqueo de dichos equipos, sobre todo teniendo en cuenta que actualmente se viene incrementando la cantidad de los equipos terminales móviles con IMEI original que han sido clonados o duplicados.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Normas Complementarias para la Implementación del RENTESEG	
Propuesta	**Fundamento**
"Artículo 25.- Información de la Lista de Excepción *El concesionario móvil* ***reporta al*** *RENTESEG la información del IMEI del equipo terminal móvil que cumple las validaciones indicadas en el artículo 27-H, así como el IMSI o Número de Servicio Telefónico Móvil vinculado con dicho IMEI, para evitar el bloqueo del equipo terminal móvil en su red por haber sido detectado con un IMEI duplicado o clonado, en la periodicidad, horario y demás indicaciones establecidas en el Instructivo Técnico.* ***En caso el Osiptel determine la pareja IMEI-IMSI que será ingresada a la Lista de Excepción, el concesionario móvil recoge del RENTESEG dicha información."***	Siendo que la empresa operadora es quien recibe los cuestionamientos de los abonados y realiza las validaciones del equipo terminal móvil y del servicio vinculado, es la idónea para determinar el desbloqueo de los equipos terminales móviles conforme a las validaciones establecidas y, en consecuencia, puede reportar al RENTESEG la pareja IMEI-IMSI habilitada a funcionar en su red móvil; sin perjuicio de aquellos cuestionamientos de abonados que requieran ser evaluados por parte del OSIPTEL.
"Artículo 27-H.- Procedimiento a seguir por el concesionario móvil ante elcuestionamiento al bloqueo del equipo terminal y suspensión del servicio ***Ante el cuestionamiento de bloqueo de equipo terminal y/o suspensión del servicio, el concesionario móvil debe informar al abonado sobre la causal de este reporte y debe:*** *(i) Validar la identidad del abonado* ***mediante verificación biométrica o el procedimiento establecido en el punto 3.4 del Anexo 5 de las Condiciones de Uso, o mediante la contraseña única a la que hace referencia el punto 3.3 del Anexo 5.*** *(ii) Verificar la coincidencia del IMEI impreso en el equipo terminal*	Se retira el supuesto de falta de ejecución del reporte de recuperación como motivo de presentación del cuestionamiento, siendo que no está relacionado al desconocimiento del bloqueo del equipo terminal móvil, sino a la falta de atención del desbloqueo. En atención a la cantidad de casos presentados, estos se continuarán gestionando a través del OSIPTEL. A fin de brindar mayor transparencia al procedimiento, se precisa que la empresa operadora debe informar al abonado sobre la causal del reporte de bloqueo del equipo terminal y/o suspensión del servicio. Cabe indicar que, actualmente, las empresas operadoras ya realizan dicha práctica.

*con el número del IMEI virtual que se muestra al digitar *#06# en el equipo terminal.* *(iii) Verificar que el SIM Card del abonado corresponda a un servicio registrado bajo su titularidad y que éste se encuentre vinculado al equipo terminal.* *(iv)* ***Validar que el TAC del IMEI corresponda a la marca y modelo del equipo terminal móvil cuestionado.*** ***(v) Verificar en su sistema comercial que el equipo terminal móvil fue adquirido por el abonado.*** ***El concesionario móvil luego de verificar que se cumple lo señalado en los numerales del (i) al (iv)*** *debe proceder, de forma inmediata,* ***a registrar en línea en el RENTESEG la información necesaria para obtener la autorización del*** *levantamiento del bloqueo del equipo y/o a la reactivación del servicio;* ***y*** *debe* ***informar al Osiptel sobre la acción ejecutada, así como*** *remitir la documentación que sustente las validaciones correspondientes a los numerales del (i) al (****v****),* ***según corresponda****, en un plazo no mayor de dos (2) días hábiles de presentado el cuestionamiento por el abonado.* *Lo dispuesto en el párrafo anterior no resulta aplicable cuando el bloqueo del equipo se realice por:* ***(i)*** *no encontrarse registrado en la Lista Blanca,* ***(ii) encontrarse en la Lista Negra como consecuencia del reporte de fraude realizado por el concesionario móvil, o (iii) incumplir las disposiciones referidas a la vinculación del equipo terminal móvil adquirido en el extranjero****.*	Las empresas operadoras para realizar la validación de la identidad de los abonados que presentan un cuestionamiento, actualmente utilizan, en su mayoría la verificación biométrica de huella dactilar, la cual brinda mayor certeza de la identidad de los abonados que se acercan a los centros de atención y cuestionan el bloqueo de sus equipos terminales móviles. Por tal motivo, se considera esta acción en el presente texto, salvo en los supuestos de excepción de verificación biométrica previstos en las Condiciones de Uso, o en caso se haga uso de la contraseña única. De otro lado, en atención a la problemática presentada para la atención de cuestionamientos relacionados a equipos terminales móviles originales cuyo IMEI ha sido duplicado o clonado, resulta necesario cotejar la coincidencia del TAC (marca y modelo) del equipo terminal móvil con sus respectivas características físicas, brindando está acción mayor seguridad en las validaciones que se realizan para el desbloqueo de equipos terminales móviles. Cabe precisar que, actualmente, la validación del TAC ya se viene utilizando en el procedimiento de suspensión y baja del servicio público móvil cuando el abonado utiliza el servicio vinculado a uno o más equipos terminales móviles con IMEI inválido por más de una vez, establecido en la Séptima Disposición Complementaria Final de las Normas Complementarias del RENTESEG. En caso de que se cumplan las validaciones necesarias para desbloquear un equipo terminal móvil con IMEI duplicado o clonado, corresponde que el concesionario móvil reporte la pareja

En caso el bloqueo del equipo terminal y/o suspensión del servicio se haya realizado por contar con un IMEI duplicado o clonado, el concesionario móvil debe habilitar inmediatamente el equipo terminal validado según los numerales del (i) al (iv) para que funcione en su red móvil, únicamente, con el servicio que el abonado tiene vinculado a esa fecha. El concesionario móvil reporta la pareja IMEI - IMSI en la Lista de Excepción del RENTESEG, según el Instructivo Técnico respectivo. ***El concesionario móvil que verifique que no se cumple alguna de las validaciones indicadas en los numerales del (i) al (iv) y/o que el RENTESEG no autoriza el levantamiento del bloqueo, debe informar al abonado que su solicitud no procede y no ejecuta el desbloqueo.*** ***En todos los casos, el concesionario móvil debe entregar al abonado una constancia de la presentación del cuestionamiento, en la cual se detalle la procedencia o no de su solicitud, precisando el motivo de su decisión, de acuerdo al formato comunicado por el Osiptel.*** ***En los casos que el abonado no se encuentre de acuerdo con el pronunciamiento del concesionario móvil, puede solicitar se eleve su cuestionamiento de bloqueo de equipo terminal móvil y/o suspensión del servicio al Osiptel. El concesionario móvil debe informar sobre este procedimiento y brindar al abonado la constancia de la referida solicitud conforme al formato comunicado por el Osiptel.*** ***En el plazo máximo de tres (3) días hábiles desde presentado***	IMEI-IMSI que será utilizada a la lista de excepción del RENTESEG y la habilite en su red. Se propone que la empresa operadora proporcione una constancia de la presentación del cuestionamiento, en la cual se detalle la procedencia o no del mismo, así como la constancia de la solicitud del abonado para elevar su cuestionamiento al OSIPTEL, debido a que diversos abonados al contactarse con el OSIPTEL para hacer seguimiento de sus cuestionamientos, informan que al momento de haberlos presentado el concesionario móvil no le proporcionó constancia alguna de su solicitud. Asimismo, sucede que en ocasiones los abonados refieren haber solicitado que su cuestionamiento sea elevado al OSIPTEL, pero no cuentan con la constancia de dicha solicitud. Se reduce a tres (3) días hábiles el plazo de elevación de los cuestionamientos a ser evaluados por el OSIPTEL, considerando que el concesionario móvil no realizará mayor análisis del cuestionamiento y a fin de agilizar el procedimiento. Del mismo modo, se reduce a diez (10) días hábiles el plazo para el pronunciamiento por parte del Osiptel. Asimismo, con la finalidad de contar con mayores elementos de juicio para la decisión del OSIPTEL respecto del cuestionamiento sobre equipos terminales móviles, se requiere que la empresa operadora verifique si el equipo fue adquirido por el abonado en alguno de sus puntos de venta, y remita dicha información al OSIPTEL, o en todo caso, remita el comprobante de pago y/o constancia de adquisición que haya sido proporcionado por el

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

el cuestionamiento, el concesionario móvil debe remitir al OSIPTEL dicha solicitud y la documentación que acredite las validaciones indicadas en los numerales del (i) al (v), adjuntando el comprobante de pago o constancia de adquisición que haya sido proporcionado por el abonado, en el que figure el IMEI, y/o marca y modelo del equipo, en remplazo del numeral (v) de ser el caso. Para tal efecto, el concesionario móvil solicita al abonado que presente dicha documentación, previo a la elevación del cuestionamiento al Osiptel. *El Osiptel se pronuncia sobre el cuestionamiento del abonado al bloqueo del equipo terminal y/o la suspensión del servicio por las causales antes señaladas, en un plazo no mayor de **diez (10)** días hábiles de recibida la información **del concesionario móvil**. El Osiptel puede habilitar un correo electrónico u otro medio informático para la remisión de la información a la que hace referencia el presente artículo."*	abonado, en el que figure el IMEI, y/o marca y modelo del equipo, de ser el caso. Cabe indicar que, el hecho que el equipo no se haya adquirido en un punto de venta de la empresa operadora, o que el abonado no haya presentado algún documento que acredite su propiedad, no impide la elevación del cuestionamiento del bloqueo al OSIPTEL.

7.3.2. Sobre la adecuación de las Normas Complementarias del RENTESEG a fin de incluir los supuestos de importadores y comercializadores y otros

Se propone modificar el artículo 9 de las Normas Complementarias para la Implementación del RENTESEG, relacionados al procedimiento de bloqueo y desbloqueo de equipos terminales reportados por los importadores, ensambladores, fabricantes en el país, casas comercializadoras de equipos y/o aparatos de telecomunicaciones, distribuidores, personas naturales o los concesionarios móviles, conforme al siguiente detalle:

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Normas de las Condiciones de Uso	
Artículo que se propone modificar	**Fundamento**
"Artículo 9.- Procedimiento de bloqueo y desbloqueo de equipos terminales móviles sustraídos, perdidos y recuperados de Perú reportados por los importadores, ensambladores, fabricantes en el país, casas comercializadoras de equipos y/o aparatos de telecomunicaciones, distribuidores, personas naturales o los concesionarios móviles ***Los importadores, los distribuidores, los fabricantes o ensambladores, las casas comercializadoras, personas naturales, o la propia empresa operadora, deben reportar ante cualquier empresa operadora el bloqueo de los equipos terminales móviles sustraídos y perdidos que no han sido vinculados lícitamente a un servicio público móvil y cuya propiedad sea acreditada por la persona que realiza el reporte, para lo cual proporcionan la información del código IMEI.*** ***El reporte de recuperación de equipo terminal se presenta únicamente en las oficinas o centros de atención a usuarios, utilizando el sistema de verificación biométrica de huella dactilar, salvo las excepciones establecidas.*** ***La empresa operadora tiene la carga de la prueba respecto del reporte efectuado por el importador, el distribuidor, el fabricante en el país, el ensamblador, la casa comercializadora,***	La modificación del texto corresponde a la alineación de este con la obligación que se encuentra establecida en los artículos 11° y 12 del Reglamento del Decreto Legislativo N° 1338, emitido en el año 2019. **Artículo 11.- Suspensión y bloqueo** 11.1. La empresa operadora suspende el servicio y bloquea el equipo terminal reportado como sustraído o perdido por parte del abonado, su representante o usuario, de manera inmediata, previa consulta en línea, a través del sistema automático implementado por las empresas operadoras y el OSIPTEL. La suspensión del servicio se sujeta a lo establecido en las Condiciones de Uso aprobadas por OSIPTEL. 11.2. En caso el bloqueo sea solicitado por las casas comercializadoras de equipos y/o aparatos de telecomunicaciones, los importadores, distribuidores, fabricantes o ensambladores, personas naturales, las empresas operadoras lo realizan en un plazo máximo de dos (2) días calendario contados desde que fue efectuado el reporte, previa consulta a través del sistema automático implementado por las empresas operadoras y el OSIPTEL. (…)

<u>o persona natural, así como sobre la entrega del código correlativo del reporte.</u>

Previa validación conforme a lo previsto en la Norma de las Condiciones de Uso, los concesionarios móviles deben registrar en el RENTESEG la información de equipos terminales móviles sustraídos, perdidos y recuperados que han sido reportados por los importadores, ensambladores, fabricantes en el país, casas comercializadoras de equipos y/o aparatos de telecomunicaciones, distribuidores, personas naturales o los concesionarios móviles, , en un plazo máximo de un (1) día calendario de efectuado el reporte, a efectos de obtener la autorización para realizar la acción que corresponda en el IMEI del equipo terminal móvil respectivo.

El RENTESEG realiza el análisis respectivo y de forma inmediata:

(i) *Envía al concesionario móvil que realiza el reporte, la autorización para realizar según corresponda, el bloqueo o desbloqueo del equipo terminal móvil, o de ser el caso, el RENTESEG le indicará que no se realizará acción alguna.*
(ii) *Envía a los otros concesionarios móviles la instrucción del bloqueo o desbloqueo, según corresponda, del equipo terminal móvil sustraído, perdido o recuperado.*

El mensaje a ser enviado por el RENTESEG se sujeta a las indicaciones establecidas en el Instructivo Técnico.

Al recibir este mensaje, los concesionarios móviles implementarán de forma inmediata la instrucción recibida por el RENTESEG, debiendo registrar la fecha y hora respectiva en que lo realizan.

Artículo 12.- Reporte de equipos terminales móviles recuperados

Para la recuperación de equipos terminales móviles registrados en la Lista Negra, **las empresas operadoras** deben considerar lo siguiente:

a) **<u>La recuperación de equipos terminales móviles previamente registrados como sustraídos o perdidos es reportada por el abonado, las casas comercializadoras de equipos y/o aparatos de telecomunicaciones, los importadores, distribuidores, fabricantes, ensambladores o empresas operadoras.</u>**

(…)

Como se puede advertir, el Reglamento del RENTESEG establece que las casas comercializadoras de equipos y/o aparatos de telecomunicaciones, los importadores, distribuidores, fabricantes o ensambladores, personas naturales reporten directamente a cualquier empresa operadora.

Sin perjuicio de ello, considerando que la Norma de las Condiciones de Uso se encuentra dirigida a regular la relación empresa operadora – usuario de los servicios públicos de telecomunicaciones, la disposición referida al reporte de sustracción, pérdida o recuperación de equipos terminales móviles por parte de los importadores, los distribuidores, los fabricantes o ensambladores, las casas comercializadoras o personas naturales será abordado en el artículo 9 de la Normas Complementarias para

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

El plazo máximo desde que se efectúa el reporte, realizado por los importadores, ensambladores, fabricantes en el país, casas comercializadoras de equipos y/o aparatos de telecomunicaciones, distribuidores, personas naturales a los Concesionarios móviles, hasta la ejecución del bloqueo del equipo terminal móvil es de dos (2) días calendario."	la implementación del RENTESEG que hace referencia a dicho reporte.

7.3.3. Sobre la actualización y modificación de artículos en la norma de las condiciones de uso con relación al Renteseg

Se propone la actualización y/o modificación de los artículos 60, 61, 61-A, 65-A, así como el numeral 3.4. del Anexo 5 de la Norma de las Condiciones de Uso, conforme a lo establecido en el Decreto Supremo N° 007-2019-IN que aprueba el Reglamento del Decreto Legislativo N° 1338 y a fin de establecer reglas que permitan una adecuada operatividad y eficacia del RENTESEG, de acuerdo con el siguiente detalle:

Artículo que se propone actualizar	Fundamento
"Artículo 60.- Suspensión del servicio y bloqueo de equipo terminal por la sustracción o pérdida de este último *Luego de efectuado el reporte por parte del abonado o usuario por la sustracción o pérdida del equipo terminal, la empresa operadora está obligada a, **simultáneamente**, suspender el servicio y bloquear el referido equipo, en forma inmediata al reporte. Si la empresa no cumpliera con ello, **no podrá facturar** los consumos que se efectúen desde el momento en que **se realizó** el reporte respectivo.*	Considerando que la Norma de las Condiciones de Uso se encuentra dirigida a regular la relación empresa operadora – usuario de los servicios públicos de telecomunicaciones, la disposición referida al reporte de sustracción o pérdida de equipos terminales móviles por parte de los importadores, los distribuidores, los fabricantes o ensambladores, las casas comercializadoras o personas naturales se dispone que sea abordado en el artículo 9 de la Normas Complementarias para la

OSIPTEL DAPU Y.RIOS
OSIPTEL DAPU L.PALACIOS
OSIPTEL DAPU M.GONZALEZ

Artículo que se propone actualizar	Fundamento
*En ningún caso, la empresa operadora puede realizar únicamente la suspensión del servicio o el bloqueo del equipo terminal, cuando se haya reportado la sustracción o pérdida del equipo terminal móvil**, salvo en los casos en los que el sistema del RENTESEG determine una sola acción.”***	implementación del RENTESEG que hace referencia a dicho reporte.
“Artículo 61.- Reporte por recuperación del equipo *El abonado puede reportar la recuperación del equipo terminal móvil **ante la misma empresa operadora,** que previamente **realizó el bloqueo** por sustracción o pérdida.* ***Dicho** reporte se presenta únicamente en forma personal en las oficinas o centros de atención a usuarios, utilizando el sistema de verificación biométrica de huella dactilar, con excepción de los supuestos contenidos en el punto 3.4 del Anexo 5. No obstante, se puede reportar la recuperación del equipo terminal móvil sin necesidad de realizar la verificación biométrica, empleando la contraseña única a la que hace referencia el punto 3.3 del Anexo 5.* *Una vez realizado el reporte **de recuperación**, la empresa operadora debe proceder de manera inmediata a**: (i)** reactivar el servicio en el mismo IMSI que fue reportado como sustraído o perdido, cuando se trate del reporte efectuado por el abonado; y **(ii)** levantar el bloqueo del equipo terminal, modificando su estado*	Del mismo modo, considerando que la Norma de las Condiciones de Uso se encuentra dirigida a regular la relación empresa operadora – usuario de los servicios públicos de telecomunicaciones, la disposición referida al reporte de recuperación de equipos terminales móviles por parte de los importadores, los distribuidores, los fabricantes o ensambladores, las casas comercializadoras o personas naturales se dispone que sea abordado en el artículo 9 de la Normas Complementarias para la implementación del RENTESEG que hace referencia a dicho reporte.

Artículo que se propone actualizar	Fundamento
en el listado de equipos terminales sustraídos, perdidos, recuperados ***o reportados por fraude.*** *Adicionalmente, la empresa operadora debe entregar al* ***abonado*** *un código correlativo de* ***dicho*** *reporte.* *La carga de la prueba del reporte* ***por recuperación*** *efectuado por el abonado, así como la entrega del código correlativo del referido reporte,* ***corresponde a*** *la empresa operadora."*	
"Artículo 61-A.- Desbloqueo por regularización de equipo terminal en el RENTESEG ***En caso el bloqueo del equipo terminal móvil haya sido realizado por no encontrarse en la Lista Blanca debido a que no fue registrado en el RENTESEG por alguna casa comercializadora o importadora, el abonado puede solicitar a la casa comercializadora o importadora la regularización del reporte del IMEI involucrado para que estas realicen el reporte respectivo.*** ***En caso se haya bloqueado un equipo terminal móvil de un abonado que no cumplió con declarar el ingreso del citado equipo adquirido en el extranjero, corresponde al abonado seguir el procedimiento indicado en el artículo 64.*** ***La empresa operadora debe ejecutar el desbloqueo del equipo terminal móvil bloqueado por no encontrarse en la Lista***	Se incluye esta disposición a fin de precisar los supuestos en los cuales corresponde el desbloqueo del equipo terminal luego de su regularización en el RENTESEG, así como que el plazo en el cual debe ejecutar dicha acción la empresa operadora.

Artículo que se propone actualizar	Fundamento
Blanca que se haya regularizado, de manera inmediata a la acción comunicada por el RENTESEG".	
"Artículo 65.- Cuestionamiento al bloqueo del equipo terminal y suspensión del servicio *En caso de existir cuestionamiento respecto al bloqueo del equipo terminal y/o suspensión del servicio por alguna de las causales previstas en el presente Título, esta situación debe ser comunicada personalmente por el abonado, en cualquiera de las oficinas o centros de atención de la empresa operadora* ***que le presta el servicio****. Para tal efecto, el abonado debe acercarse conjuntamente con el equipo terminal bloqueado y el SIM Card o Chip correspondiente****, así como, de ser posible, con el documento físico o virtual que acredite la propiedad del equipo****.* *Al respecto, rigen las disposiciones establecidas en las Normas Complementarias del RENTESEG."*	Se precisa que el abonado debe acercarse a presentar su cuestionamiento de bloqueo de equipo terminal móvil, de ser posible, con el documento físico o virtual que acredite la propiedad o posesión lícita del equipo. Ello con la finalidad que pueda acreditar que el equipo bloqueado por un tercero le pertenece. Este documento cobra relevancia en el caso de equipos bloqueados por IMEI clonado, considerando que, en estos casos, muchas veces, el IMEI físico no se encuentra visible y por tanto no hay forma de determinar cuál es el equipo original. Sin perjuicio de ello, es de precisar que los documentos que acredite la propiedad del equipo por parte del abonado no son requisitos para la presentación del cuestionamiento, por lo que su no presentación no limita su derecho a cuestionar el bloqueo del equipo terminal ante la empresa operadora, y solicitar la elevación de su caso al Osiptel en caso no haya superado las demás validaciones y la empresa no haya dispuesto su desbloqueo inmediato.
"Artículo 65-A.- Bloqueo del equipo terminal móvil por fraude ***La empresa operadora de forma inmediata a la presentación del reclamo por contratación no solicitada y/o portabilidad numérica no solicitada, procede a registrar en el RENTESEG el bloqueo del equipo terminal que fue vinculado al servicio para su adquisición o financiamiento."***	Actualmente la normativa establece que con la presentación del reclamo de portabilidad numérica no solicitada también se cuestiona la adquisición del equipo terminal y se considera como una causal de bloqueo. No obstante, corresponde ampliar el alcance de dicha disposición siendo que los fraudes que pueden impactar en equipos terminales móviles no se limitan a

Artículo que se propone actualizar	Fundamento
"IMSI**: **De las siglas en inglés International Mobile Subscriber Identity (Identificador Internacional de Suscriptor Móvil). Es el código de identificación internacional único para cada abonado del servicio público móvil, el cual se encuentra integrado a la SIM card, chip u otro equivalente, que permite su identificación a través de las redes de servicios móviles."	portabilidades no solicitadas, sino también ocurren en casos de contratación no solicitada sea prepago o pospago. Cabe indicar que, las Normas complementarias del RENTESEG establece que el equipo terminal móvil reportado por fraude comprende a aquellos que han sido adquiridos al concesionario móvil a través de una contratación no solicitada o portabilidad sin consentimiento. Por lo que con esta modificación solo se adecúa la Norma de las Condiciones de Uso a las Normas Complementarias para la implementación del RENTESEG. **Normas Complementarias para la Implementación del RENTESEG** **Artículo 3.- Definiciones** Para efectos de la presente norma se tendrán en cuenta las siguientes definiciones: (…) **3.22 Equipo terminal móvil reportado por fraude:** Equipo terminal móvil que ha sido adquirido al concesionario móvil a través de una contratación no solicitada o portabilidad sin consentimiento. (…)

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Artículo que se propone actualizar	Fundamento
Se propone modificar las siguientes definiciones del "Anexo 1: Glosario de Términos" de la Norma de las Condiciones de Uso, de acuerdo con el siguiente texto: ***"RENTESEG:** Al Registro Nacional de Equipos Terminales Móviles para la Seguridad a que se hace referencia en el Decreto Legislativo Nº 1338, "Decreto Legislativo 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" **y su Reglamento**."*	Se adecua la definición del término "RENTESEG", considerando que el Reglamento del Decreto Legislativo Nº 1338 aprobado por el Decreto Supremo N° 007-2019-IN reemplazó al anterior Decreto Supremo-Nº 009-2017-IN.
Se propone modificar el numeral 3.4. del Anexo 5 de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, de acuerdo con el siguiente texto: ***"3.4. Excepciones a la verificación biométrica por huella dactilar*** *No resulta exigible a la empresa operadora de los servicios públicos móviles la verificación biométrica por huella dactilar en los siguientes supuestos:* *(i) Cuando el solicitante del servicio público móvil adolezca de alguna discapacidad física o su huella se encuentre desgastada de modo que le impida materialmente someterse a la verificación biométrica de huella dactilar.*	El artículo 8.1 del Decreto Legislativo N° 1338 establece la obligación de las empresas operadoras de verificar la identidad del contratante mediante el sistema de verificación biométrica, salvo las excepciones señaladas en su reglamento. A partir de ello, el Decreto Supremo N° 007-2019-IN -Reglamento del Decreto Legislativo N° 1338- estableció que, en tanto se implemente el sistema de acceso en línea que permita validar el movimiento migratorio de los extranjeros o sus datos personales contenidos en el Registro Central de Extranjería, la contratación del servicio se realiza previa presentación del original de su documento legal de identidad y conservación de la copia de dicho documento.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Artículo que se propone actualizar	Fundamento
(ii) En el caso de fallas en la conectividad con la base de datos del RENIEC o la Superintendencia Nacional de Migraciones debidamente acreditadas. *En todos los casos, la empresa operadora debe exigir al solicitante del servicio la exhibición del documento legal de identidad, **conservar una copia del referido documento** y para las personas nacionales, requerir una declaración jurada suscrita en la que conste que no ha podido realizarse la verificación biométrica, especificando la causal indicada por la empresa operadora, de ser el caso. Dicha declaración jurada debe contener como campos obligatorios a ser llenados por el solicitante del servicio, sus datos personales correspondientes al nombre de la madre, nombre del padre y el distrito de nacimiento. La empresa operadora debe conservar la referida declaración jurada.* *Las empresas operadoras deben contrastar la información contenida en los campos obligatorios señalados en el párrafo anterior, con la información de la base de datos del RENIEC, dentro de los dos (2) días hábiles siguientes. En caso de encontrarse inconsistencias al hacer la validación contra la base de datos del RENIEC, se desactiva el servicio en un plazo no mayor de dos (2) días hábiles de advertida la inconsistencia.* *En el caso del numeral (ii), no es exigible la suscripción de la declaración jurada, en caso las empresas operadoras hayan conservado la huella digital del solicitante del servicio, previa autorización de este, y dentro del plazo señalado en el párrafo*	***Artículo 41.- Contratación del servicio para los extranjeros*** *En el caso de las personas extranjeras que no están registradas en el RENIEC, a quienes no les resulta aplicable el sistema de verificación de identidad señalado en el artículo 38 del presente reglamento, **en tanto se implemente el sistema de acceso en línea que permita validar el movimiento migratorio de los extranjeros o sus datos personales contenidos en el Registro Central de Extranjería**, la contratación del servicio se realiza previa presentación del original de su documento legal de identidad, con la finalidad que la empresa operadora proceda a registrar los datos personales del abonado **y archivar copia del documento legal presentado**.* Al respecto, de la revisión de la normativa vigente, se advierte que con fecha 28 de setiembre de 2023, la Superintendencia Nacional de Migraciones emitió la Resolución de Superintendencia N° 171-2023-MIGRACIONES, a través de la cual (i) autorizó la prestación de los servicios no exclusivos: "Consulta de Carnet de Extranjería", "Consulta de Movimiento Migratorio" y "Verificación Biométrica", que se brindan a través del aplicativo "MIGRACIONES Servicios en Línea" para las empresas de telefonía móvil que se encuentran bajo el ámbito de supervisión del OSIPTEL, (ii) estableció los costos de los servicios y (iii) aprobó el modelo de contrato de acceso a dicho aplicativo.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Artículo que se propone actualizar	Fundamento
anterior, realicen el contraste biométrico con la base de datos del RENIEC o la Superintendencia Nacional de Migraciones. *En los casos que corresponda, la empresa operadora debe conservar y almacenar el reporte de la verificación en el que conste que la huella dactilar del solicitante del servicio no puede ser reconocida por el dispositivo analizador, la declaración jurada,* ***así como la copia del documento legal de identificación del solicitante del servicio****, durante el plazo establecido en el punto 2.2.* *La empresa operadora debe comunicar y acreditar al Osiptel las interrupciones por fallas de conexión y el periodo de las mismas, a través de los mecanismos que se dispongan para tal efecto.* ***La empresa operadora es responsable de aplicar las disposiciones de este punto solo luego de verificar la ocurrencia de cualquiera de los supuestos indicados en los numerales (i) y (ii) antes mencionados. La empresa operadora tiene la carga de la prueba de la ocurrencia de tales supuestos****".*	En ese sentido, al haberse implementado, a la fecha, el sistema de acceso en línea de consulta de movimiento migratorio y verificación biométrica por parte de la Superintendencia Nacional de Migraciones, el supuesto de excepción de verificación biométrica del contratante extranjero no resulta aplicable; por lo que debe seguirse la regla general de validar la identidad del contratante mediante verificación biométrica. En consecuencia, en el caso del solicitante de nacionalidad extranjera dicha verificación debe ser realizada por las empresas operadoras a través del servicio en línea de verificación biométrica contrastada con la base de datos de la Superintendencia Nacional de Migraciones. Solo para el caso de personas con discapacidad física o huella desgastada que impida la verificación biométrica, o fallas de conectividad con RENIEC o la Superintendencia Nacional de Migraciones, se admite que pueda validarse la identidad siguiendo el procedimiento de excepción previsto en el numeral 3.4 del Anexo 5 de la Norma de las Condiciones de Uso, y, por tanto, en tales casos el medio probatorio a considerar es la copia del documento legal de identidad presentado por el solicitante para la contratación, así como, para el caso de personas nacionales la declaración jurada correspondiente.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

De otro lado, se propone incluir una definición al “Anexo 1; Glosario de Términos” de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, conforme al siguiente detalle:

Artículo que se propone actualizar	Fundamento
Se propone incluir la siguiente definición al “Anexo 1: Glosario de Términos” de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobada mediante Resolución de Consejo Directivo N° 172-2022-CD/OSIPTEL, de acuerdo con el siguiente texto: ***“IMSI**: **De las siglas en inglés International Mobile Subscriber Identity (Identificador Internacional de Suscriptor Móvil). Es el código de identificación internacional único para cada abonado del servicio público móvil, el cual se encuentra integrado a la SIM card, chip u otro equivalente, que permite su identificación a través de las redes de servicios móviles.”***	Se considera la inclusión de los términos y sus definiciones, conforme a lo establecido en el artículo 3° del Decreto Supremo N° 007-2019-IN. ***IMSI:** De las siglas en inglés International Mobile Subscriber Identity (Identificador Internacional de Suscriptor Móvil). Es el código de identificación internacional único para cada abonado del servicio público móvil, el cual se encuentra integrado a la SIM card, chip u otro equivalente, que permite su identificación a través de las redes de servicios móviles.*

7.3.4. Sobre medidas de seguridad para la entrega de la contraseña única

Se propone modificar el numeral 3.3 del Anexo 5de la Norma de las Condiciones de Uso, respecto de la entrega de la contraseña única, conforme se detalla a continuación:

Artículo que se propone modificar	Fundamento
3.3. Contraseña Única ***La contraseña única es un mecanismo de validación de identidad del abonado y puede ser empleada por la empresa operadora como mecanismo de contratación al que se refiere el numeral 3 del artículo 19.*** ***La empresa operadora del servicio público móvil debe entregar de oficio al abonado la contraseña única al momento de realizar la contratación u otro trámite en el que se valide su identidad, así como a requerimiento expreso del abonado.*** *La empresa operadora que presta servicios distintos al servicio público móvil puede implementar la utilización de esta contraseña* ***sujeto a lo establecido en la presente norma.*** *La empresa operadora al momento de su entrega debe informar al usuario sobre el uso de la contraseña única, los trámites en los cuales es obligatoria y la forma de recuperación.* ***Para el servicio público móvil, previo a su entrega, se requiere validar la identidad del abonado mediante verificación biométrica de huella dactilar contrastada con la base de datos del RENIEC o mediante el procedimiento establecido en el numeral 3.4 del Anexo 5. En los demás servicios, la validación de identidad del abonado se realiza conforme a lo establecido en el numeral 3.1 del Anexo 5. La empresa operadora puede emplear otro mecanismo de***	En el mes de junio de 2022 entró en vigencia la disposición sobre la entrega obligatoria de la contraseña única por parte de las empresas operadoras, no obstante, pese a haber transcurrido más de un año, siguen llegando casos a conocimiento del Osiptel de usuarios que no se les brindó la contraseña única por encontrarse dentro de las excepciones de verificación biométrica o por no contar con un Smartphone que les permita acceder a los aplicativos de las empresas operadoras que habrían establecido la empresa únicamente por dicho medio. En ese sentido, con la finalidad de masificar el uso de la contraseña única, se establecen reglas detalladas sobre su entrega las cuales recogen las actuales prácticas de las empresas operadoras. Asimismo, se precisa la obligación de la empresa operadora de permitir que cualquiera de sus abonados obtenga su contraseña única, incluyendo aquellos que no cuentan con acceso a Internet fijo o móvil o correo electrónico. En ese sentido, para cumplir dicha finalidad deberá implementar no solo mecanismos digitales sino también físicos de modo que todos sus usuarios puedan obtener su contraseña única.

Artículo que se propone modificar	Fundamento
validación de identidad del abonado previa aprobación del Osiptel. *La empresa operadora entrega la contraseña única en cualquiera de las oficinas o centros de atención de la empresa operadora y los* ***puntos de atención habilitados según*** *lo dispuesto en el Reglamento de Atención, previamente reportados al OSIPTEL. La empresa operadora podrá habilitar* ***otros canales o*** *mecanismos para hacer efectiva la entrega o recuperación de la contraseña única, previa aprobación del OSIPTEL.* ***La empresa operadora realiza la entrega de la contraseña única mediante:*** ***i) Un código provisional que, de forma directa, se proporciona al abonado a través de un documento físico cerrado, un mensaje de texto al servicio móvil bajo su titularidad y/o al correo electrónico registrado por el abonado al momento de la contratación o en otro en que haya validado su identidad conforme al quinto párrafo. La empresa operadora debe exigir que el abonado modifique dicha contraseña antes de realizar el primer trámite que requiera su uso. La modificación se realiza a través de un equipo físico que se encuentre a disposición y uso exclusivo de los abonados o en un sitio web, plataforma o aplicativo informático de la empresa operadora.*** ***ii) El envío de un enlace personalizado que deriva a un sitio web o plataforma que permite su generación directa, remitido a través de un mensaje de texto al servicio móvil***	

Artículo que se propone modificar	Fundamento
bajo su titularidad y/o al correo electrónico registrado por el abonado al momento de la contratación o en otro momento en que haya validado su identidad conforme al quinto párrafo. ***iii) El ingreso de una clave secreta por parte del abonado a través de un equipo físico que se encuentre a su disposición y uso exclusivo, el cual transfiere la información de la contraseña única directamente al sistema comercial de la empresa operadora.*** ***La vigencia máxima del código provisional o enlace es de siete (7) días calendario desde su entrega.*** *En ningún caso el sistema implementado por la empresa operadora para el cumplimiento de lo dispuesto en el presente artículo, permite que su personal de atención obtenga o tenga acceso a la contraseña del abonado.* ***La empresa operadora debe permitir y garantizar que cualquiera de sus abonados obtenga su contraseña única, incluyendo aquellos que no cuentan con acceso a Internet fijo o móvil o correo electrónico, para lo cual implementa las formas de entrega descritas en los numerales (i), (ii) y/o (iii).*** ***La empresa operadora debe remitir un mensaje de texto a el(los) servicio(s) público(s) móvil(es) del abonado, así como un correo electrónico a la dirección registrada por este, informando sobre la fecha y hora de generación de la***	

Artículo que se propone modificar	Fundamento
contraseña única, y de su modificación o recuperación, de ser el caso. ***La empresa operadora debe permitir que el abonado pueda cambiar dicha contraseña las veces que lo requiera a través de los canales establecidos para su generación. La recuperación de la contraseña única sigue el procedimiento establecido para su obtención.*** *Las empresas operadoras tienen la obligación de comunicar al Osiptel, de manera previa a su utilización, los mecanismos que implementen en aplicación del presente artículo, así como los mecanismos de seguridad que son empleados para tales efectos.* *En el caso de servicios móviles, para la contratación de nuevos servicios, cambio de titularidad y reposición de SIM Card, de manera adicional a las validaciones de identidad previstas en el artículo 18, los puntos 1.2 y 7 del anexo 2 y los puntos 3.1 y 3.2 del presente anexo, se requiere que* ***el abonado o el representante legal designado de acuerdo con lo establecido en el artículo 4,*** *proporcione la contraseña única de forma exitosa.* ***La empresa operadora que decida emplear la contraseña única como mecanismo de contratación para nuevos servicios*** *debe contar con la aprobación previa del Osiptel, de conformidad con lo dispuesto en punto 1.2.”*	

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

Con relación al régimen sancionador se propone incluir el artículo 77 a la Norma de las Condiciones de Uso, conforme al siguiente detalle:

Propuesta	Fundamento
Artículo 77.- Régimen de Infracciones *Las empresas operadoras serán sancionadas en los casos de incumplimiento de las obligaciones contenidas en las presentes Condiciones de Uso, de acuerdo al procedimiento y disposiciones previstas en la Ley Nº 27336, Ley de Desarrollo de las Funciones y Facultades de Osiptel, y en el Reglamento General de Infracciones y Sanciones aprobado por Osiptel.* *Constituyen infracciones el incumplimiento, por parte de la empresa operadora, de cualquiera de las disposiciones contenidas en:* *Los artículos 2 (segundo párrafo) 3, 4, 5 (segundo y cuarto párrafo), 7, 7-A, 8, 9, 10, 11, 11-A, 12, 13, 14, 15, 16, 18, 18-A 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 35, 36, 37, 38, 39, 39-A, 40, 42, 43, 44, 45, 46, 47, 48-A, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61,* ***61-A,*** *64, 65,* ***65-A,*** *66, 67, 68, 69, 70, 71, 72, 73, 74, 75 y 76 y las Disposiciones Finales Tercera, Cuarta y Sétima.* *Los puntos 1.1, 1.2, 1.3, 2.1, 2.2, 3.2, 4.1, 4.2, 4.4, 5, 6, 7, 8.1 del Anexo 2; 1, 2 y 3 del Anexo 3; 1.1, 1.2, 2, 3.1, 3.2, 3.3, 3.4 y 3.5 del Anexo 4; 1.2, 1.3, 1.4, 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 3.1, 3.2, 3.3, 3.4 y 4 del Anexo 5; 1, 2, 3, 4.1, 5 y 6 del Anexo 6; 1.1, 1.3, 1.5, 2.1, 2.4, 3.1, 3.2, 3.3, 3.4 del Anexo 8.* *También constituye infracción el incumplimiento de la Resolución de Gerencia General a que se refiere el punto 2.1 del Anexo 5, que ordena revocar o corregir cualquier modificación implementada por la empresa operadora."*	Con la finalidad de generar los incentivos adecuados respecto del cumplimiento de las modificaciones propuestas, se propone modificar el régimen de infracciones de la Norma de las Condiciones de Uso, a fin de establecer como infracción administrativa el incumplimiento de los numerales 61-A y 65-A del Anexo 5 que se propone incorporar.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

7.3.5. Sobre la vigencia de la propuesta normativa

Sobre la vigencia de la normativa y demás disposiciones complementarias, se propone lo siguiente:

Propuesta	Fundamento
Norma que modifica la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones **Primera.- Vigencia** Las disposiciones de la presente norma entran en vigencia a partir del inicio de la tercera fase del RENTESEG, con excepción de: - El numeral 3.4 del Anexo 5, el cual entra en vigencia a los seis (6) meses de publicada la presente norma en el diario oficial El Peruano, y - El numeral3.3 del Anexo 5, el cual entra en vigencia el primer día hábil del mes de enero de 2025. **Norma que modifica las Normas Complementarias para la Implementación del RENTESEG** **Primera.- Vigencia** Las disposiciones de la presente norma entran en vigencia a partir del inicio de la tercera fase del RENTESEG con excepción del artículo 15-A, el cual entra en vigencia el primer día hábil del mes de enero de 2025.	Se propone que la norma entre en vigencia de forma escalonada, conforme al siguiente detalle: • **Al inicio de la III fase del RENTESEG:** Todas las disposiciones que no implican nuevas obligaciones, en tanto, conforme se desarrolla en el presente Informe, corresponden a adecuaciones de algunas disposiciones de la Norma de Condiciones de Uso y las Normas Complementarias del RENTESEG al Reglamento del RENTESEG. Asimismo, aquellas obligaciones referidas al reporte y recojo de Lista de excepción; y el procedimiento de cuestionamiento ante equipo bloqueado por IMEI clonado y otros motivos. Considerando que se tratan de obligaciones que se encuentran previstas en otros cuerpos normativos, instructivos y/o manuales de operación, en los cuales se otorgó un plazo de adecuación, el cual –en algunos casos- fue prorrogado en varias oportunidades, se dispone la vigencia de estas disposiciones al inicio de la tercera fase del RENTESEG, siendo que se requiere su aplicación a partir de dicha fecha. • **Al primer día hábil del mes de enero de 2025:** Aquellas obligaciones referidas a: **(i)** las reglas sobre contraseña única**,** y **(ii)** el reporte de bloqueo y desbloqueo de los equipos

	terminales móviles que hayan sido reportados por Uso Prohibido a través del RENTESEG. Asimismo, la eliminación del procedimiento de cuestionamiento de titularidad prepago. Considerando los comentarios de las empresas operadoras se brinda un plazo para que realicen las adecuaciones de sus sistemas y procesos a fin de dar estricto cumplimiento a las disposiciones emitidas.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

8. DIFUSIÓN Y PARTICIPACIÓN DE LOS AGENTES INVOLUCRADOS

De acuerdo con el artículo 7 del Reglamento General del OSIPTEL, toda decisión de este Organismo deberá adoptarse de tal manera que los criterios a utilizarse sean conocidos y predecibles por los administrados.

Asimismo, el artículo 27 del Reglamento antes citado dispone que constituye un requisito para la aprobación de los reglamentos, normas y disposiciones regulatorias de carácter general que dicte el OSIPTEL, el que sus respectivos proyectos sean publicados en el diario oficial El Peruano, con el fin de recibir las sugerencias o comentarios de los interesados.

Este proyecto normativo fue aprobado para comentarios mediante la Resolución N° 00228-2023-CD/SIPTEL, publicada el 2 de agosto de 2023. En la referida resolución se estableció un plazo de quince (15) días hábiles para que los agentes interesados presenten sus comentarios. Durante este período se recibieron los comentarios de Viettel Perú S.A.C. (en adelante, Viettel), Entel Perú S.A. (en adelante, Entel), Flash Servicios Perú S.R.L. (en adelante, Flash), América Móvil Perú S.A.C. (en adelante, América Móvil) y Telefónica del Perú (en adelante, Telefónica).

9. CONCLUSIONES Y RECOMENDACIONES

9.1 De enero de 2017 a noviembre de 2023, se han reportado 12.7 millones de equipos terminales móviles por sustracción, según lo registrado en lista de negra administrada por el RENTESEG. Dentro de las medidas implementadas para combatir la problemática de robo y/o sustracción de equipos terminales móviles, se procedió a ejecución del bloqueo de dispositivos que cuenten con un código IMEI que no cumple con los estándares establecidos por la GSMA. No obstante, las organizaciones criminales han optado por la implementación de técnicas de clonación del código IMEI genuino u original para hacer frente al bloqueo de equipos terminales móviles.

9.2 Según la última evaluación, se detectó que los IMEI identificados como clonados se encuentran asociados a 881 236 líneas móviles, esto implica que, en promedio, un IMEI original o genuino ha sido clonado 1.6 veces dentro de la propia red móvil. Comparando con lo observado en marzo del 2022, donde se identificaron 471 660 líneas asociadas a IMEI originales, se ha encontrado que la cantidad de clonaciones se ha mantenido en 1.7 veces. Cabe señalar que el 95.6% de los IMEI con líneas asociadas clonadas ha sido clonada entre 2 y 4 veces, el 4.1% entre 5 y 20 veces y el 0.3% más de 20 veces.

9.3 Con la finalidad de dar solución a los problemas presentados, se analizaron dos alternativas de solución, mediante un análisis costo-beneficio (ACB). Para el ACB, se adoptaron una serie de supuestos para estimar los costos y beneficios proyectados para un período de 6 años, obteniendo como ratio beneficio-costo el valor de 5.64 lo que indica que resulta más beneficioso socialmente adoptar el paquete de medidas en su conjunto.

En atención a ello, se ha elaborado la propuesta de norma que establece el procedimiento de bloqueo de equipos terminales móviles detectados con IMEI clonados con derecho a cuestionamiento.

Del mismo modo, se propone modificar la Norma de las Condiciones de Uso a fin de eliminar el procedimiento de cuestionamiento de titularidad prepago y establecer un procedimiento detallado sobre la contraseña única.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

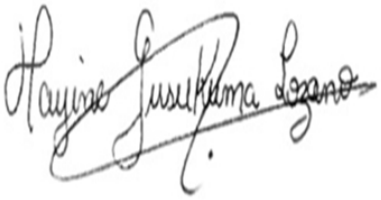
OSIPTEL DAPU M.GONZALEZ

9.4 Asimismo, se propone actualizar algunos artículos contenidos en la Norma de Condiciones de Uso y las Normas Complementarias RENTESEG considerando la última modificación del Reglamento del Decreto Legislativo N° 1338, y, en esa línea, establecer reglas sobre el desbloqueo por regularización de equipo terminal en el Renteseg, así como respecto del boqueo del equipo terminal móvil en los casos de contratación o portabilidad no solicitada.

9.5 De acuerdo con lo antes expuesto, se advierte que los cambios normativos incluidos en esta propuesta normativa obedecen a adecuaciones necesarias para garantizar la seguridad en la contratación y la continuidad en la prestación de los servicios públicos de telecomunicaciones, en atención a modificaciones establecidas en los cuerpos normativos emitidos por el Osiptel, así como otros de mayor rango.

9.6 Se recomienda elevar al Consejo Directivo del OSIPTEL el presente informe sustentatorio y la propuesta normativa, para su respectiva aprobación, de considerarlo pertinente.

Atentamente,



Firmado digitalmente por: GUSUKUMA LOZANO Hayine Juana FAU 20216072155 soft

HAYINE JUANA GUSUKUMA LOZANO.
DIRECTORA DE ATENCIÓN Y PROTECCIÓN DEL USUARIO (E)
DIRECCIÓN DE ATENCIÓN Y PROTECCIÓN DEL USUARIO

REFERENCIAS

Besanko, D., Braeutigam, R. (2010). *Microeconomics 4th Edition*

CRC (2019). *Simplificación del marco regulatorio para la restricción de equipos terminales hurtados. Documento de Formulación del Problema, Colombia.*

GSMA (2018). *Seguridad y privacidad en las redes móviles. Desafios, propuestas y consideraciones para los gobiernos.*

GSMA (2021). *Access to Mobile Services and Proof of Identify 2021.*

INEI (Febrero 2022). *Informe Técnico N° 2: Estadísticas de Seguridad Ciudadana, Lima.*

Kumar, Saurabh (2015). *Mobile Security, Phone Tracking and IMEI Cloning Detection.* Computer Science & Engineering Department, Delhi Technological University Delhi *– 110042, India.*

Kumar, Kumar & Kaur, Prabhpreet (Mayo 2015). *Vulnerability Detection of International Mobile Equipment Identity Number of Smartphone and Automated Reporting of Changed IMEI Number.* International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, pg. 527-533.

Díaz, E., del Valle, C. (2017) *Manual de Economía del Comportamiento. Volumen III: Finanzas del comportamiento*, Instituto Mexicano de Economía del Comportamiento. Disponible en el siguiente enlace: https://static1.squarespace.com/static/57081929356fb0c9e49157eb/t/595994883a0411448680d5e5/1499042991279/Manual+FINANZAS.pdf

Mjaku, Gentiana (2020). *Why is customer loyalty so important in the banking sector? - An overview.* International Journal of Scientific and Research Publications, Volume 10. Disponible en el siguiente enlace al 03/06/2023): https://www.ijsrp.org/research-paper-0920/ijsrp-p10596.pdf

Ordoñez, J. (2009). *Aspectos económicos del funcionamiento competitivo de los mercados.* Agencia de Defensa de la Competencia de Andalucía.

Salmiah Mohamad Amin et al. (2012). *Factors Contributing to Customer Loyalty Towards Telecommunication Service Provider.* The 2012 International Conference on Asia Pacific Business Innovation & Technology Management.

Telecomunications Management Group (2018). *Hurto de equipos móviles en América Latina. Políticas e iniciativas actuales.*

Torrão Pinheiro, José Carlos Silva (2022). *Understanding Customer Loyalty And Satisfaction In The Portuguese Telecommunications Sector*. Disertación del Master en Gestión. Universidad de Porto, Facultad de Economía. Disponible en el siguiente enlace al 03/06/2023): https://repositorio-aberto.up.pt/bitstream/10216/146637/2/596997.pdf

UIT (2020a). *Recomendación UIT-T Q-5051. Marco para luchar contra la utilización de dispositivos móviles robados.*

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

UIT (2020b). Technical Report *QTR-RLB-IMEI. Reliability of International Mobile station Equipment Identify (IMEI).*

UIT (2020c). *Recomendación ITU-T Q5052. Adressing mobile devices with duplicate unique identifier.*

ANEXO N° 1 Proyección de los IMEI clonados o duplicados intra-red

En este anexo se exponen las consideraciones metodológicas adoptadas para poder proyectar, a 5 años, la cantidad de nuevos IMEI clonados o duplicados intra-red en el escenario base y en los escenarios contrafactuales.

a) Stock de IMEI clonados o duplicados intra-red – escenario base

A octubre del 2023, se tiene un stock de 944 624 IMEI clonados, los cuales se han ido acumulando en el tiempo debido a que todavía no se ha procedido a la desconexión de estas líneas. Comparando con el stock de marzo de 2022, el cual se estima en 605 209 IMEI clonado, se ha encontrado que la cantidad acumulada se estaría incrementando en 17 864 IMEI clonados al mes, como se puede apreciar en el cuadro siguiente. A partir de esta información, se proyecta que, a diciembre de 2023, el stock de IMEI clonados debería llegar a 962 488, dado que se le están sumando los nuevos casos que podrían darse de abril a diciembre. Finalmente, asumiendo que en el escenario base se mantiene la misma cantidad mensual de nuevos IMEI clonados (17 864), se estima que anualmente se darían 214 368 nuevos casos de IMEI clonados.

CUADRO N° 9:STOCK DE IMEI CLONADOS O DUPLICADOS INTRA-RED

	Marzo 2022	Octubre 2023	Incremento en 19 meses	Promedio mensual
IMEI clonados	605 209	944 624	339 415	17 864
Proyección a Dic	-	962 488		

Nota: En marzo 2022, se estima la cantidad de IMEI clonados de Entel debido a que no aplicó la metodología de detección. El stock de IMEI clonados sin Entel es 471 660.
Fuente: RENTESEG
Elaboración: OSIPTEL

Para estimar el acumulado de casos del 2023 y los nuevos casos en el período 2024 al 2029 para los escenarios contrafactuales (alternativa 2.1 y alternativa 2.2), se está asumiendo que ambas medidas regulatorias generan tasas decrecientes de nuevos casos de IMEI clonados.

b) Proyección de nuevos IMEI clonados intra-red

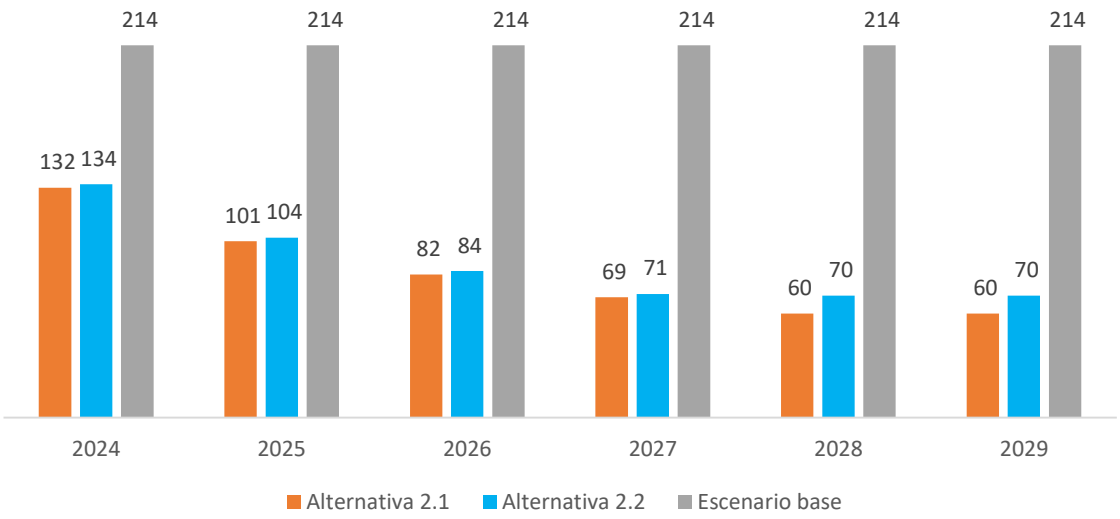
Con el objetivo de estimar la senda de nuevos casos de IMEI clonados en las alternativas 2.1 y 2.2, se ha asumido que esta debería tener semejanza con la evolución observada en la cantidad de IMEI inválidos. Para ello, se procedió a estimar la línea tendencia logarítmica de la cantidad acumulada de IMEI inválidos, obteniéndose el siguiente resultado:

$$y = 472\,203 \ln(x) + 82578$$

Esta ecuación se ha utilizado para obtener una proyección mensual de la cantidad acumulada de IMEI inválidos, la cantidad de nuevos IMEI inválidos y tasas mensuales de nuevos IMEI inválidos. Finalmente, se ha extrapolado estas tasas mensuales a la cantidad mensual inicial de nuevos IMEI clonados (17 864) y se ha obtenido una serie decreciente de nuevos IMEI clonados. Cabe señalar que, respecto a estas proyecciones, la diferencia entre la alternativa 2.1 y la alternativa 2.2 radica solamente en que para la alternativa 2.2 se aplica un rezago de un mes, ello debido a que esta propuesta supone aplicar la desconexión de IMEI clonados luego de una etapa de regularización.

Finalmente, en el gráfico 25 se reporta la proyección de nuevos IMEI clonados para el período 2024 – 2029 en las correspondientes alternativas.

GRÁFICO N° 14: PROYECCIÓN DE NUEVOS IMEI CLONADOS O DUPLICADOS INTRA-RED (Miles)



Fuente: RENTESEG
Elaboración: OSIPTEL

ANEXO N° 2: Supuestos de costos del Análisis Costo-beneficio

Fuentes de costo:	Supuestos y parámetros	
	Alternativa 2	**Alternativa 3**
C1 Costo del abonado presentar un cuestionamiento	- Se obtiene multiplicando el Total de cuestionamientos con el costo de tiempo de espera de un cuestionamiento. - El costo de tiempo de espera de un cuestionamiento se calcula del costo por hora en el Perú (S/ 2.04)[47], dividido por la cantidad promedio de cuestionamientos atendidos por hora[48].	
C2 Costo de la empresa en la evaluación del cuestionamiento	- Se obtiene multiplicando el Total de Cuestionamientos con el costo de evaluar cada cuestionamiento. - Se asume que costo de evaluar cada cuestionamiento de la empresa es igual al costo que asume el OSIPTEL, el cual se estima en S/ 40,7 en el 2021[49].	
C3 Costo de no contar con el servicio	- Este costo se calcula por separado para 2 tipo de abonado: (i) los propietarios originales del IMEI y (ii) abonados estafados con IMEI clonado. - En la alternativa 2 este costo se mide para 90 días calendarios y en la alternativa 3 para 60 días calendarios. - El costo del tiempo sin servicios se obtiene a partir del ARPU promedio, el cual es S/ 17,45 en el 2021[50].	
C4 Costo de baja de servicio	- Es la cantidad de líneas que pierde la empresa multiplicado por el ARPU (S/ 17.45)	
C5 Costo de envío de SMS	- No aplica	- Se obtiene multiplicando la cantidad de IMEI clonados con el precio del SMS y por 15 SMS. - Valor del SMS: S/ 0.002
C6 Costo de la atención presencial por verificación previa	- No aplica	- Se obtiene multiplicando el Total de verificaciones con el costo de tiempo de espera de una verificación. - El costo de tiempo de espera de una verificación se calcula del costo por hora en el

[47] Parámetro obtenido del Anexo N°4 del Informe N°043-DAPU/2022 (Costo por hora del Ministerio de Economía y Finanzas). Disponible en: https://www.osiptel.gob.pe/media/bd5lxazn/informe043-dapu-2022.pdf

[48] En el 2021 se atendieron 7131 cuestionamientos, ello dividido entre 2008 horas, se obtiene 4 cuestionamientos por hora. Se considera que el tiempo que conlleva presentar un cuestionamiento es similar al trámite de reclamo. Parámetro obtenido del Informe N°043-DAPU/2022 (Cuadro N°52). Disponible en: https://www.osiptel.gob.pe/media/bd5lxazn/informe043-dapu-2022.pdf

[49] Calculado a partir de las remuneraciones de dos analistas y dos asistentes legales percibidas en el año 2021, establecidas en Anexo N°01 del Memorando N°00393-GPSU/2019. Adicionalmente, se considera que, durante el año 2021 se atendieron 7 131 cuestionamientos; obteniéndose un costo promedio de S/ 40,72.

[50] Obtenido del Portal PUNKU (ARPU por Servicio Móvil 2021). Disponible en: https://punku.osiptel.gob.pe/FrmLogin.aspx

C7 Costo de atender la verificación previa	- No aplica	Perú (S/ 2.04)[51], dividido por la cantidad promedio de cuestionamientos atendidos por hora[52]. - Se obtiene multiplicando el Total de verificaciones con el costo de evaluar cada cuestionamiento. - Se asume que costo de verificar el equipo es similar a evaluar cada cuestionamiento de la empresa, y es igual al costo que asume el OSIPTEL, el cual se estima en S/ 40,7 en el 2021.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

[51] Parámetro obtenido del Anexo N°4 del Informe N°043-DAPU/2022 (Costo por hora del Ministerio de Economía y Finanzas). Disponible en: https://www.osiptel.gob.pe/media/bd5lxazn/informe043-dapu-2022.pdf

[52] En el 2021 se atendieron 7131 cuestionamientos, ello dividido entre 2008 horas, se obtiene 4 cuestionamientos por hora. Se considera que el tiempo que conlleva presentar un cuestionamiento es similar al trámite de reclamo. Parámetro obtenido del Informe N°043-DAPU/2022 (Cuadro N°52). Disponible en: https://www.osiptel.gob.pe/media/bd5lxazn/informe043-dapu-2022.pdf

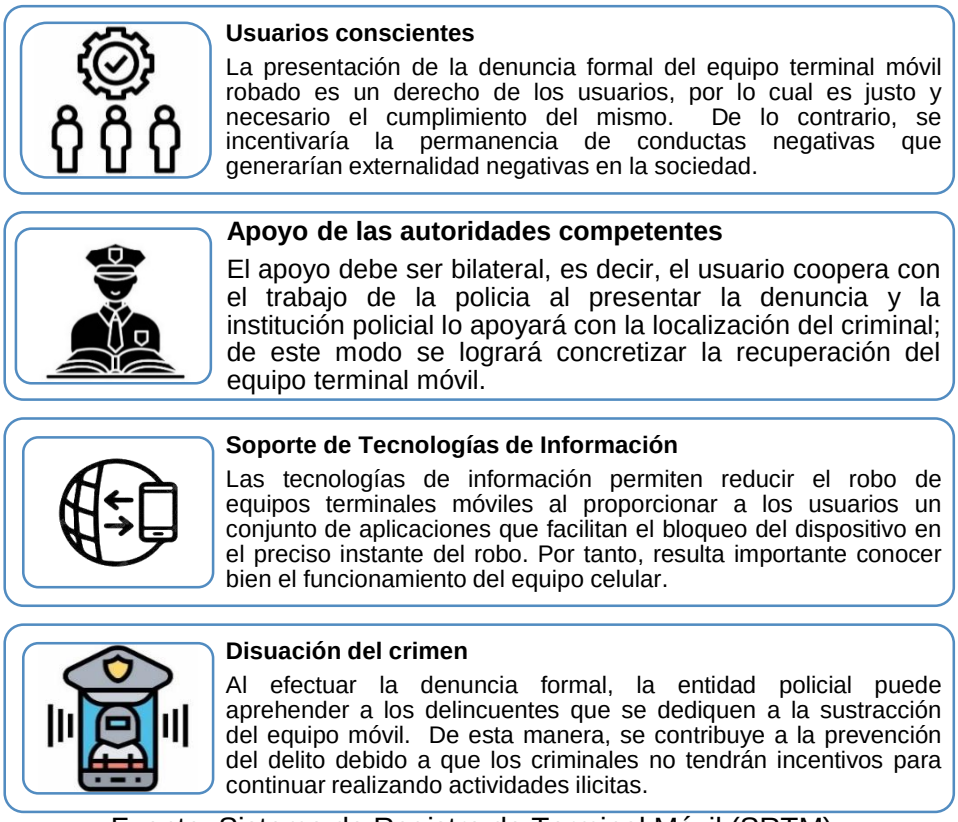
ANEXO N° 3: Comparación internacional de las herramientas de seguridad

En este contexto, la GSMA (2018) ha evaluado esta problemática, proponiendo que los países deberían desarrollar una solución integral y coordinada entre usuarios, concesionarios móviles, gobierno y fabricantes. Específicamente, se propone 4 pilares fundamentales para combatir la comercialización ilegal de equipos móviles (i) Establecer un procedimiento de denuncia de equipos terminales robados, (ii) Creación de Registro de abonados, lista negra (que incluya los equipos terminales reportados como robados) y lista blanca, (iii) Penalizar la adulteración del código IMEI, y (iv) Fabricar y configurar los equipos terminales de manera que cuenten con más mecanismos de seguridad.

- **Establecer un procedimiento de denuncia de equipos terminales robados**

En relación al primer pilar, según el Sistema de Registro de Terminal Móvil (SRTM)[53], es fundamental que las personas tomen conciencia de la importancia de denunciar el robo y/o hurto de un equipo terminal móvil. En ese sentido, se debe tener como objetivo principal la sensibilización de los usuarios a fin de que reflexionen en torno a la presentación de la denuncia de forma oportuna y así, incorporarlo como parte de la cultura con el propósito de generar beneficios para la sociedad en general, tales como:

FIGURA N° 8: BENEFICIOS DE LA DENUNCIA OPORTUNA POR ROBO DE EQUIPO TERMINAL MÓVIL EN LA SOCIEDAD



Fuente: Sistema de Registro de Terminal Móvil (SRTM)

[53] Fuente: SRTM de Colombia. Disponible en: Denunciar robo de celular | Registrarimei.com ©

De este modo, se incentiva a los usuarios a reportar el robo y/o hurto del equipo terminal móvil a fin de que estos equipos no lleguen a formar parte del mercado negro de equipos usados. Así, a través del constante registro de estos dispositivos se obtiene una lista negra robusta y precisa que permita ser consultada por las autoridades policiales, y así impedir que se sigan comercializando equipos robados o perdidos (Telecommunications Management Group – TMG, 2018).

Aunado a lo anterior, es fundamental que los concesionarios móviles incorporen mecanismos de seguridad durante los procedimientos de reporte de sustracción, pérdida y recuperación del equipo terminal móvil, para fortalecer y mejorar los niveles de protección de los usuarios. En ese sentido, según la UIT (2020a), se recomienda priorizar la protección de los datos privados del usuario cuando sea víctima de la sustracción de su dispositivo. Tal es así que, como medida principal, se debe implementar procedimientos que impidan utilizar el equipo terminal de forma rápida y efectiva; complementada con campañas de sensibilización a los usuarios sobre la importancia de proteger sus datos personales y disponer de copias de seguridad.

Al respecto, se evidencia que el reducido nivel de seguridad en los procedimientos de reporte de sustracción, pérdida y recuperación generaría la problemática potencial de reposición fraudulenta del *SIM Card*, denominada también como *SIM Swap*, la cual consiste en que el estafador reporta el equipo móvil como robado, bloqueando la línea para luego poder solicitar la reposición del *SIM Card.* Una vez obtenido el nuevo *SIM Card*, activa la línea y comienza a buscar tener acceso a los datos personales del usuario para realizar algún tipo de transacción.

Se debe señalar que, el *SIM Swapping* ha tomado relevancia al atacar a empresas de telecomunicaciones, lo que representa un problema de alta complejidad. Así, Tamas K. (2021b) enfatiza que, a pesar de las alertas existentes respecto a este tipo de fraude, las empresas pertenecientes al sector de telecomunicaciones aún no han desarrollado algún mecanismo para hacer frente a la problemática, mientras el *SIM Swap* sigue creciendo de manera rampante y sin control, al igual que los ataque a las cuentas *online* de los usuarios.

Ante lo expuesto, resulta de vital importancia concientizar a los usuarios para involucrarlos en la lucha contra el robo de teléfonos móviles (GSMA, 2018), mediante la implementación de herramientas o aplicativos tales como el Sistema de Verificación de Dispositivos que la propia GSMA pone a disposición de los usuarios a través de la página web del regulador para verificar el estado del equipo terminal móvil, en conjunto con las campañas de sensibilización y prevención a los usuarios, destinadas a mejorar su conocimiento y protección con la finalidad de ayudarlos a minimizar su exposición los riesgos que implica ser víctima de robo y/o hurto del equipo terminal móvil.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOS

OSIPTEL DAPU M.GONZALEZ

Creación de registro de abonados, lista negra y lista blanca

Respecto al segundo pilar – creación de lista blanca, lista negra y registro de abonados- se han implementado estas herramientas antirrobo como respuesta al problema actual de sustracción de equipos terminales móviles por parte de los encargados de las políticas públicas y la industria, desarrollando soluciones dirigidas a hacer menos atractivos estos dispositivos para las organizaciones criminales y compradores potenciales. En ese sentido, la implementación de la lista blanca tiene como propósito establecer cuáles son los dispositivos que pueden acceder a las redes a fin de garantizar que solo los equipos móviles autorizados se encuentren habilitados para utilizar la red móvil. En relación a la lista negra, esta incorpora a todos los dispositivos móviles reportados por robo o pérdida por los abonados de los concesionarios de redes móviles con la finalidad de inhabilitar el equipo móvil y, por consiguiente, disuadir el acceso a la red móvil. Por último, la adopción del registro de abonados, que tiene como objetivo asociar a cada dispositivo móvil el registro civil del abonado correspondiente; lo que genera un mayor nivel de precisión respecto a la identificación del mismo.

Cabe señalar que, en América Latina, las soluciones se han enfocan en medidas de bloqueo basadas en el IMEI.

Aunque existe un cierto grado de coordinación regional en la lucha contra el robo de equipos terminales móviles, las medidas legislativas y las regulaciones se adoptan a nivel nacional. De forma complementaria a lo mencionado, se han implementado sistemas que se basan en listas de dispositivos bloqueados (listas negras) o en dispositivos permitidos (listas blancas).

- **Listas Negras o *blacklists***

De acuerdo a TMG[54] (2018), la lista negra contiene información centralizada de equipos terminales móviles excluidos, que incluye los IMEI de los dispositivos que han sido reportados por los usuarios como sustraídos o perdidos. Los equipos incluidos en esta lista deben ser bloqueados por las empresas operadoras, con el objetivo de impedir que se haga uso de equipos móviles robados o perdidos. Mediante este mecanismo, se pretende que los equipos móviles se tornen inutilizables en la red móvil, así disminuirían su valor, lo cual a su vez reduce el incentivo de robarlos.

En tal sentido, las listas negativas suelen operar en varios niveles, dado que, tanto el usuario como la policía reportan los IMEI de equipos terminales móviles robados a los concesionaros móviles, los cuales a su vez reportan dicha información a la base de datos nacional o la comparten con todos los concesionarios móviles del país. Posteriormente, los concesionarios sincronizan sus bases de datos con la base de datos global de la GSMA. Cabe señalar que, el intercambio de datos con la base global es gratuito para los miembros de la asociación y se permite el acceso a los entes reguladores.

- **Listas Blancas o *whitelists***

La implementación de las listas positivas o blancas refleja la intención de combatir no solo el robo, sino también el comercio de equipos ilegales, falsificados y alterados, y de complementar las soluciones de listas negras. Específicamente, las listas positivas buscan superar la dificultad que implica usar listas negras para capturar equipos cuyo IMEI ha sido alterado o que de otra forma es inválido. Para que equipo sea incluido en la lista blanca y, por lo tanto, pueda conectarse a la red, debe cumplir con criterios

[54] Telecommunications Management Group

específicos como estar registrado por el importador del equipo como por los abonados finales.

Las listas positivas también ocasionan complicaciones imprevistas a los usuarios de dispositivos legítimos. Por ejemplo, la Comisión de Regulación de las Comunicaciones (CRC) de Colombia verificó que, entre otras formas de alterar los números IMEI, sus listas positivas también incluyen los duplicados de números IMEI legítimos. En atención a esta problemática, se procedió a bloquear a dos equipos con número IMEI duplicado, debido a que no existía forma de saber quién es el titular legítimo; lo que conllevo a desconectar de las redes a usuarios inocentes y legítimos cuyos IMEI han sido duplicados.

Asimismo, se han aplicado políticas complementarias como el registro de usuarios o SIM Card, que busca asociar el registro de equipos nuevos en la lista blanca al registro correspondiente del comprador en el registro civil con la finalidad de aumentar el nivel de precisión requerido para el correcto funcionamiento de la lista blanca. No obstante, cualquier error en las bases de datos de la lista blanca o del registro civil podría ocasionar una situación en que los usuarios no puedan usar sus equipos móviles. (TMG, 2018).

En efecto, la regulación del registro de la SIM Card tiene por finalidad obligar que las empresas operadoras comercialicen las líneas mediante la previa identificación de los compradores. Cabe señalar que el objetivo de identificar a las personas que han adquirido una línea móvil o están solicitando la reposición es evitar que personas inescrupulosas adquieran una SIM Card y lo usen para cometer actos ilícitos Al respecto, la GSMA (2021) ha reportado que el registro de la SIM Card es obligatorio en 157 países abril de 2021. A nivel del continente americano, no sería obligatorio en EEUU, Canadá, México, Colombia, Nicaragua y Chile.

Asimismo, la GSMA (2021) también ha identificado que existen tres modelos de implementación: (i) captura de la información personal y conservación por parte de la empresa operadora, (ii) captura de la información personal y se comparte con el regulador, y (iii) captura de la información personal y validación con alguna base de datos del gobierno. El primero modelo ha sido implementado por el 80% de los países, el segundo y tercer modelo lo tienen el 7% y 13% de países, respectivamente. A nivel del continente americano, Ecuador, Republica Dominicana y Perú han implementado el tercer modelo, mientras que el resto se encuentra en el primer modelo.

Por otra parte, se debe señalar que reglas establecidas para el registro de una SIM Card varía en cada país, pero las más comunes son: registro de los comercializadores autorizados, definición de los lugares apropiados para el registro, tipos de documentos que se requieren para la identificación, número de máximo de líneas que se pueden adquirir, etc.

En base a lo expuesto, es evidente el número creciente de gobiernos que ha implementado recientemente el registro obligatorio de usuarios de SIM Card con la esperanza de que esta política pudiera colaborar con los esfuerzos de la lucha contra crimen. Esto significa que debe registrarse un titular responsable al momento del alta de la línea, verificándose su identidad, comúnmente a través de la presentación de un documento oficial. (TMG, 2018).

- **Penalizar la adulteración del código IMEI**

Respecto al tercer pilar, de acuerdo a la Comisión Interamericana de Telecomunicaciones (en adelante, CITEL) resulta indispensable que todos los Estados miembros tipifiquen la

alteración del IMEI como un delito en sus ordenamientos jurídicos para que las autoridades competentes puedan arrestar y judicializar a los responsables. En ese contexto, además de tipificar la alteración, es necesario incluir en el tipo penal la oferta de hardware o software para alteración del IMEI, la importación, el uso, porte o venta de equipos para la alteración del IMEI y la oferta o propagación en internet de aplicaciones, manuales, tutoriales e IMEI con el objetivo de alterar los equipos terminales móviles[55].

CUADRO 10: TIPIFICACIÓN DE LA ALTERACIÓN DE IMEI COMO DELITO EN AMÉRICA LATINA

País	Ley que tipifica la alteración de IMEI como delito
Bolivia	Decreto Supremo 353, articulo 11.
Colombia	Ley 1453 de 2011, articulo 105.
Guatemala	Decreto Ley 8 de 2013, articulo 23.
México	Código Penal Federal, articulo 166.
Perú	Reglamento del Decreto Legislativo 1338 de 2017.

Fuente: CITEL (2019)

En paralelo a las medidas mencionadas, la CITEL también considera necesario actuar desde las altas instancias del gobierno y autoridades competentes, agencias de seguridad, policías, fiscales, jueces, etc., para combatir la delincuencia en las calles, la receptación de equipos terminales móviles robados, la alteración del IMEI, el contrabando de exportación e importación de equipos robados y se procure sancionar la compra, venta, posesión o uso de equipos sustraídos, alterados o clonados. En esta área de trabajo, varios hallazgos han demostrado que la acción transnacional entre las referidas autoridades es infaltable, dado que estas organizaciones criminales operan a través de las fronteras utilizando las redes sociales y otros medios digitales desarrollados por los estados. Por tal motivo, la cooperación y coordinación entre las policías y fiscalías de los estados miembros, así como su capacitación oportuna sobre el problema y su carácter técnico, es fundamental para enfrentar a la cadena transnacional de delito organizado.

- **Fabricar y configurar los equipos terminales de manera que cuenten con más mecanismos de seguridad**

Finalmente, el cuarto pilar corresponde a los fabricantes, señala la obligación de implementar equipos terminales más seguros con el objetivo de minimizar los riesgos y amenazas a los que el usuario y su equipo móvil está expuesto. Por tanto, es fundamental que los fabricantes innoven en la seguridad digital para poder combatir la comercialización ilegal de estos equipos. Cabe señalar que, este pilar es exógeno respecto a países en vías de desarrollo, dado que estos países no influyen en los cambios y/o innovaciones tecnológicas.

Al respecto, de acuerdo al reporte de la TMG (2018) se han demostrado que estos métodos tienen un impacto significativo en las tasas de robo de dispositivos a cargo de los propios fabricantes quienes han estado a la vanguardia en este campo, desarrollando y utilizando soluciones tecnológicas para reducir el robo de dispositivos, como lo demuestra el compromiso de la industria en los Estados Unidos[56], el cual fue firmado por

[55] Fuente: Nota Conceptual de la CITEL sobre el uso de equipos terminales móviles hurtados o robados, extraviados o adulterados. Disponible en: http://scm.oas.org/doc_public/SPANISH/HIST_19/CP40751S03.doc

[56] Smartphone Anti-Theft Voluntary Commitment [Compromiso Voluntario Anti Hurto] (CTIA). Disponible en: https://www.ctia.org/the-wireless-industry/industry-commitments/smartphone-anti-theft-voluntary-commitment

16 concesionario móviles, fabricantes y partes interesadas, agregando otra dimensión a los esfuerzos para combatir el robo de dispositivos a nivel mundial.

En ese sentido, la solución técnica más frecuente es una herramienta antirrobo ubicada en el dispositivo, que ha sido denominada *killswitch* o mecanismo de desactivación total. Esta solución ha demostrado ser capaz de reducir las tasas de robo. Si bien la funcionalidad específica de esta característica varía según los dispositivos, generalmente viene preinstalada o se puede descargar en los teléfonos inteligentes y le permite al usuario bloquear el teléfono remotamente, borrar su contenido o impedir el uso del mismo, haciéndolo inutilizable, y estas soluciones producen efecto inmediato. De manera similar, los usuarios también pueden reactivar fácil e instantáneamente un dispositivo recuperado sin necesidad de que intervenga la empresa operadora y sin necesidad de hacer cambios en una base de datos centralizada.

Cabe señalar que, los principales fabricantes de la industria de equipos terminales como Apple y Samsung, adoptaron tempranamente esta tecnología antirrobo en el año 2013 y 2014 respectivamente. De acuerdo a un informe de 2014 del Fiscal General del Estado de Nueva York encontró que en Londres y San Francisco el hurto de productos Apple se redujo un 24% en Londres y un 38% en San Francisco durante los seis meses siguientes a la introducción de esta tecnología del botón de desactivación total o *killswitch.* Durante ese mismo período, el robo de productos Samsung, empresa que aún no había incorporado ampliamente esta tecnología, aumentó un 3% en Londres y un 12 % en San Francisco. Durante el año siguiente a la introducción de este mecanismo de desactivación en los teléfonos inteligentes por parte de múltiples fabricantes, el hurto de teléfonos celulares se redujo un 16% en Nueva York, un 27% en San Francisco y un 38% en Londres.

No obstante, una desventaja del *killswitch* o mecanismo de desactivación y de soluciones similares es que únicamente se pueden usar en teléfonos inteligentes (smartphones), por lo que, únicamente pueden ser empleados para disuadir el hurto y/o robo de teléfonos inteligentes. Al respecto, de acuerdo a la GSMA, la tasa de adopción de teléfonos inteligentes en América Latina alcanzó el 74%, lo que representa a 500 millones de conexiones a fines de 2021[57]. De este modo, a medida que la penetración de los teléfonos inteligentes en América Latina siga aumentando, la gran mayoría de los dispositivos móviles de la región podrá incluir la tecnología antirrobo. Estas tendencias deben ser cuidadosamente consideradas por las partes interesadas para poder darle el mejor uso posible a todas las herramientas que están disponibles para disuadir el hurto y/o robo de equipos.

La segunda desventaja es que se requiere que el usuario active este servicio antes de que el dispositivo se extravíe o sea sustraído. Este enfoque es necesario porque el propietario de un dispositivo nuevo debe pasar por el proceso de registro o de alguna forma de vinculación del dispositivo al servicio antirrobo, para habilitar así a un dispositivo distinto (como un PC o el teléfono celular de un amigo) para que éste último, remotamente, pueda ubicar o deshabilitar el dispositivo extraviado o sustraído, o borrarle toda la información contenida en el equipo. Sin embargo, las organizaciones criminales no tienen manera de saber de antemano si el usuario ha seleccionado la opción del servicio antirrobo, y esto precisamente hace que todos los teléfonos inteligentes con tecnología antirrobo sean igualmente poco atractivos para los ladrones.

Por último, aunque la mayor parte del cubrimiento de prensa y de la investigación sobre las soluciones de mecanismo de desactivación o *killswitch* se refiere a los Estados Unidos

[57] Fuente: GSMA. Disponible en: | GSMA La Economía Móvil América Latina 2021 - La Economía Móvil

y el Reino Unido, la funcionalidad está disponible para todos los usuarios de teléfonos inteligentes a nivel mundial, en virtud de que es posible habilitarla mediante una aplicación que se puede descargar de Internet. En tal contexto, es necesario que los gobiernos, concesionarios móviles y entes reguladores de América Latina implementen campañas de información para poder educar a los usuarios sobre la disponibilidad de estas herramientas antirrobo.

OSIPTEL DAPU Y.RIOS

OSIPTEL DAPU L.PALACIOSS

OSIPTEL DAPU M.GONZALEZ

ANEXO N° 4: Experiencia internacional respecto a los IMEI clonados - duplicados

País/Regulador	Normativa	Agentes Responsables	Plazo para que el usuario se presente ante su operador	Información que recibe el operador para la identificación de IMEI original
Colombia/ Comisión de Regulación de Comunicaciones (CRC)	Resolución 5050 de 2016[58]	1° PRSTM[59]: (*Recibe la información del usuario y remite a la autoridad competente)* 2° Autoridad Competente *(Recibe información y determina IMEI duplicado)*	30 días	-Documento de identificación. -Información respecto de la marca y modelo correspondiente al TAC del IMEI duplicado. -Formato Anexo 2.6.[60] -Información de IMEI físico y lógico. -De ser el caso, Formato Anexo 2.8.[61]
República Dominicana/ Instituto Dominicano de Telecomunicaciones (INDOTEL)	Resolución 041-20[62]	Prestadoras de servicio móvil	5 días	-Verificación mediante procedimiento TS.06 - IMEI Allocation and Approval Process de la GSMA y la 3GPP TS 22.016. -Correspondencia entre el equipo móvil y las características técnicas y de fabricación indicadas en el TAC/IMEI de dicho equipo.
Costa Rica/ Superintendencia de Telecomunicaciones (SUTEL)	Resolución 234-2020[63]	Operador móvil	60 días[64]	-Documento de identidad. -Factura o comprobante de pago. -Contrato con el Operador, de ser el caso.

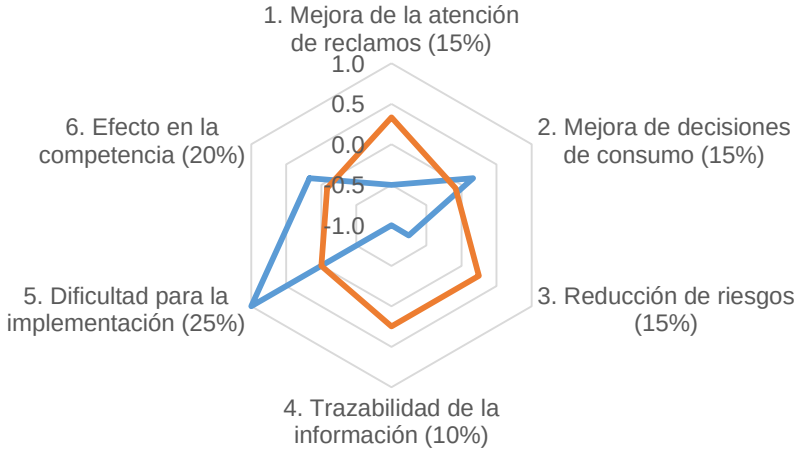
ANEXO N° 5: Análisis multicriterio

[58] Disponible: https://normograma.info/crc/docs/resolucion_crc_5050_2016.htm
[59] Proveedor de Redes y Servicios de Telecomunicaciones Móviles.
[60] Formato de Información Necesaria para la declaración de Uso de Equipo Terminal Móvil con IMEI duplicado.
[61] Formato de Constancia para la transferencia de propiedad de un equipo terminal móvil usado.
[62] Disponible: https://transparencia.indotel.gob.do/media/214136/norma-que-establece-el-mecanismo-de-control-para-detectar-prevenir-y-sancionar-la-activaci%C3%B3n-de-l%C3%A9fonos-m%C3%B3viles-que-son-objeto-de-sustracci%C3%B3n-o-extrav%C3%ADo.pdf
[63] Disponible: https://www.sutel.go.cr/sites/default/files/rcs-234-2020_disposiciones_y_aspectos_operativos_sistema_terminales_moviles.pdf
[64] Disponible: https://sutel.go.cr/noticias/comunicados-de-prensa/plataforma-impedira-utilizar-celulares-robados-o-adulterados

CUADRO N° 11: AMC DEL OBJETIVO 2 – MEJORAR LOS NIVELES DE IDONEIDAD Y AUTENTICIDAD DE LA INFORMACIÓN REPORTADA POR LAS EMPRESAS OPERADORAS EN EL REGISTRO DE ABONADO

Criterio	Peso	Escenario base	Alternativa 2
CALIFICACIÓN GLOBAL		0.02	0.08
1. Mejora de la atención de reclamos (15%)	**15%**	-0.5	0.3
2. Mejora de decisiones de consumo (15%)	**15%**	0.2	-0.1
3. Reducción de riesgos (15%)	**15%**	-0.75	0.25
4. Trazabilidad de la información (10%)	**10%**	-1.0	0.3
5. Dificultad para la implementación (25%)	**25%**	1.0	0.0
6. Efecto en la competencia (20%)	**20%**	0.2	-0.1

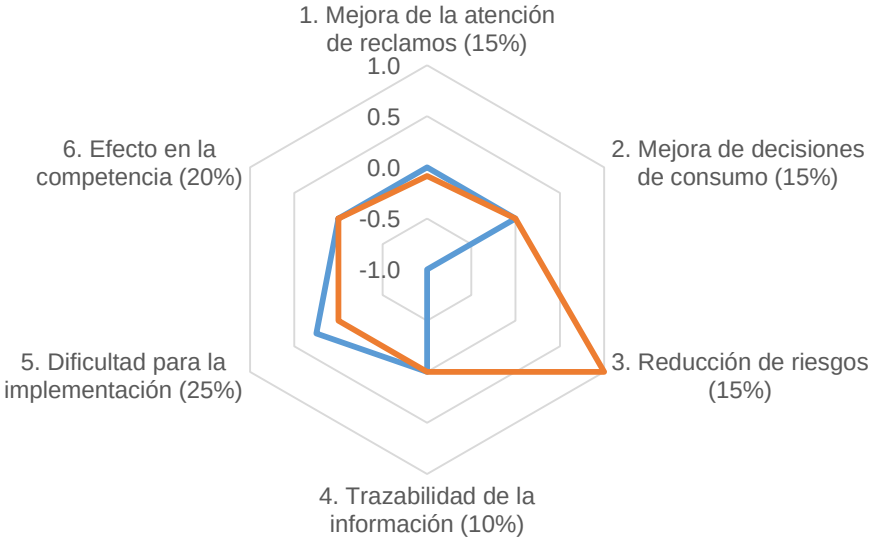
GRÁFICO N° 15: DIAGRAMA DEL OBJETIVO 2



CUADRO N° 12: AMC DEL OBJETIVO 3 – FACILITAR LA ENTREGA DE LA CONTRASEÑA ÚNICA A TRAVÉS DE UN PROCESO SEGURO Y CONFIABLE

Criterio	Peso	Escenario base	Alternativa 2
CALIFICACIÓN GLOBAL		**-0.09**	**0.14**
1. Mejora de la atención de reclamos (15%)	**15%**	0.0	-0.1
2. Mejora de decisiones de consumo (15%)	**15%**	0.0	0.0
3. Reducción de riesgos (15%)	**15%**	-1	1
4. Trazabilidad de la información (10%)	**10%**	0.0	0.0
5. Dificultad para la implementación (25%)	**25%**	0.3	0.0
6. Efecto en la competencia (20%)	**20%**	0.0	0.0

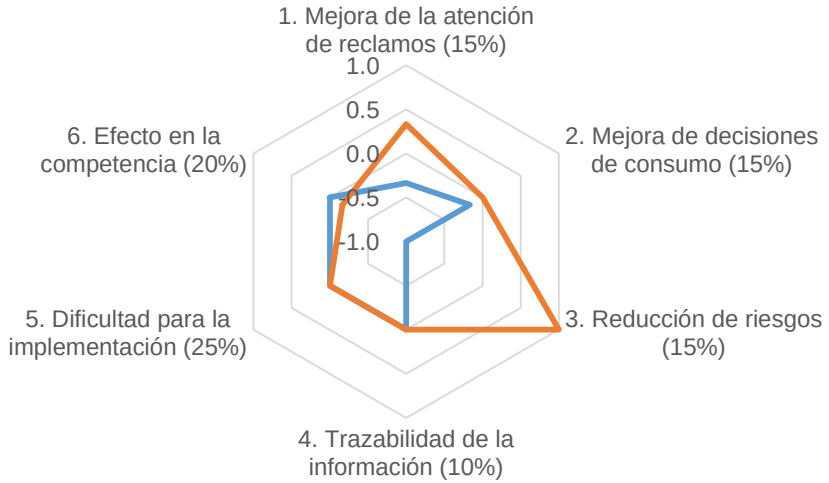
GRÁFICO N° 16: DIAGRAMA DEL OBJETIVO 3



CUADRO N° 13: AMC DEL OBJETIVO 4 – REDUCIR LOS ESCENARIOS EN LOS QUE LA DELINCUENCIA PUEDE UTILIZAR UNA LINEA PREPAGO CONTRATADA A NOMBRE DE OTRA PERSONA

Criterio	Peso	Escenario base	Alternativa 2
CALIFICACIÓN GLOBAL		-0.23	0.17
1. Mejora de la atención de reclamos (15%)	**15%**	-0.3	0.3
2. Mejora de decisiones de consumo (15%)	**15%**	-0.2	0.0
3. Reducción de riesgos (15%)	**15%**	-1	1
4. Trazabilidad de la información (10%)	**10%**	0.0	0.0
5. Dificultad para la implementación (25%)	**25%**	0.0	0.0
6. Efecto en la competencia (20%)	**20%**	0.0	-0.2

GRÁFICO N° 17: DIAGRAMA DEL OBJETIVO 4



ANEXO N° 6: Evaluación de la robustez del Análisis Multicriterio (AMC)

1. Planteamiento

Para sustentar la robustez de los resultados expuestos en el Análisis Multicriterio (AMC) se ha empleado la técnica de la simulación de Monte Carlo. Esta técnica simula una variable objetivo (valor final del AMC) en función a determinadas variables de entrada (calificaciones de los criterios) la cual se expresa mediante un modelo matemático. Así, el modelo matemático puede ser descrito de la siguiente manera:

$$Valor\ AMC_i = \sum p_i \times A_i$$

Donde A_i corresponde al valor de la calificación de cada aspecto analizado y p_i indica el peso correspondiente a cada uno de estos aspectos. Además, el valor de cada aspecto es igual al promedio simple de las calificaciones de cada uno de sus criterios C_i de tal manera que $A_i = \frac{\sum C_i}{n}$, donde n indica el número de criterios dentro de cada aspecto analizado.

Para la determinación de los resultados se simularon 10 000 escenarios alternativos posibles. Vale decir que los resultados son más o menos robustos en la medida que, ante los diversos valores posible que puedan tomar las calificaciones, los resultados no varíen significativamente respecto al valor esperado de la calificación final del AMC.

Para el modelo se asume que las calificaciones tienen una distribución triangular[65]. Los parámetros de las calificaciones para el modelo son las siguientes:

CALIFICACIONES DE LOS PARÁMETROS DE LA SIMULACION DEL OBJETIVO 3

CALIFICACIÓN GLOBAL	Moda	Mínimo	Máximo
1. Mejora de la atención de reclamos (15%)			
· Mejora la capacidad de presentar reclamos	-0.25	-0.40	0.00
· Reduce la probabilidad de ocurrencia de problemas	0	-0.05	0.05
· Mejora la capacidad de verificar incumplimientos	0	-0.05	0.05
2. Mejora de decisiones de consumo (15%)			
· Mejora el conocimiento de la información tarifaria	0.0	-0.1	0.1
· Facilita el cambio de operador	0.0	-0.1	0.1
· Limita la contratación de servicios	0.0	-0.1	0.1
3. Reducción de riesgos (15%)			
· Incidencia de delitos y riesgos	1	0.9	1
· Contrataciones seguras	1	0.9	1
4. Trazabilidad de la información (10%)			
· Identificación posterior del solicitante	0.0	0.0	0.1
· Trazabilidad del proceso	0.0	0.0	0.0
· Oportunidad de la información	0.0	0.0	0.1
5. Dificultad para la implementación (25%)			
· Niveles de inversión	0.0	-0.1	0.0
· Incidencia de escenario de difícil implementación	0.0	-0.1	0.1
6. Efecto en la competencia (20%)			
· Retención de clientes	0.0	-0.1	0.1
· Limitaciones para captar clientes	0.0	-0.1	0.1
· Diferenciación entre empresas operadoras	0.0	-0.1	0.1

CALIFICACIONES DE LOS PARÁMETROS DE LA SIMULACION DEL OBJETIVO 4

[65] Se emplea esta distribución dado que resulta sencilla al solamente depender de tres parámetros: i) valor mínimo, ii) valor máximo; y iii) moda. Se recomienda emplear en situaciones donde no se conoce la distribución específica de una variable ya que penaliza de mayor manera las colas de la distribución.

CALIFICACIÓN GLOBAL	Moda	Mínimo	Máximo
1. Mejora de la atención de reclamos (15%)	**0.3**		
· Mejora la capacidad de presentar reclamos	0.00	0.00	0.00
· Reduce la probabilidad de ocurrencia de problemas	1	0.95	1
· Mejora la capacidad de verificar incumplimientos	0	0	0
2. Mejora de decisiones de consumo (15%)	**0.0**		
· Mejora el conocimiento de la información tarifaria	0.0	0.0	0.0
· Facilita el cambio de operador	0.0	0.0	0.0
· Limita la contratación de servicios	0.0	0.0	0.0
3. Reducción de riesgos (15%)	**1**		
· Incidencia de delitos y riesgos	1	0.9	1
· Contrataciones seguras	1	0.9	1
4. Trazabilidad de la información (10%)	**0.0**		
· Identificación posterior del solicitante	0.0	0.0	0.0
· Trazabilidad del proceso	0.0	0.0	0.0
· Oportunidad de la información	0.0	0.0	0.0
5. Dificultad para la implementación (25%)	**0.0**		
· Niveles de inversión	0.0	0.0	0.0
· Incidencia de escenario de difícil implementación	0.0	0.0	0.0
6. Efecto en la competencia (20%)	**-0.2**		
· Retención de clientes	-0.5	-0.6	-0.4
· Limitaciones para captar clientes	0.0	0.0	0.0
· Diferenciación entre empresas operadoras	0.0	0.0	0.0

CALIFICACIONES DE LOS PARÁMETROS DE LA SIMULACION DEL OBJETIVO 5

CALIFICACIÓN GLOBAL	Moda	Mínimo	Máximo
1. Mejora de la atención de reclamos (15%)	**0.7**		
· Mejora la capacidad de presentar reclamos	0.50	0.40	0.60
· Reduce la probabilidad de ocurrencia de problemas	0.5	0.4	0.6
· Mejora la capacidad de verificar incumplimientos	1	0.85	1
2. Mejora de decisiones de consumo (15%)	**0.3**		
· Mejora el conocimiento de la información tarifaria	1.0	0.8	1.0
· Facilita el cambio de operador	0.0	0.0	0.0
· Limita la contratación de servicios	0.0	0.0	0.0
3. Reducción de riesgos (15%)	**0**		
· Incidencia de delitos y riesgos	0	0	0
· Contrataciones seguras	0	0	0
4. Trazabilidad de la información (10%)	**0.3**		
· Identificación posterior del solicitante	0.0	0.0	0.0
· Trazabilidad del proceso	0.0	0.0	0.0
· Oportunidad de la información	1.0	0.9	1.0
5. Dificultad para la implementación (25%)	**-0.5**		
· Niveles de inversión	-0.5	-0.6	-0.4
· Incidencia de escenario de difícil implementación	-0.5	-0.6	-0.4
6. Efecto en la competencia (20%)	**-0.1**		
· Retención de clientes	-0.3	-0.4	-0.1
· Limitaciones para captar clientes	0.0	0.0	0.0
· Diferenciación entre empresas operadoras	0.0	0.0	0.0

2. Resultados

2.1 Objetivo 3.- Como puede observarse en el gráfico final, la estimación del modelo permite determinar que la media de la calificación final del AMC coincide con el valor estimado para la misma.

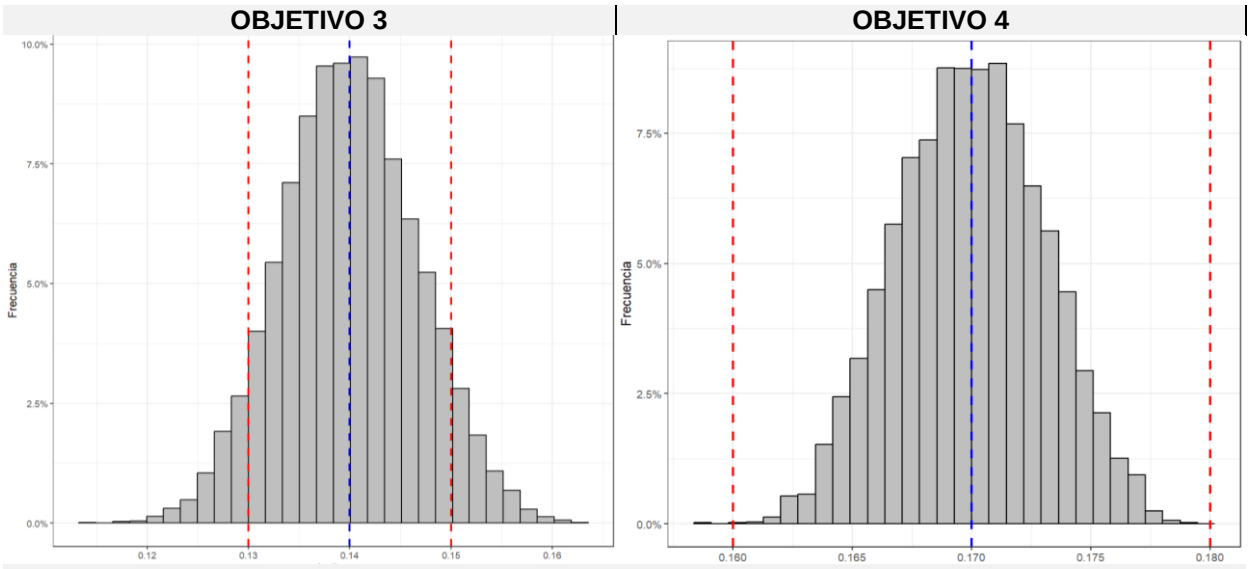
Por otra parte, tomando umbrales en valores circundantes (+/- 0.01) se observa que la probabilidad que el valor real se encuentre dentro de estos umbrales resulta ser bastante

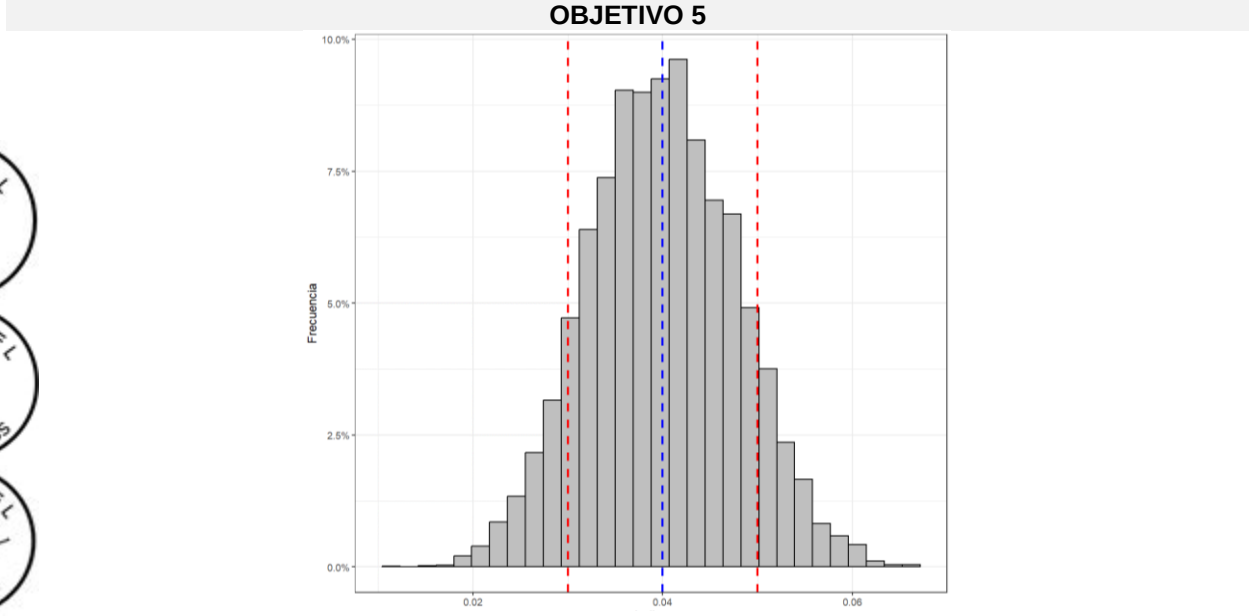
alta ya que llega al 86.21%, es decir, en más del 85% de los 10 000 escenarios evaluados la variable de salida genera un resultado consistente.

2.2 Objetivo 4.- De manera similar al caso anterior, en función a las simulaciones planteadas, el modelo arroja que, en el intervalo (+/- 0.01), la probabilidad que los valores de salida simulados se encuentren localizados dentro del área limitada por los umbrales es del 99.98%.

2.3 Objetivo 5.-Finalmente, respecto al objetivo 5, el valor obtenido para el AMC es de 0.04, por lo cual tomamos umbrales (+/- 0.01) alrededor de este valor para analizar los escenarios. Así, alrededor del 80.37% de las 10 000 simulaciones se encuentra dentro del rango planteado.

DISTRIBUCIÓN DE LAS CALIFICACIONES FINALES DEL AMC





Como se pudo apreciar, los valores de las calificaciones finales del AMC obtenidos de la simulación no difieren en más de 0.01 respecto a sus valores esperados, inclusive llegando a superar el 99% en algunos casos. Por ello podemos considerar que los resultados son consistentes y robustos con las simulaciones planteadas.