Firmado digitalmente por PICCINI ANTON Tatiana Mercedes FAU 20216072155 soft
Cargo: Directora De Atencion Y Proteccion Del Usuario
Motivo: Soy el autor del documento
Fecha: 07.04.2026 06:47:59 -05:00

San Borja, 07 de Abril del 2026

INFORME N° 000033-2026-DAPU/OSIPTEL

A	:	JOHNNY ANALBERTO MARCHAN PEÑA GERENTE GENERAL
CC	:	MILAGROS JUDITH VARGAS FIERRO OFICINA DE COMUNICACIONES Y RELACIONES INSTITUCIONALES
ASUNTO	:	ATENCIÓN A LAS CONSULTAS FORMULADAS POR EL CONGRESISTA DE LA REPÚBLICA MARÍA ANTONIETA AGÜERO GUTIÉRREZ RELACIONADAS A MECANISMOS NORMATIVOS, REGULATORIOS, TÉCNICOS E INSTITUCIONALES PARA LA PREVENCIÓN, ATENCIÓN, BLOQUEO, TRAZABILIDAD Y PERSECUCIÓN DE ESTAFAS TELEFÓNICAS Y DELITOS INFORMÁTICOS COMETIDOS MEDIANTE LÍNEAS MÓVILES, EQUIPOS TERMINALES Y APLICACIONES MÓVILES
REFERENCIA	:	OFICIO N° 758-2025-2026-MAG-CR

	CARGO	**NOMBRE**
ELABORADO POR	**ESPECIALISTA LEGAL**	EVELYN LEO OLORTEGUI CRUZADO
	COORDINADOR DE LA UNIDAD FUNCIONAL DEL RENTESEG	LUIS MIGUEL CÉSAR TAMO
REVISADO POR	**COORDINADOR LEGAL**	MATILDE GONZALEZ VILLANUEVA
	SUBDIRECTOR DE PROTECCIÓN DEL USUARIO	HAYINE GUSUKUMA LOZANO
APROBADO POR	**DIRECTORA DE ATENCIÓN Y PROTECCIÓN DEL USUARIO**	TATIANA MERCEDES PICCINI ANTÓN
	DIRECTOR DE FISCALIZACIÓN E INSTRUCCIÓN	LUIS ALEJANDRO PACHECO ZEVALLOS

Firmado digitalmente por PACHECO ZEVALLOS Luis Alejandro FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 06.04.2026 23:51:13 -05:00

Firmado digitalmente por CESAR TAMO Luis Miguel FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 06.04.2026 17:04:21 -05:00

Firmado digitalmente por GUSUKUMA LOZANO Hayine Juana FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 06.04.2026 16:25:02 -05:00

Firmado digitalmente por GONZALEZ VILLANUEVA Matilde Judith FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 06.04.2026 16:04:59 -05:00

Firmado digitalmente por OLORTEGUI CRUZADO Evelyn Leo FAU 20216072155 soft
Motivo: Doy V° B°
Fecha: 06.04.2026 16:01:23 -05:00

I. OBJETIVO

El presente informe tiene por objetivo atender el Oficio N° 758-2025-2026-MAG-CR[1] remitido por la Congresista María Antonieta Agüero Gutiérrez, quien solicita información documentada, técnica y normativa relacionada con los mecanismos de prevención, supervisión, bloqueo, trazabilidad y persecución de estafas telefónicas y delitos informáticos cometidos mediante líneas móviles, equipos terminales, servicios públicos móviles y aplicaciones maliciosas.

II. ANTECEDENTES

2.1. Mediante Oficio N° 758-2025-2026-MAG-CR, la Congresista solicita información técnica y normativa del OSIPTEL respecto a la prevención, supervisión, reporte, suspensión y bloqueo de líneas móviles y equipos terminales vinculados a estafas telefónicas, fraude informático, suplantación de identidad digital y distribución de aplicaciones maliciosas.

2.2. El requerimiento se enmarca en la elaboración de propuestas legislativas destinadas a fortalecer la capacidad del Estado para enfrentar delitos informáticos cometidos mediante servicios móviles.

2.3. El oficio incluye 12 consultas específicas que comprenden: marco normativo, competencias institucionales, mecanismos operativos, coordinación interinstitucional, estadísticas y propuestas legislativas.

III. MARCO NORMATIVO

- Reglamento General del Organismo Supervisor de la Inversión Privada en Telecomunicaciones – OSIPTEL, aprobado mediante el Decreto Supremo N.º 008-2001-PCM.
- Ley N.º 27336[2], Ley de Desarrollo de las Funciones y Facultades del OSIPTEL.
- Decreto Legislativo N° 1338 a través del cual se creó el Registro Nacional de Equipos Terminales Móviles para la Seguridad (en adelante, RENTESEG), orientado a la prevención y combate del comercio ilegal de equipos terminales móviles y al fortalecimiento de la seguridad ciudadana, y modificatorias.
- Decreto Supremo N° 007-2019-IN, mediante el cual se aprobó el Reglamento del Decreto Legislativo N.º 1338, y modificatorias (en adelante, Reglamento del RENTESEG).
- Resolución de Consejo Directivo N.º 007-2020-CD/OSIPTEL, que aprobó las Normas Complementarias para la Implementación del RENTESEG, y modificatorias (en adelante, Normas Complementarias del RENTESEG).
- Decreto Supremo N.º 124-2025-PCM, Decreto Supremo que declara el Estado de Emergencia en Lima Metropolitana del departamento de Lima y en la Provincia Constitucional del Callao; modificada por el Decreto Supremo N.º 127-2025-PCM.
- Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado por la Resolución de Consejo Directivo N.º 172-2022-CD/OSIPTEL y sus modificatorias (en adelante, la Normas de las Condiciones de Uso).

[1] Recibido el 19.03.2026 y con Registro de Mesa de Partes Virtual N° 0008459-2026.
[2] Publicada en el diario oficial El Peruano con fecha 27.07.2000.

- Resolución de Consejo Directivo N.º 070-2025-CD/OSIPTEL que establece la Norma que establece el Procedimiento de Baja de los Servicios Públicos Móviles en el marco de la validación de información del registro de abonados y del vendedor o persona natural que intervenga directamente en la contratación de los servicios públicos de telecomunicaciones
- Ley N.º 31839 que modifica el Decreto Legislativo 1338, Decreto Legislativo que crea el Registro Nacional de Equipos Terminales Móviles para la Seguridad, y la Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, para prohibir y sancionar la comercialización y contratación de los servicios públicos móviles de telecomunicaciones de forma ambulatoria o en la vía pública y sin contar con la verificación biométrica.
- Ley N.º 32323, Ley que modifica la Ley N.º 29571, amplió la prohibición de las comunicaciones SPAM e introdujo el artículo 58.3, en el cual se señaló que el Estado establecerá las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones
- Ley N.º 32451 que modifica la Ley 30096, Ley de Delitos Informáticos, y el Código Penal – Decreto Legislativo 635, respecto a la activación ilegal de líneas de servicios móviles y a la posesión ilegal de SIM Card.
- Decreto Legislativo N.º 1723[3], Decreto Legislativo que establece reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

IV. ANÁLISIS

4.1 Respecto del marco normativo vigente, dentro del ámbito de competencia del OSIPTEL, aplicable a la prevención, supervisión, reporte, suspensión, baja, bloqueo o trazabilidad de líneas móviles y equipos terminales vinculadas a: estafas telefónicas, fraude informático, suplantación de identidad digital, captación indebida de datos y distribución de archivos o aplicaciones maliciosas mediante servicios públicos móviles.

Sobre el particular, debemos precisar que, el artículo 20° del Reglamento General del Organismo Supervisor de la Inversión Privada en Telecomunicaciones – OSIPTEL, aprobado mediante el Decreto Supremo N.º 008-2001-PCM, establece que el OSIPTEL ejerce sus funciones sobre aquellas actividades que involucran la prestación de los servicios públicos de telecomunicaciones.

En ese sentido, en el marco de las funciones otorgadas al OSIPTEL mediante Ley N.º 27336[4], Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, se colige que este Organismo no tiene competencia para emitir normas relacionadas con la comisión de delitos y el tratamiento de datos personales, siendo que el organismo competente para la persecución del delito es el Ministerio Público, mientras que la Autoridad Nacional de Protección de Datos Personales, se encarga del cumplimiento de lo dispuesto en la Ley N.º 29733.

Sin perjuicio de ello, debemos precisar lo siguiente:

4.1.1 Con relación a las estafas telefónicas, captación de datos y distribución de archivos o aplicaciones maliciosas mediante servicios públicos móviles.

[3] Publicado en el diario oficial El Peruano con fecha 7.02.2026.
[4] Publicada en el diario oficial El Peruano con fecha 27.07.2000.

Sobre el particular, con relación al uso de las llamadas telefónicas para promover productos y servicios sin consentimiento del usuario, pueden calificarse como métodos comerciales agresivos y engañosos según lo dispuesto en el literal e) del artículo 58 de la Ley N.º 29571, Código de Protección y Defensa del Consumidor[5] (en adelante, Código de Protección y Defensa del Consumidor).

En concordancia con ello, la Ley N.º 32323, Ley que modifica la Ley N.º 29571, amplió la prohibición de las comunicaciones SPAM e introdujo el artículo 58.3, en el cual se señaló que el Estado establecerá las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones.

Además, la Única Disposición Complementaria Final de dicha Ley dispuso que el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas SPAM que reciban, así como los mecanismos de validación de la información transmitida.

En ese marco, se aprobó el Decreto Legislativo N.º 1723[6], Decreto Legislativo que establece reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad, a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones. Dicho Decreto Legislativo tiene como finalidad establecer medidas para la identificación y trazabilidad de las llamadas y envíos de mensajes de texto ilícitas en perjuicio de los usuarios.

En la referida normativa se establecieron obligaciones tanto a las empresas operadoras de los servicios públicos de telecomunicaciones como a los agentes vinculados en la trazabilidad de las llamadas y mensajes de texto. Aunado a ello, dichas empresas facilitarán el acceso y monitoreo constante de las llamadas y/o envío de mensajes de texto al Ministerio de Transportes y Comunicaciones.

También, se establece que la potestad de fiscalizar y sancionar a las empresas operadoras y agentes vinculados a trazabilidad de llamadas y/o mensajes de

[5] **Artículo 58.- Definiciones y alcances**
58.1. El derecho de todo consumidor a la protección contra los métodos comerciales agresivos o engañosos implica que los proveedores no pueden llevar a cabo prácticas que mermen de forma significativa la libertad de elección del consumidor a través de figuras como el acoso, la coacción, la influencia indebida o el dolo. En tal sentido, están prohibidas todas aquellas prácticas comerciales que importen:
(…)
e. Emplear centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo a consumidor alguno, con la única excepción del envío de comunicación comercial o publicitaria a aquel consumidor que, por iniciativa propia, se contacte directamente con el proveedor y manifieste su consentimiento libre, previo, informado, expreso e inequívoco de ser contactado a través de un número telefónico, dirección electrónica o cualquier otro medio análogo de comunicación. Este consentimiento puede ser revocado, con efecto inmediato y sin expresión de causa, en cualquier momento y conforme a la normativa que rige la protección de datos personales. La vulneración a esta prohibición o a su revocatoria es considerada infracción muy grave.
(…)
58.3. Para garantizar la protección del consumidor contra los métodos comerciales agresivos y engañosos, el Estado establece reglas para el adecuado uso e envío de mensajes y llamadas en las redes de telecomunicaciones.

[6] Publicado en el diario oficial El Peruano con fecha 7.02.2026.

texto por el incumplimiento de las obligaciones establecidas en dicho Decreto Legislativo, es competencia del Ministerio de Transportes y Comunicaciones.

4.1.2 Con relación al fraude informático y/o suplantación de identidad.

El 30 de septiembre de 2025 se publicó en el diario oficial El Peruano la Ley N.º 32451, mediante la cual se modifica la Ley N.º 30096, Ley de Delitos Informáticos, y el Código Penal (Decreto Legislativo N.º 635), con el objetivo de sancionar penalmente la activación ilegal de líneas móviles y la posesión ilegítima de SIM cards. Esta norma se enmarca en el esfuerzo del Estado por combatir el fraude en telecomunicaciones y fortalecer la seguridad ciudadana, en coordinación con el Ministerio Público, la Policía Nacional del Perú y el OSIPTEL.

En primer lugar, se incorpora el artículo 9-A a la Ley N.º 30096, estableciendo que quien active una SIM card o línea móvil sin el consentimiento del titular, ya sea mediante sistemas informáticos o cualquier otro mecanismo, será sancionado con pena privativa de libertad no menor de cuatro ni mayor de ocho años, además de inhabilitación conforme al artículo 36 del Código Penal. Esta disposición busca frenar la suplantación de identidad y el uso fraudulento de datos personales en la contratación de servicios móviles.

Asimismo, se modifica el artículo 222-B del Código Penal para sancionar la posesión ilegítima de SIM cards activadas ilegalmente. La norma distingue entre dos conductas: por un lado, quien provea, comercialice o facilite la adquisición de SIM cards activadas ilegalmente será sancionado con pena privativa de libertad de cinco a nueve años; por otro lado, quien las adquiera o posea será sancionado con pena de cuatro a ocho años. Esta diferenciación permite perseguir tanto a los proveedores como a los usuarios que participan en el circuito ilegal de comercialización de líneas móviles.

Por otro lado, la Ley N.º 32451 modifica el literal f) del artículo 16 de la Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, obligando a las entidades supervisadas a proporcionar al OSIPTEL, mediante herramientas informáticas, toda la información del proceso de comercialización, contratación y activación de servicios móviles, incluyendo la identificación del personal que interviene. Esta información deberá ser entregada al Ministerio Público, la Policía Nacional del Perú y otras entidades competentes, lo que fortalece la trazabilidad y fiscalización de las operaciones comerciales en el sector.

4.1.3 Con relación suspensión y/o baja de servicios públicos móviles y/o bloqueo de equipos terminales móviles en el marco de la comisión de delitos

En el marco de lo dispuesto en el numeral 6.4 del artículo 6 del Decreto Supremo N.º 124-2025-PCM y sus modificatorias[7], así como a través del Decreto Supremo N.º 027-2026-PCM que declaró el Estado de Emergencia en Lima Metropolitana del departamento de Lima y en la Provincia Constitucional del Callao[8], se facultó a la PNP a requerir al OSIPTEL que disponga que las empresas operadoras suspendan de manera inmediata las líneas móviles que se venden previamente activados, así como las vinculadas a casos de

[7] Modificado mediante Decreto Supremo Nros. 127-2025-PCM cuya vigencia fue ampliada a través de Decreto Supremo Nros. 132-2025-PCM, 140-2025-PCM y 006-2026-PCM.
[8] Cuya vigencia fue ampliada mediante Decreto Supremo Nro. 044-2026-PCM.

extorsión, secuestro, sicariato, entre otros delitos, cuya cancelación se realiza conforme a la ley de la materia.

Asimismo, de forma similar se declaró el Estado de Emergencia en:

- Las provincias de Trujillo y Virú del departamento de La Libertad (Decreto Supremo N°(s) 130-2025-PCM, 008-2026-PCM y 041-2026-PCM).
- Las provincias de Tumbes y Zarumilla del departamento de Tumbes (Decreto Supremo N°(s) 131-2025-PCM y 007-2026-PCM).
- Los distritos de Palca, Tacna y La Yarada - Los Palos de la provincia de Tacna del departamento de Tacna (Decreto Supremo N°(s) 135-2025-PCM y 013-2026-PCM).
- Los distritos de Tambopata, Inambari, Las Piedras y Laberinto de la provincia de Tambopata y en los distritos de Madre de Dios y Huepetuhe de la provincia de Manu del departamento de Madre de Dios (Decreto Supremo N°(s) 136-2025-PCMy 017-2026-PCM).
- Los distritos de Piura, Castilla, Veintiséis de Octubre y Catacaos de la provincia de Piura, en los distritos de Sullana y Bellavista de la provincia de Sullana, en la provincia de Paita y en la provincia de Talara del departamento de Piura (Decreto Supremo N°(s) 146-2025-PCM y 030-2026-PCM).
- La provincia de Pisco del departamento de Ica (Decreto Supremo N.º 004-2026-PCM y 038-2026-PCM).

De otro lado, el literal d) del numeral 6.1 del artículo 6 del Decreto Legislativo N.º 1338 establece que el OSIPTEL tiene como atribución, entre otros, requerir a las empresas operadoras de servicios públicos móviles de telecomunicaciones, de oficio o a solicitud del Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, el Ministerio Público o el Poder Judicial el bloqueo del IMEI de los equipos terminales móviles y/o la baja del servicio público móvil, de acuerdo al reporte de los equipos terminales móviles utilizados o vinculados para la comisión de delitos, según el procedimiento establecido para tal fin.

Asimismo, de acuerdo con el dispositivo antes señalado, corresponde al OSIPTEL requerir a las empresas operadoras, a solicitud expresa del usuario afectado, cuya circunstancia se encuentre acreditada con la respectiva denuncia y constatación policial, el bloqueo del IMEI o la suspensión temporal del servicio público móvil vinculados a la comisión de delitos.

En línea con ello, mediante el Decreto Supremo N.º 018-2025-IN, el Ministerio del Interior aprobó el Lineamiento para la baja o suspensión temporal de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles que hayan sido utilizados o vinculados en la comisión de delitos. El punto 3 del numeral 5.1. del mencionado Lineamiento, establece que los reportes de baja y/o bloqueo de equipos terminales móviles que hayan sido utilizados o vinculados en la comisión de delitos deben ser remitidos a través de un sistema de transmisión de información, implementado por el OSIPTEL.

Asimismo, de acuerdo con la Primera Disposición Complementaria Transitoria del Decreto Supremo N.º 018-2025-IN, hasta la implementación del sistema de transmisión de información a cargo del OSIPTEL, los funcionarios responsables de las entidades competentes son acreditados ante el OSIPTEL y remiten sus reportes a través del correo electrónico que comunique este Organismo.

4.2 Sobre las competencias específicas de OSIPTEL respecto de:

- **El requerimiento de bloqueo o baja de líneas móviles.**
- **El bloqueo de equipos terminales móviles por IMEI.**
- **La supervisión de obligaciones de las empresas operadoras frente a fraude o uso ilícito de líneas móviles.**
- **La articulación con otras entidades del Estado para fines de seguridad ciudadana e investigación de delitos.**

De acuerdo con el Decreto Legislativo N.º 1338, el OSIPTEL se encuentra encargado de administrar el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG), a través del cual se ordena el bloqueo de los equipos terminales móviles y la suspensión de las líneas móviles, en virtud de reportes de sustracción o pérdida del mismo efectuados por los abonados y usuarios.

Por otro lado, conforme con lo dispuesto en el literal d) del artículo 6 del Decreto Legislativo N.º 1338, el OSIPTEL articula con otras entidades del Estado para fines de seguridad ciudadana e investigación del delito, tal es así que, el Regulador puede requerir a las empresas operadoras de servicios públicos de telecomunicaciones, de oficio o a solicitud del Ministerio del Interior, de la Policía Nacional del Perú, del Instituto Nacional Penitenciario, del Ministerio Público o del Poder Judicial, el bloqueo del IMEI de los equipos terminales móviles detectados como alterados, duplicados, clonados, inválidos, que no se encuentren en la Lista Blanca del RENTESEG; y/o la baja del servicio público móvil, de acuerdo al reporte de los equipos terminales móviles utilizados o vinculados a la comisión de delitos.

Asimismo, de acuerdo con el dispositivo citado, corresponde al OSIPTEL requerir a las empresas operadoras, a solicitud expresa del usuario afectado -cuya circunstancia se encuentre acreditada con la respectiva denuncia y constatación policial-, el bloqueo del IMEI o la suspensión temporal del servicio público móvil vinculados a la comisión de delitos.

Cabe indicar que, en el marco de lo dispuesto en el literal d) del artículo 6 del Decreto Legislativo N.º 1338, el OSIPTEL supervisa a las empresas operadoras del servicio público móvil, respecto de la obligación de ejecutar la suspensión o baja del servicio público móvil y/o el bloqueo del IMEI de los equipos terminales.

Por último, de acuerdo con el inciso f) del artículo 6 del Decreto Legislativo N.º 1338, el OSIPTEL puede requerir a las empresas operadoras la baja de los servicios públicos móviles que no cumplan con los requisitos de validez establecidos por el Regulador. Estos requisitos de validez se encuentran establecidos en el artículo 18-A[9] de la Norma de las Condiciones de Uso de los Servicios Públicos de

[9] "Artículo 18-A.- Requisitos esenciales para la contratación de los servicios públicos móviles

Para el caso específico del servicio público móvil, son requisitos esenciales para su contratación:

1. Realizar la contratación y adquisición de SIM card en: (i) centros de atención, (ii) la dirección específica del punto de venta previamente reportado al OSIPTEL, (iii) el canal telefónico, (iv) forma virtual, (v) la dirección indicada por el solicitante del servicio (modalidad delivery), o (vi) excepcionalmente ferias itinerantes; aplicando las disposiciones establecidas en el numeral 2.8 del Anexo 5.

2. Validar la identidad de la persona natural, nacional o extranjera, que interviene en la contratación por parte de la empresa operadora, únicamente a través de la identificación biométrica, conforme a la normativa vigente, previo a la validación de la identidad del solicitante en cada contratación, salvo en las contrataciones realizadas a través del mecanismo de contratación por auto-activación.

Telecomunicaciones, aprobada por Resolución N.º 172-2022-CD/OSIPTEL y modificatorias.

4.3 Sobre la existencia de procedimientos, protocolos, lineamientos o mecanismos operativos que permitan a OSIPTEL, por iniciativa propia o a solicitud de otra autoridad competente, requerir a las empresas operadoras:

- **La suspensión temporal de líneas;**
- **La baja del servicio móvil;**
- **El bloqueo de equipos terminales;**
- **El envío de mensajes de advertencia a abonados o usuarios;**
- **La preservación de información técnica o evidencia digital asociada a líneas o equipos presuntamente vinculados a hechos delictivos.**

El OSIPTEL se encuentra facultado, tanto por iniciativa propia como a solicitud de otras autoridades competentes, para requerir a las empresas operadoras la suspensión temporal de líneas, la baja del servicio móvil, el bloqueo de equipos terminales, el envío de mensajes de advertencia a abonados o usuarios.

En virtud de ello, se han establecido procedimientos específicos:

Suspensión y baja del servicio móvil

- Mediante la **Resolución N.º 070-2025-CD/OSIPTEL**, se aprobó el procedimiento de baja de los servicios públicos móviles por registro inconsistente, cuando los datos del abonado, vendedor o persona natural que interviene en la contratación no coinciden con la información consignada en las bases de datos del RENIEC o de la Superintendencia Nacional de Migraciones.

- Asimismo, mediante la **Resolución N.º 134-2025-CD/OSIPTEL,** se aprobó la norma que establece el procedimiento de baja de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles utilizados o vinculados a la comisión de delitos. Dicho procedimiento se encuentra vigente y contempla un canal alternativo para la recepción temporal de solicitudes de las entidades competentes, hasta la implementación de un sistema de transmisión de información.

Bloqueo de equipos terminales y mensajes de advertencia

A través de las **Normas Complementarias del RENTESEG,** se establece la obligación de las empresas operadoras de realizar la validación diaria de los equipos terminales móviles vinculados a líneas en servicio, a fin de determinar si corresponde mantener habilitado el servicio en el IMEI del equipo.

En caso corresponda, el concesionario móvil debe enviar mensajes de advertencia a los abonados o usuarios en un plazo máximo de dos (2) días hábiles desde la recepción de la instrucción del RENTESEG. Posteriormente, el bloqueo del equipo

3. Validar la identidad del solicitante del servicio, a través de la identificación biométrica, para cada contratación, conforme a la normativa vigente; o mediante el procedimiento establecido en el numeral 3.4 del Anexo 5, cuando corresponda.

El contrato de los servicios públicos móviles se perfecciona con el cumplimiento de todos los requisitos esenciales."

terminal móvil debe efectuarse también en un plazo máximo de dos (2) días hábiles contados desde el envío del SMS.

Proyecto normativo para suspensión temporal y bloqueo por usuario afectado

- El OSIPTEL ha elaborado un proyecto de norma que establece reglas operativas para que las empresas operadoras y el OSIPTEL atiendan de manera célere las solicitudes de suspensión temporal de servicios móviles y/o bloqueo de equipos terminales trasladadas por el OSIPTEL a solicitud expresa del usuario afectado.

- En esa línea, mediante la **Resolución de Consejo Directivo N.º 036-2026-CD/OSIPTEL,** publicada en el diario oficial *El Peruano*, se sometió a consulta pública el proyecto de modificación de la norma aprobada por la Resolución N.º 134-2025-CD/OSIPTEL, a efectos de recibir comentarios y sugerencias de los interesados.

4.4 Sobre el marco legal vigente que habilita o limita a OSIPTEL para intervenir frente a supuestos en los que una línea móvil o equipo terminal sea utilizado para difundir: mensajes fraudulentos masivos; enlaces maliciosos; archivos sospechosos (.APK u otras extensiones); mecanismos de suplantación de entidades financieras, empresas operadoras o entidades públicas y aplicaciones móviles vinculadas a fraude o captación ilícita de información.

Sobre el particular, el marco normativo vigente no atribuye competencia específica al OSIPTEL sobre los supuestos en los que una línea móvil o equipo terminal sea utilizado para difundir mensajes fraudulentos masivos; enlaces maliciosos; archivos sospechosos (.APK u otras extensiones); mecanismos de suplantación de entidades financieras, empresas operadoras o entidades públicas; ni aplicaciones móviles vinculadas a fraude o captación ilícita de información.

No obstante, el Decreto Legislativo N.º 1338 atribuye al OSIPTEL determinadas competencias respecto a la suspensión o baja de servicios públicos móviles o bloqueo de equipos terminales móviles vinculados a la comisión de delitos, siempre y cuando exista un pedido de entidades competentes en materia de investigación delictiva o a pedido del usuario afectado que acredite dicha situación.

En efecto, conforme al literal d) del artículo 6 del Decreto Legislativo N.º 1338, el OSIPTEL tiene competencia para requerir a las empresas operadoras de servicios públicos móviles de telecomunicaciones, a solicitud de entidades competentes como el Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, el Ministerio Público y el Poder Judicial la baja del servicio público móvil, de acuerdo al reporte de los equipos terminales móviles utilizados o vinculados a la comisión de delitos.

Asimismo, en virtud de dicha norma, corresponde al OSIPTEL requerir, a solicitud expresa del usuario afectado, cuya circunstancia debe ser acreditada mediante la respectiva denuncia y una constatación policial, el bloqueo del IMEI o la suspensión temporal del servicio público móvil ante la empresa operadora correspondiente.

En ese sentido, en la medida que el uso de una línea móvil y/o equipo terminal móvil para difundir los mensajes, información o contenido indicado en la consulta, implique la comisión de un delito, el OSIPTEL podría requerir la suspensión o baja del servicio público móvil o el bloqueo del equipo terminal móvil a solicitud de la autoridad competente o del usuario afectado, conforme a lo antes mencionado.

4.5 Informe si OSIPTEL cuenta con registros, reportes, estadísticas o diagnósticos sobre:

- **denuncias o reportes de estafas telefónicas;**
- **uso de líneas móviles para fraude;**
- **casos asociados a SIM box, spoofing, smishing, vishing o modalidades afines;**
- **incidencia de equipos terminales móviles alterados, clonados, duplicados o inválidos vinculados a actividades ilícitas.**

De existir, sírvase remitir la información consolidada de los años 2024, 2025 y lo que va del 2026.

El OSIPTEL no cuenta con registros, reportes, estadísticas ni diagnósticos relacionados con denuncias o reportes de estafas telefónicas, uso de líneas móviles para fraude, casos asociados a modalidades como SIM box, spoofing, smishing, vishing u otras afines, ni sobre la incidencia de equipos terminales móviles alterados, clonados, duplicados o inválidos vinculados a actividades ilícitas.

Ello se fundamenta en que, conforme a lo dispuesto en la Ley N.° 27336 – Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, así como en su Reglamento General, no corresponde a este organismo la persecución penal ni la investigación de delitos, competencias que recaen en las autoridades jurisdiccionales y en los órganos especializados en materia de seguridad y persecución del delito. Sin embargo, el organismo pone a disposición de las entidades del Estado facultadas el Módulo de Consulta Especializado para entidades del Estado, mediante el cual se facilita información relevante a las autoridades competentes, a fin de que estas puedan llevar a cabo las investigaciones correspondientes.

No obstante, en el marco del estado de emergencia decretado por el Poder Ejecutivo, OSIPTEL ha recibido solicitudes de suspensión de líneas vinculadas a presuntos actos ilícitos, las cuales han sido gestionadas y remitidas oportunamente a las empresas operadoras para su ejecución.

En dicho contexto, desde el 22 de octubre de 2025 al 30 de marzo de 2026, este Organismo ha solicitado a las empresas operadoras del servicio público móvil la suspensión inmediata de cuatro mil novecientos cuarenta y seis (4 946) líneas de servicios públicos móviles vinculadas a casos de extorsión, secuestro, sicariato, entre otros delitos.

Tabla N° 01: Requerimientos de suspensión de líneas de servicios públicos móviles de Entidades Públicas – Estado de Emergencia

Ministerio del Interior	Ministerio Público	Total
4860 líneas	86 líneas	4946 líneas

Fuente: DAPU - OSIPTEL

Sin perjuicio de lo antes señalado, se adjunta información estadística de sobre la cantidad de equipos bloqueados por ser detectados en la red de las empresas operadoras con IMEI inválido e IMEI clonados desde enero de 2024, con corte a febrero de 2026; cabe precisar que dicha información corresponde a equipos identificados en la red móvil con dichas casuísticas y que los mismos no necesariamente estuvieron vinculados a actividades ilícitos de tipo denuncias, fraudes u otros similares.

Cuadro N° 01: Cantidad de IMEI inválidos bloqueados por mes

Año	Mes	Cantidad IMEI	Total
2024	Ene-24	7,264	126,507
	Feb-24	6,576	
	Mar-24	6,477	
	Abr-24	7,171	
	May-24	18,064	
	Jun-24	12,820	
	Jul-24	13,055	
	Ago-24	12,776	
	Set-24	11,858	
	Oct-24	10,698	
	Nov-24	9,229	
	Dic-24	10,519	
2025	Ene-25	11,129	244,691
	Feb-25	8,701	
	Mar-25	9,868	
	Abr-25	9,382	
	May-25	10,592	
	Jun-25	14,909	
	Jul-25	22,200	
	Ago-25	36,543	
	Set-25	32,611	
	Oct-25	32,457	
	Nov-25	25,409	
	Dic-25	30,890	
2026	Ene-26	36,365	68,696
	Feb-26	32,331	

Cuadro N° 02: Cantidad de IMEI clonados bloqueados por mes

Año	Mes	Cantidad de IMEI	Total
2024	Ene-2024	16,821	1,114,460
	Feb-2024	129,721	
	Mar-2024	-	
	Abr-2024	400,713	
	May-2024	279,562	
	Jun-2024	125,793	
	Jul-2024	17,943	
	Ago-2024	49,009	
	Set-2024	25,292	
	Oct-2024	21,409	
	Nov-2024	28,381	
	Dic-2024	19,816	
2025	Ene-2025	20,823	235,664
	Feb-2025	19,821	
	Mar-2025	20,406	
	Abr-2025	25,593	
	May-2025	23,228	
	Jun-2025	16,987	
	Jul-2025	23,535	
	Ago-2025	22,390	
	Set-2025	19,990	
	Oct-2025	8,641	
	Nov-2025	8,264	
	Dic-2025	25,986	
2026	Ene-2026	20,414	36,003
	Feb-2026	15,589	

4.6 Indique si existen actualmente canales de interoperabilidad, intercambio de información o coordinación institucional entre OSIPTEL y:

- **el Ministerio del Interior;**
- **la Policía Nacional del Perú;**
- **el Ministerio Público;**
- **el Poder Judicial;**
- **el Instituto Nacional Penitenciario;**
- **el Ministerio de Transportes y Comunicaciones;**
- **otras entidades públicas vinculadas a la investigación o prevención de delitos cometidos mediante servicios móviles.**

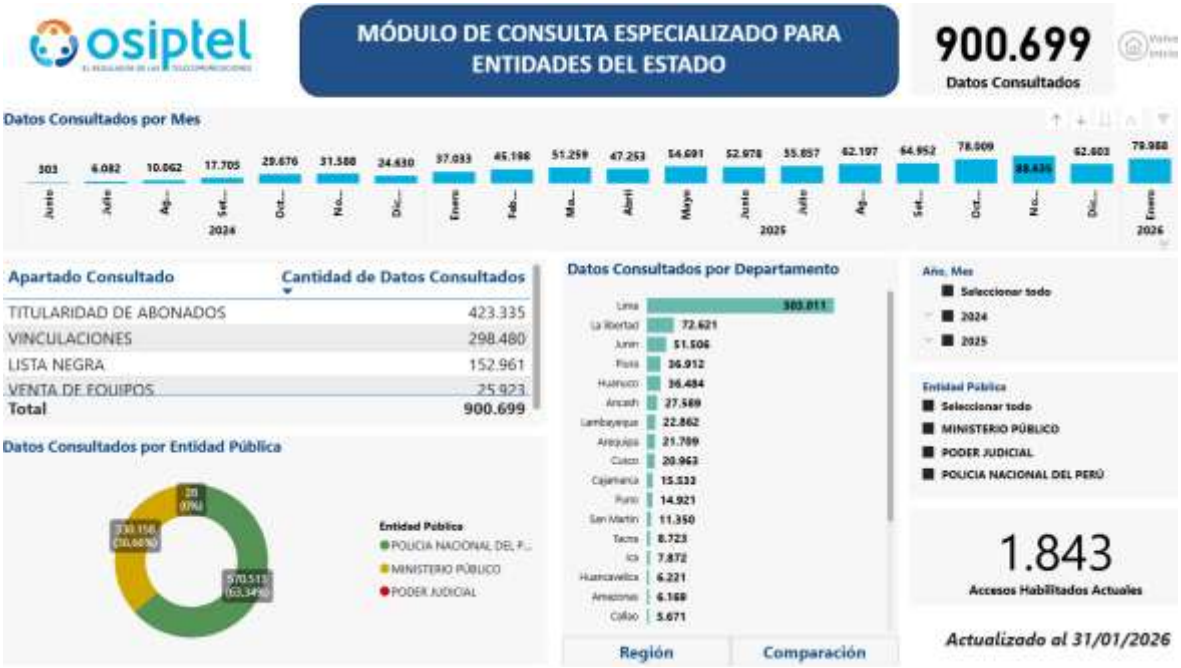
Sírvase precisar la naturaleza de tales mecanismos, su sustento normativo y sus límites.

El OSIPTEL, como administrador del RENTESEG, en atención a lo establecido en el numeral 18.3 del artículo 18 del Reglamento[10] del RENTESEG, desarrolló e implementó el Módulo de Consulta Especializado para Entidades del Estado (en adelante Módulo de Consulta) que permite atender requerimientos de información a nivel nacional del Ministerio del Interior, Policía Nacional del Perú, Ministerio de Justicia, así como, del Ministerio Público (Fiscalías) acceder a información del RENTESEG, proporcionada por las empresas operadoras de servicios públicos móviles en el Perú.

El 22 de abril de 2024 se inició la operatividad del sistema Módulo de Consulta, el cual permite atender requerimientos las 24 horas del día, durante los siete días de la semana, de forma inmediata y a nivel nacional, a los requerimientos de información relacionados a: la titularidad de los servicios públicos móviles[11], el registro de los equipos terminales móviles reportados como sustraídos o perdidos en el Perú[12], la vinculación entre IMEI y servicios públicos móviles[13] y el Registro de Ventas de equipos terminales móviles[14].

Esta herramienta optimizó el acceso a la información, fortaleciendo la articulación institucional y la eficiencia en la lucha contra la criminalidad. Desde su puesta en funcionamiento, a enero de 2026, se han registrado 900 699 datos consultados, lo que demuestra un uso progresivo y sostenido del sistema, consolidándolo como una herramienta eficaz en el marco de investigaciones fiscales y policiales.

[10] Aprobado mediante el Decreto Supremo Nº 007-2019-IN y sus modificatorias.
[11] **Apartado de Consulta Servicios Móviles**: Permite obtener información de los números de Servicios Móviles de Perú. La fuente de información es el Registro de Abonados del RENTESEG (contiene información histórica).
[12] **Apartado de Consulta Terminales Móviles:** Permite obtener información de los números de IMEI que se encuentran reportados como sustraídos, perdidos y aquellos con estado recuperado. La fuente de información es la Lista Negra del RENTESEG (contiene información histórica).
[13] **Apartado de Consulta Lista de Vinculaciones:** Permite obtener información de las Vinculaciones entre IMEI y Servicio Móvil. La fuente de información es la Lista de Vinculaciones Diarias del RENTESEG. (a partir del 22/04/2024).
[14] **Apartado de Consulta del Registro de Ventas:** Permite obtener información de las ventas de equipos terminales móviles reportada por las empresas operadoras y s cazas comercializadoras que requieran el acceso al registro. La fuente de información es el Registro de Ventas del RENTESEG (a partir del 22/04/2024).



4.7 Precise cuáles son las obligaciones actualmente exigibles a las empresas operadoras de servicios públicos móviles de telecomunicaciones respecto de:

- **identificación y registro de abonados;**
- **validación de titularidad;**
- **atención de requerimientos de bloqueo o baja;**
- **conservación de datos técnicos asociados a líneas y equipos;**
- **colaboración con autoridades competentes en casos de fraude o delitos informáticos.**

4.7.1 Identificación, validación del titular y registro de Abonados

En primer término, resulta relevante indicar que, el Decreto Legislativo N.º 1338[15], estableció que las empresas operadoras de servicios públicos móviles de telecomunicaciones tienen la obligación de verificar la identidad de quien contrata el servicio público móvil mediante el sistema de verificación biométrica. Debido a ello, este Organismo en el marco de sus competencias y funciones ha adoptado diversas medidas orientadas a combatir la suplantación de identidad y la contratación ilegal de servicios móviles.

En ese sentido, en ejercicio de su función normativa, contemplada en el literal c) del artículo 3 de la Ley N.º 27332, Ley Marco de los Organismos Reguladores de la Inversión Privada en los Servicios Públicos, el OSIPTEL, a través de su Consejo Directivo, ha emitido la siguiente normativa:

- La Resolución N.º 056-2015-CD/OSIPTEL[16], que modificó el TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones (derogado por la actual Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones[17]), estableció que, para la contratación del servicio público móvil en la modalidad prepago, el abonado debe validar su identidad a través de verificación biométrica de huella dactilar.

[15] Publicada en el diario oficial El Peruano con fecha 6.01.2017.
[16] Publicada en el diario oficial El Peruano con fecha 5.06.2015.
[17] Aprobada mediante Resolución de Consejo Directivo N° 172-2022-CD/OSIPTEL.

- La Resolución N.º 072-2022-CD/OSIPTEL[18] que modificó el TUO de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, mediante la cual se estableció la obligación a la empresa operadora que, para la contratación del servicio público móvil, debe verificar correctamente la identidad del solicitante del servicio. Para tal fin, se determinó diversas medidas de autenticación, entre estas, que la empresa solicite la exhibición del documento de identidad y realice la consulta de verificación biométrica de huella dactilar con la base de datos del RENIEC. Sobre dicha consulta, se estableció un máximo de 5 intentos o consultas de verificación biométrica por persona en el día, y por tipo de trámite.

  Asimismo, la empresa operadora debe llevar un registro actualizado de los abonados que hubieran contratado servicios bajo la modalidad prepago, control y/o postpago.

- La Resolución N.º 059-2024-CD/OSIPTEL[19] mediante la cual se establecieron los requisitos esenciales para la contratación del servicio público móvil, siendo estos los siguientes: (i) Realizar la contratación y adquisición de chip en lugares autorizados, (ii) Validar la identidad del vendedor que interviene en la contratación y (iii) Validar la identidad del solicitante del servicio.

  Asimismo, en caso de incumplimiento de alguno de los requisitos esenciales, la empresa operadora comunica de ello al abonado dándole un plazo de cinco (5) días para regularizar la contratación. Caso contrario debe proceder con la suspensión y posterior baja del servicio.

- La Resolución N.º 061-2024-CD/OSIPTEL[20] precisó, entre otros, el procedimiento para la entrega de la contraseña única a los abonados al momento de realizar la contratación u otro trámite del servicio público móvil en el que se requiera la validación de su identidad.

- La Resolución N.º 070-2025-CD/OSIPTEL[21] estableció el procedimiento de baja de los servicios públicos móviles por registro inconsistente cuyos datos del abonado, así como del vendedor o persona natural que interviene en el proceso de contratación no coinciden con la información consignada en la base de datos del RENIEC y la Superintendencia Nacional de Migraciones.

- La Resolución N.º 116-2025-CD/OSIPTEL, estableció la obligación a las empresas operadoras de aplicar el procedimiento de validación de identidad a los abonados nacionales o extranjeros que mantengan más de diez (10) servicios públicos móviles bajo su titularidad.

4.7.2 Atención de los requerimientos de bajas y bloqueos de equipo

El literal d) del numeral 6.1 del artículo 6 del Decreto Legislativo N.º 1338 establece que el OSIPTEL tiene como atribución, entre otros, requerir a las empresas operadoras de servicios públicos móviles de telecomunicaciones, de oficio o a solicitud del Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, el Ministerio Público o el Poder Judicial la suspensión temporal de las líneas, la remisión de mensajes de advertencia a los abonados o usuarios, el

[18] Publicada en el diario oficial El Peruano con fecha 12.04.2022.
[19] Publicada en el diario oficial El Peruano con fecha 28.02.2024.
[20] Publicada en el diario oficial El Peruano con fecha 14.03.2024.
[21] Publicada en el diario oficial El Peruano con fecha 6.07.2025.

bloqueo del IMEI de los equipos terminales móviles detectados como alterados, duplicado, clonados, inválidos, que no se encuentren en la Lista Blanca del RENTESEG; y/o la baja del servicio público móvil, de acuerdo al reporte de los equipos terminales móviles utilizados o vinculados para la comisión de delitos, según el procedimiento establecido para tal fin.

De igual manera, el literal j) del numeral 8.1 del artículo 8 del referido marco normativo establece que las empresas operadoras tienen la obligación de dar de baja el servicio público móvil y bloquear el equipo terminal, de acuerdo al reporte proporcionado por el Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, el Ministerio Público o el Poder Judicial de los equipos terminales móviles utilizados o vinculados para la comisión de delitos, según el procedimiento establecido para tal fin.

Por otro lado, con relación a los requerimientos de bloqueo de equipo, en los artículos 75 y 76 de las Normas de las condiciones de uso de los servicios públicos de telecomunicaciones, ante el incumplimiento de los requisitos esenciales de contratación, las empresas operadoras deberán suspender, dar de baja o deshabilitar el servicio público móvil. Previamente, enviarán un mensaje de texto a cada servicio público móvil que no cuente con sustento válido sobre el cumplimiento de los requisitos.

Asimismo, en el artículo 60 sobre la suspensión del servicio y bloqueo de equipo terminal por la sustracción o pérdida de este último, se establece después 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.

Por otro lado, mediante el Decreto Supremo N.º 017-2025-IN[22], se modificó el Reglamento del Decreto Legislativo N.º 1338, a fin de incluir entre otras, las disposiciones necesarias, relacionadas a las facultades del OSIPTEL y las obligaciones de las empresas operadoras para la ejecución de la suspensión temporal de servicios públicos móviles y/o el bloqueo de equipos terminales móviles a solicitud expresa del usuario afectado por la comisión de delitos.

Cabe precisar que, el artículo 9 del Decreto Legislativo N.º 1338, establece que el incumplimiento de las disposiciones establecidas en los artículos 8, 8-A y 8-D[23] de dicho decreto legislativo y su reglamento constituye infracción, recayendo en el OSIPTEL la facultad sancionadora y el establecimiento de la tipificación de las infracciones y sanciones administrativas.

Por su parte, mediante la Resolución de Consejo Directivo N.º 000134-2025-CD/OSIPTEL[24], se aprobó la Norma que establece el procedimiento de baja de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles utilizados o vinculados a la comisión de delitos, el cual contempla la ejecución de dicho procedimiento a solicitud de la Entidad Competente, esto es, del Ministerio del Interior, de la Policía Nacional del Perú (PNP), del Instituto Nacional Penitenciario, del Ministerio Público y del Poder Judicial.

4.7.3 Conservación de datos técnicos asociados a líneas y equipos

[22] Publicado en el diario oficial El Peruano el 21 de noviembre de 2025.
[23] Mediante el Decreto Legislativo N° 1738, se modificó, entre otros, el artículo 9 del Decreto Legislativo N° 1338.
[24] Publicada en el Diario Oficial El Peruano el 25 de diciembre de 2025.

Sobre el particular, se debe señalar que el artículo 11 del TUO de las Condiciones de USO fue modificado mediante Resolución N.º 072-2022-CD/OSIPTEL, que regula la obligación de las empresas operadoras de llevar un registro de abonados. Según el texto vigente, dicho artículo dispone lo siguiente:

> "**Artículo 11.- Registro de abonados de acuerdo a la modalidad de contratación del servicio**
> (…)
> Asimismo, la empresa operadora debe llevar un registro actualizado de los abonados que hubieran contratado servicios bajo la modalidad prepago, control y/o postpago.
>
> Cada registro debe ser independiente, debiendo contener como mínimo:

N°	Contratante Persona Natural	Contratante Persona Jurídica
(i)	Nombre y apellidos completos del abonado	Razón social
(ii)	Nacionalidad del abonado	Registro Único de Contribuyentes (RUC)
(iii)	Número y tipo de documento legal de identificación del abonado, de acuerdo al siguiente detalle: - Nacionales: Documento Nacional de Identidad. - Extranjeros: Carné de Extranjería, Pasaporte o el documento legal de identidad válido requerido por la Superintendencia Nacional de Migraciones.	Nombre y apellidos completos, número y tipo de documento legal de identificación del representante legal, de acuerdo al siguiente detalle: - Nacionales: Documento Nacional de Identidad. - Extranjeros: Carné de Extranjería, Pasaporte o el documento legal de identidad válido requerido por la Superintendencia Nacional de Migraciones.
(iv)	- Servicios de telefonía fija y servicios públicos móviles: número telefónico. - Demás servicios: número de contrato o de identificación del abonado.	
(v)	Fecha y hora de instalación y/o activación del servicio	
(vi)	Reporte de verificación biométrica (de aplicar)	

Por su parte, el Reglamento del Decreto Legislativo N.º 1338, en su artículo 4 dispone que el RENTESEG es un sistema conformado por la Lista Blanca, la Lista Negra y otra información pertinente. Asimismo, dispone que las empresas operadoras tienen la obligación de interconectarse al RENTESEG con la finalidad de intercambiar la información requerida para los fines que correspondan.

En ese sentido, de acuerdo con el marco normativo vigente, las empresas operadoras deben conservar la información de tanto de los servicios públicos

móviles contratados, así como la información relacionada a equipos terminales móviles previamente registradas en el RENTESEG.

4.7.4 Colaboración entre entidades para combatir delitos informáticos

El 30 de septiembre de 2025 se publicó en el diario oficial El Peruano la Ley N.º 32451, mediante la cual se modifica la Ley N.º 30096, Ley de Delitos Informáticos, y el Código Penal (Decreto Legislativo N.º 635), con el objetivo de sancionar penalmente la activación ilegal de líneas móviles y la posesión ilegítima de SIM cards. Esta norma se enmarca en el esfuerzo del Estado por combatir el fraude en telecomunicaciones y fortalecer la seguridad ciudadana, en coordinación con el Ministerio Público, la Policía Nacional del Perú y el Osiptel.

Por otro lado, se modificó el literal f) del artículo 16 de la Ley N.º 27336, Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, obligando a las entidades supervisadas a proporcionar al OSIPTEL, mediante herramientas informáticas, toda la información del proceso de comercialización, contratación y activación de servicios móviles, incluyendo la identificación del personal que interviene. Esta información deberá ser entregada al Ministerio Público, la Policía Nacional del Perú y otras entidades competentes, lo que fortalece la trazabilidad y fiscalización de las operaciones comerciales en el sector.

4.8 Informe si, a criterio de OSIPTEL, el marco legal actual presenta vacíos, restricciones o insuficiencias para una actuación más rápida y eficaz frente al uso del servicio público móvil en estafas telefónicas o delitos informáticos. En particular, sírvase señalar si existen limitaciones respecto de:

- **plazos de atención por parte de empresas operadoras;**
- **causales habilitantes para la suspensión o baja de líneas;**
- **facultades regulatorias o supervisoras del OSIPTEL;**
- **tratamiento de evidencia digital o datos técnicos;**
- **coordinación interinstitucional.**

Respecto al uso del servicio público móvil en estafas telefónicas o delitos informáticos, en la medida que esto implica el uso de dicho servicio para la comisión de delitos, se vincula a lo establecido en el literal d) del artículo 6 del Decreto Legislativo N.º 1338.

En efecto, conforme al literal d) del artículo 6 del Decreto Legislativo N.º 1338, el OSIPTEL tiene competencia para requerir a las empresas operadoras de servicios públicos móviles de telecomunicaciones, a solicitud de entidades competentes como el Ministerio del Interior, la Policía Nacional del Perú, el Instituto Nacional Penitenciario, el Ministerio Público y el Poder Judicial, la baja del servicio público móvil, de acuerdo al reporte de los equipos terminales móviles utilizados o vinculados a la comisión de delitos; así como, corresponde al OSIPTEL requerir, a solicitud expresa del usuario afectado, el bloqueo del IMEI o la suspensión temporal del servicio público móvil ante la empresa operadora correspondiente.

Con relación a lo anterior, mediante Decreto Supremo N.º 018-2025-IN se aprobó el Lineamiento para la baja o suspensión temporal de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles utilizados o vinculados en la comisión de delitos, con la finalidad de fortalecer la coordinación y cooperación entre las entidades competentes, asegurando el intercambio oportuno, seguro y uniforme de la información que permita la ejecución efectiva de los requerimientos.

Asimismo, mediante Resolución N.º 000134-2025-CD/OSIPTEL, el OSIPTEL aprobó la "Norma que establece el procedimiento de baja de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles utilizados o vinculados a la comisión de delitos.

Aunado a lo anterior, el OSIPTEL se encuentra elaborando el proyecto de norma a efectos de establecer las reglas operativas que las empresas operadoras y el OSIPTEL deben observar para atender de forma célere las solicitudes de suspensión temporal de los servicios públicos móviles y/o el bloqueo de los equipos terminales móviles trasladadas por el OSIPTEL a solicitud expresa del usuario afectado.

En ese sentido, el marco normativo antes reseñado, establece los plazos de atención por parte de empresas operadoras, las causales habilitantes para la suspensión o baja de líneas, las facultades regulatorias o supervisoras del OSIPTEL, el tratamiento de evidencia digital o datos técnicos, así como, la coordinación interinstitucional.

Debido a que las normas antes mencionadas han sido recientemente emitidas, a partir del seguimiento de su aplicación en los sucesivos meses, se podrá identificar si es necesario mejorar o complementar dicha regulación.

Ahora bien, en el caso específico del uso del servicio público móvil en estafas telefónicas o delitos informáticos, es preciso tener en cuenta que la normativa aplicable a dicha problemática corresponde al ámbito administrativo y al ámbito penal, involucrando a distintas entidades, como la Policía Nacional del Perú, el Ministerio Público, el Ministerio de Transportes y Comunicaciones (MTC), las entidades financieras, las empresas operadoras, el OSIPTEL.

Precisamente, dichas entidades, desde sus competencias, vienen emitiendo normas con relación a la problemática bajo comentario. Así, por ejemplo, el MTC ha emitido, en el mes de febrero de este año, el Decreto Legislativo N.° 1723, Decreto Legislativo que establece reglas, medidas y/o mecanismos para el adecuado uso de la numeración en llamadas y mensajes de texto y su trazabilidad a fin de evitar el anonimato y comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones, cuya emisión se justifica en la comisión de actos ilícitos, tales como fraudes, estafas, extorsiones, amenazas o suplantación de identidad, que representa un riesgo creciente para la seguridad ciudadana, al afectar directamente la integridad, el patrimonio y la confianza de la población en el uso de los servicios públicos de telecomunicaciones.

Cabe indicar que, el MTC a la fecha se encuentra en elaboración del reglamento del Decreto Legislativo N.° 1723, para definir las reglas específicas, obligaciones y mecanismos que permitan el adecuado uso de la numeración en llamadas y mensajes de texto con el objetivo de combatir su anonimato y evitar las comunicaciones ilícitas en perjuicio de los usuarios de los servicios públicos de telecomunicaciones.

En ese sentido, en línea con lo que se mencionó previamente, es necesario una evaluación en conjunto con las diferentes entidades involucradas para analizar los distintos factores en torno a la problemática específica y así poder identificar los vacíos, restricciones o insuficiencias del marco legal vigente para una actuación más rápida y eficaz para enfrentar el uso de los servicios públicos móviles para la comisión de estafas telefónicas o delitos informáticos o vinculados a fraude.

4.9 Sírvase remitir opinión técnica e institucional sobre la viabilidad regulatoria y legal de implementar o reforzar medidas tales como:

- **bloqueo inmediato de líneas presuntamente vinculadas a estafas telefónicas o delitos informáticos;**
- **baja acelerada de servicios móviles utilizados para fraude;**
- **ampliación de causales de bloqueo de equipos terminales;**
- **preservación obligatoria de evidencia digital por parte de empresas operadoras;**
- **protocolos de atención permanente de requerimientos urgentes;**
- **fortalecimiento del RENTESEG respecto del uso delictivo de líneas y equipos.**

Como se mencionó previamente, en la normativa vigente ya se ha contemplado la baja de los servicios y bloqueo de equipos terminales vinculados a la comisión de delitos en general, otorgando un plazo célere para la ejecución de estas acciones por parte de las empresas operadoras.

En ese sentido, tanto por estafas telefónicas, delitos informáticos, fraude u otro delito previsto en el ordenamiento jurídico penal, las entidades competentes de la investigación de delitos se encuentran facultadas para requerir al OSIPTEL la baja de los servicios móviles y equipos terminales vinculados a dichos delitos, de conformidad con lo dispuesto en el literal d) del artículo 6 del Decreto Legislativo N.º 1338. Cabe mencionar que el procedimiento se encuentra regulado tanto en el Decreto Supremo N.º 018-2025-IN como en la Resolución N.º 134-2025-CD/OSIPTEL.

Asimismo, de acuerdo con el literal d) del artículo 6 del Decreto Legislativo N.º 1338, el mismo usuario afectado puede solicitar al OSIPTEL la baja del equipo terminal o la suspensión temporal del servicio vinculado a la comisión de delitos.

Aunado a ello, debemos indicar que, en virtud del literal e) del artículo 16 de la Ley de Desarrollo de las Funciones y Facultades del OSIPTEL, las empresas operadoras de servicios públicos de telecomunicaciones se encuentran obligadas a conservar, por un periodo de al menos tres años después de originada, la información realizada con la tasación, los registros fuentes del detalle de las llamadas y facturación de los servicios que explota y con el cumplimiento de normas técnicas declaradas de observancia obligatoria en el país por una autoridad competente, o de obligaciones contractuales o legales aplicables a dichos servicios.

Sin perjuicio de ello, para definir la viabilidad de implementar o reforzar la normativa vigente en cuanto al caso específico de estafas telefónicas o delitos informáticos o vinculados a fraude que se cometen utilizando los servicios públicos móviles, es preciso que previamente se evalúe en conjunto con las entidades involucradas en la problemática particular, esto es, la Policía Nacional del Perú, el Ministerio Público, el Ministerio de Transportes y Comunicaciones (MTC), las entidades financieras, las empresas operadoras, el OSIPTEL, entre otros, cuáles son las causas identificadas que aún persisten, las modalidades comunes, los canales a través de los cuales se vienen cometiendo, el impacto que ocasionan, las dificultades que se presentan en su investigación o sanción; así como, es preciso realizar el análisis comparado de normativa internacional en relación a dicho tema, para, a partir de ello, poder definir qué aspectos no han sido cubiertos por la normativa vigente o son necesarios reforzar, a fin de evitar que los referidos delitos se sigan cometiendo.

En ese sentido, el Regulador muestra su interés por participar, conforme a sus competencias, en la evaluación técnica de propuestas que impliquen fortalecer el marco normativo sobre el RENTESEG u otra normativa con la finalidad de enfrentar el uso de los servicios públicos móviles para la comisión de estafas telefónicas o delitos informáticos o vinculados a fraude.

4.10 Informe si OSIPTEL ha formulado, propuesto o recomendado anteriormente modificaciones normativas, reglamentarias o procedimentales orientadas a fortalecer la respuesta frente al uso indebido de servicios móviles para fines delictivos. De ser así, sírvase remitir copia de los informes, propuestas, opiniones técnicas o documentos de trabajo correspondientes.

El OSIPTEL no ha formulado, propuesto ni recomendado modificaciones normativas, reglamentarias o procedimentales específicamente orientadas a fortalecer la respuesta frente al uso indebido de servicios móviles para fines delictivos.

Debe precisarse que el uso indebido de los servicios públicos de telecomunicaciones se encuentra regulado en las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobadas mediante Resolución de Consejo Directivo N.° 138-2012-CD/OSIPTEL y sus modificatorias. En particular, el Capítulo IV – "Del Uso Indebido de los Servicios Públicos de Telecomunicaciones" establece las conductas que constituyen uso indebido, así como las facultades de las empresas operadoras para suspender o dar por terminado el servicio en tales casos.

El concepto de "uso indebido" regulado en dicho capítulo no se vincula necesariamente con la comisión de delitos, sino con prácticas que afectan la prestación del servicio y la operación de las empresas operadoras, tales como la reventa no autorizada de servicios o el uso de líneas para fines distintos a los contratados.

En consecuencia, las disposiciones emitidas por OSIPTEL en esta materia han estado orientadas a preservar la calidad y continuidad de los servicios de telecomunicaciones y a proteger la sostenibilidad de las operaciones de las empresas operadoras, sin que ello implique competencia directa en la investigación o persecución de ilícitos penales, funciones que corresponden a las autoridades jurisdiccionales y de seguridad del Estado.

No obstante, a través de la Resolución N.º 000139-2025-CD/OSIPTEL el OSIPTEL estableció los criterios para la detección del uso prohibido, en cumplimiento del mandato contenido en el Decreto Legislativo N.º 1688 y su reglamento.

Es pertinente mencionar que los criterios establecidos se sustentan en el uso de herramientas de geolocalización para identificar el origen de las comunicaciones dentro de los establecimientos penitenciarios o centros juveniles. Dicho mecanismo es técnicamente viable, pues los sistemas de geolocalización se encuentran estandarizados y forman parte nativa de las redes móviles en sus distintas tecnologías (2G, 3G, 4G y 5G). Estos mecanismos permiten geolocalizar los equipos terminales independientemente del tipo de servicio usado (voz, SMS o datos). En consecuencia, una vez que el equipo se conecta a la red móvil, la red puede identificarlo y determinar su ubicación.

Cabe resaltar que el mercado cuenta con oferta tecnológica disponible en materia de geolocalización. Ejemplo de ello son las soluciones presentadas por proveedores como Polaris Wireless, SS8 y Hacom.

Sin embargo, las empresas operadoras han manifestado su renuencia a dar cumplimiento a lo establecido en el Decreto Legislativo N.º 1688, y su reglamento, alegando principalmente que cualquier acción y costo involucrado para frenar las telecomunicaciones dentro establecimientos penitenciarios o centros juveniles, debe ser asumida por el Estado en el marco de su política para garantizar la seguridad ciudadana.

De otro lado, mediante la Resolución Ministerial N.° 1127-2025-IN, de fecha 17 de junio de 2025, se constituyó el Grupo de Trabajo Multisectorial encargado de la mejora y

actualización de la normativa que regula el Registro Nacional de Equipos Terminales Móviles para la Seguridad (RENTESEG). Este grupo tiene por finalidad revisar, actualizar y proponer modificaciones al marco normativo vigente, garantizando su adecuada implementación y fortaleciendo su contribución a la seguridad ciudadana.

Al respecto, en el Informe Final del referido grupo de trabajo, de fecha 30 de diciembre de 2025, se brindaron recomendaciones que buscan consolidar un sistema integral, sostenible y efectivo, que refuerce la seguridad ciudadana, garantice la trazabilidad de los equipos terminales móviles y fortalezca la cooperación interinstitucional, el mismo que se anexa a la presente.

4.11 Remita relación de normas, resoluciones, informes, directivas, lineamientos, estudios técnicos o cualquier otro documento emitido por OSIPTEL que resulte relevante para la materia consultada.

- Resolución N.º 059-2024-CD/OSIPTEL, que establece los requisitos esenciales para la contratación del servicio público móvil, siendo estos los siguientes: (i) Realizar la contratación y adquisición de chip en lugares autorizados, (ii) Validar la identidad del vendedor que interviene en la contratación y (iii) Validar la identidad del solicitante del servicio.

- Resolución N.º 070-2025-CD/OSIPTEL[25] que establece el procedimiento de baja de los servicios públicos móviles por registro inconsistente cuyos datos del abonado, así como del vendedor o persona natural que interviene en el proceso de contratación no coinciden con la información consignada en la base de datos del RENIEC y la Superintendencia Nacional de Migraciones.

- Resolución N.º 116-2025-CD/OSIPTEL, que establece la obligación a las empresas operadoras de aplicar el procedimiento de validación de identidad a los abonados nacionales o extranjeros que mantengan más de diez (10) servicios públicos móviles bajo su titularidad.

- Resolución N.º 000134-2025-CD/OSIPTEL que aprobó la Norma que establece el procedimiento de baja de los servicios públicos móviles de telecomunicaciones y/o el bloqueo de equipos terminales móviles utilizados o vinculados a la comisión de delitos.

4.12 Finalmente, sírvase indicar, desde una perspectiva técnica y regulatoria, qué medidas legislativas considera OSIPTEL pertinentes para reforzar la prevención, detección, suspensión, baja, bloqueo, trazabilidad y colaboración en la persecución de estafas telefónicas y delitos informáticos cometidos mediante servicios públicos móviles de telecomunicaciones.

Desde una perspectiva técnica y regulatoria, corresponde precisar que la prevención, detección, suspensión, baja, bloqueo, trazabilidad y colaboración en la persecución de estafas telefónicas y delitos informáticos cometidos mediante servicios públicos móviles de telecomunicaciones no constituye una competencia exclusiva del OSIPTEL, dado que la investigación y persecución de los hechos delictivos corresponde a las autoridades jurisdiccionales y de seguridad del Estado.

En esa línea, para definir la viabilidad de implementar o reforzar la normativa vigente en cuanto al caso específico de estafas telefónicas o delitos informáticos o vinculados a fraude que se cometen utilizando los servicios públicos móviles, es preciso que previamente se evalúe en conjunto con las entidades involucradas en la problemática

[25] Publicada en el diario oficial El Peruano con fecha 6.07.2025.

particular, esto es, la Policía Nacional del Perú, el Ministerio Público, el Ministerio de Transportes y Comunicaciones (MTC), las entidades financieras, las empresas operadoras, el OSIPTEL, entre otros, cuáles son las causas identificadas que aún persisten, las modalidades comunes, los canales a través de los cuales se vienen cometiendo, el impacto que ocasionan, las dificultades que se presentan en su investigación o sanción; así como, es preciso realizar el análisis comparado de normativa internacional en relación a dicho tema, para, a partir de ello, poder definir qué aspectos no han sido cubiertos por la normativa vigente o son necesarios reforzar, a fin de evitar que los referidos delitos se sigan cometiendo.

En ese sentido, el Regulador muestra su interés por participar, conforme a sus competencias, en la evaluación técnica de propuestas que impliquen fortalecer el marco normativo sobre el RENTESEG u otra normativa con la finalidad de enfrentar el uso de los servicios públicos móviles para la comisión de estafas telefónicas o delitos informáticos o vinculados a fraude.

V. CONCLUSIONES Y RECOMENDACIÓN

5.1 Se concluye que el OSIPTEL cuenta con facultades regulatorias y técnicas para supervisar y controlar el uso del servicio móvil, incluyendo la identificación del abonado, la trazabilidad del servicio, la suspensión y baja de líneas vinculadas a delitos, y el bloqueo de equipos terminales móviles.

5.2 Se recomienda remitir el presente Informe a la Congresista de la República, señora María Antonieta Agüero Gutiérrez, para los fines correspondientes.

Atentamente,

TATIANA MERCEDES PICCINI ANTON
DIRECTORA DE ATENCION Y
PROTECCION DEL USUARIO