

EXPOSICIÓN DE MOTIVOS

I. Objeto

El presente reglamento tiene por objeto desarrollar las disposiciones contenidas en el Decreto Legislativo N° 1688, Decreto Legislativo que regula obligaciones y sanciones administrativas para las empresas operadoras de servicios públicos de telecomunicaciones en relación con las comunicaciones ilegales en establecimientos penitenciarios y centros juveniles (en adelante, el Decreto Legislativo N° 1688).

II. Finalidad

El presente reglamento tiene por finalidad prevenir, mitigar y/o controlar la problemática de las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles.

III. Antecedentes

El artículo 44 de la Constitución Política del Perú establece que son deberes primordiales del Estado, garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Asimismo, la Disposición Preliminar del Texto Único Ordenado de la Ley de Telecomunicaciones aprobado por Decreto Supremo N° 013-93-TCC (en adelante, el TUO de la Ley de Telecomunicaciones), declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional.

Por su parte, el artículo 2 del TUO de la Ley de Telecomunicaciones, declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y control corresponde al Estado de acuerdo a dicha Ley. Asimismo, en su artículo 3 establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia.

Cabe considerar que los numerales 1, 3, 9 y 10 del artículo 75 del TUO de la Ley de Telecomunicaciones, establecen que son funciones del Ministerio de Transportes y Comunicaciones (en adelante, el MTC), fijar la política de telecomunicaciones a seguir y controlar sus resultados; otorgar y revocar concesiones, autorizaciones, permisos, licencias y controlar su correcta utilización; administrar el uso del espectro radioeléctrico, así como elaborar y aprobar el Plan Nacional de Asignación de Frecuencias; y, organizar el sistema de control, monitoreo e investigación del espectro radioeléctrico.

Mediante el Decreto Supremo N° 006-2011-JUS, que modificó el Reglamento del Código de Ejecución Penal, aprobado mediante Decreto Supremo N° 015-2003-JUS, se estableció la obligación de las empresas operadoras de los servicios públicos móviles de cortar el servicio y/o bloquear el equipo terminal móvil por uso prohibido en los establecimientos penitenciarios, conforme al artículo 37 del Código de Ejecución Penal, de acuerdo a los criterios y al procedimiento que para

tal efecto mediante directiva apruebe el Organismo Supervisor de Inversión Privada en Telecomunicaciones (en adelante, el OSIPTEL).

Asimismo, el Decreto Supremo N° 012-2012-MTC estableció disposiciones para la regulación de la operación de equipos bloqueadores o inhibidores de señales radioeléctricas en los establecimientos penitenciarios y centros juveniles de diagnóstico y rehabilitación y cautela el derecho de las personas a usar y prestar servicios de telecomunicaciones en los exteriores de estos establecimientos.

Por su parte, el Decreto Legislativo N° 1182, que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado (en adelante, el Decreto Legislativo N° 1182), modificó el artículo 368-A del Código Penal aprobado por Decreto Legislativo N° 635 que penaliza el ingreso indebido de equipos de comunicación en centros penitenciarios; así como, obliga a los concesionarios de servicios públicos de telecomunicaciones a advertir al destinatario de cualquier comunicación proveniente de una prisión o sus inmediaciones.

Así también, mediante el Decreto Legislativo N° 1229 y su reglamento aprobado mediante el Decreto Supremo N° 007-2016-JUS, se prohibió a las empresas operadoras de telefonía móvil y/o satelital emitir señales hacia el interior y sobre los establecimientos penitenciarios; así como, declara una zona de intangibilidad, inalienable e imprescriptible de doscientos (200) metros alrededor de los establecimientos penitenciarios.

Además, a través de la Resolución Ministerial N° 954-2016-MTC/01.03, se estableció que las operadoras no deben instalar ni operar infraestructura y equipos de telecomunicaciones dentro de la Zona de Intangibilidad, informar modificaciones en las características técnicas de sus estaciones radioeléctricas, permitir la instalación de equipos de monitoreo remoto por parte del MTC, garantizar un nivel de recepción menor o igual a -100 dBm en el límite de la zona, entre otros.

A través 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 (en adelante, el Decreto Legislativo N° 1338), se estableció 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 terminales móviles, dentro del marco del fortalecimiento de la seguridad ciudadana; garantizando la contratación de los servicios públicos móviles de telecomunicaciones.

En el mismo sentido, el artículo 161 del Reglamento del Código de Responsabilidad Penal de Adolescentes, aprobado mediante Decreto Legislativo N° 1348, aprobado por Decreto Supremo N° 004-2018-JUS, prohibió el uso de cualquier otro servicio de telecomunicaciones que permita la transmisión de voz y/o datos, distinto a los teléfonos públicos o las cartas; así como, prohibió el ingreso de equipos terminales y sus componentes, correspondientes a los servicios de telecomunicaciones, tales como equipos celulares, satelitales, radios transceptores y cualquier otro que permita la transmisión de voz y/o datos.

Asimismo, mediante el Reglamento del Decreto Legislativo N° 1338, aprobado por Decreto Supremo N° 007-2019-IN y las Normas Complementarias para la

Implementación del Registro Nacional de Equipos Terminales Móviles para la Seguridad, aprobadas a través de la Resolución de Consejo Directivo N° 07-2020-CD-OSIPTEL, se desarrollaron las disposiciones sobre el Registro Nacional de Equipos Terminales Móviles para la Seguridad - RENTESEG.

Ahora bien, mediante la Ley N° 32089 se delegó en el Poder Ejecutivo la facultad de legislar en materias de reactivación económica, simplificación y calidad regulatoria, actividad empresarial del Estado, seguridad ciudadana y defensa nacional, por el plazo de noventa (90) días calendario.

Así, en el sub numeral 2.8.2 del numeral 2.8 del artículo 2 de la Ley N° 32089, se facultó al Poder Ejecutivo a unificar y sistematizar el marco legal sobre las obligaciones y sanciones de los concesionarios de servicios públicos de telecomunicaciones e internet en el contexto de la prohibición de comunicaciones ilegales desde el interior de establecimientos penitenciarios y centros juveniles de diagnóstico y rehabilitación, salvaguardando los derechos de acceso a las telecomunicaciones e internet de las poblaciones aledañas. En mérito a dicha delegación de facultades, se emitió el Decreto Legislativo N° 1688, con el objeto de establecer las obligaciones y sanciones administrativas para las empresas operadoras de servicios públicos de telecomunicaciones, en relación con las medidas adoptadas por el Estado para prevenir, controlar y sancionar las comunicaciones ilegales provenientes de establecimientos penitenciarios y centros juveniles.

IV. Marco jurídico y las habilitaciones en cuyo ejercicio se dicta

El artículo 1 del Decreto Legislativo N° 1688 dispone que esta norma tiene por objeto establecer las obligaciones y sanciones administrativas para las empresas operadoras de servicios públicos de telecomunicaciones, en relación con las medidas adoptadas por el Estado para prevenir, controlar y sancionar las comunicaciones ilegales provenientes de establecimientos penitenciarios y centros juveniles.

De acuerdo con la Segunda Disposición Complementaria Final del Decreto Legislativo N° 1688, el MTC, en coordinación con el OSIPTEL, en un plazo no mayor a ciento ochenta (180) días calendarios contados desde la publicación de la mencionada norma, mediante Decreto Supremo aprueba el Reglamento correspondiente.

Cabe mencionar que, acorde con el artículo 4 de la Ley N° 29370, Ley de Organización y Funciones del MTC (en adelante, la LOF del MTC), el MTC es competente de manera exclusiva, en materia de infraestructura y servicios de comunicaciones.

Por su parte, el artículo 5 de la LOF del MTC dispone que, este Ministerio tiene, entre otras funciones rectoras, formular, planear, dirigir, coordinar, ejecutar, fiscalizar, supervisar y evaluar la política nacional y sectorial bajo su competencia, aplicable a todos los niveles de gobierno; así como, dictar normas y lineamientos técnicos para la adecuada ejecución, supervisión y evaluación de las políticas, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, la sanción, la fiscalización y ejecución coactiva en materias de su competencia.

De acuerdo con el numeral 2 del artículo 6 de la LOF del MTC, en el marco de sus competencias exclusivas, el MTC cumple con la función específica de administrar,

supervisar y evaluar los servicios públicos de telecomunicaciones, servicios de radiodifusión y servicios privados de telecomunicaciones.

Por otro lado, el artículo 2 del Texto Integrado actualizado del Reglamento de Organización y Funciones del MTC, aprobado mediante Resolución Ministerial N° 658-2021-MTC/01 (en adelante, el ROF del MTC), establece que, el MTC ejerce jurisdicción en el ámbito nacional, regional y local, como ente rector del sector Transportes y Comunicaciones, en el marco de sus competencias exclusivas y compartidas que le otorga la ley, comprendiendo, la competencia exclusiva en infraestructura y servicios de comunicaciones y la competencia compartida en promoción de la infraestructura de telecomunicaciones y el planeamiento de los servicios de telecomunicaciones de alcance regional.

De otra parte, el artículo 75 del TUO de la Ley de Telecomunicaciones establece que, además de las atribuciones señaladas en su propia Ley Orgánica, son funciones del MTC en materia de telecomunicaciones, entre otras, las siguientes: fijar la política de telecomunicaciones a seguir y controlar sus resultados, así como, elaborar y proponer la aprobación de los reglamentos y planes de los distintos servicios contemplados en la Ley y expedir resoluciones relativas a los mismos.

Asimismo, el artículo 76 del TUO de la Ley de Telecomunicaciones, dispone que el OSIPTEL, 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.

Por su parte, de conformidad con lo establecido en el artículo 3° de la Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos, aprobada mediante la Ley N° 27332 y modificada en parte por la Ley N° 27631, el OSIPTEL tiene 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, y otras de carácter general referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de usuarios.

En ese sentido, considerando el marco jurídico habilitante, se sustenta el presente Decreto Supremo, que tiene por objeto desarrollar las disposiciones contenidas en el Decreto Legislativo N° 1688.

V. Fundamento Técnico de la Propuesta Normativa

5.1. Problemática Identificada

Sobre el particular, se ha identificado el siguiente problema público: *“Incremento de comunicaciones ilegales realizadas a través de dispositivos no autorizados desde establecimientos penitenciarios y centros juveniles durante el periodo 2020-2024.”*

Al respecto, la seguridad pública es una prioridad fundamental para los gobiernos de todo el mundo y constituye una base esencial para el desarrollo de los Estados modernos, por lo que el uso estratégico de las redes de comunicaciones, la protección de los servicios públicos de telecomunicaciones y la restricción de las comunicaciones ilegales se convierten en asuntos de suma importancia para los países.

De esta manera, el control de las llamadas provenientes desde los establecimientos penitenciarios ha constituido un asunto relevante para la mayoría de los gobiernos durante las últimas décadas.

En el Perú, el problema de las extorsiones y otras actividades delictivas coordinadas desde establecimientos penitenciarios y, a su vez, desde centros juveniles, representan una amenaza creciente para la seguridad pública. Las investigaciones¹, tanto periodísticas como policiales han revelado que algunos internos continúan participando en redes criminales desde el interior de estos centros, utilizando comunicaciones no autorizadas para coordinar extorsiones, fraude y otros delitos que afectan a la población. De esta forma, estas actividades ilícitas se han vuelto especialmente complejas de manejar debido al fácil acceso a dispositivos móviles y SIM Cards, los cuales permiten a los internos mantener un flujo constante de comunicaciones hacia el exterior, incluso con restricciones físicas de seguridad².

En este contexto, los registros de la Policía Nacional del Perú (en adelante, PNP) muestran un crecimiento exponencial de ciertos delitos en los últimos cinco años, como la extorsión agravada y la coacción, que han aumentado en un 453.7% y 97%, respectivamente. Asimismo, durante este periodo se ha registrado un incremento en los delitos de robo de celulares y secuestro, como se puede observar en la siguiente tabla y gráfico.

Tabla N° 1: Denuncias por comisión de delitos según modalidad registrados por la PNP a nivel nacional, 2019-2023

Modalidad	2019	2020	2021	2022	2023	Var. % 2023/2019
Extorsión agravada	369	333	535	1,558	2,043	453.7%
Coacción	2,546	2,075	2,252	3,157	5,015	97.0%
Robo de celular	2,560	1,373	1,785	2,348	3,226	26.0%
Secuestro	864	706	885	993	1,022	18.3%

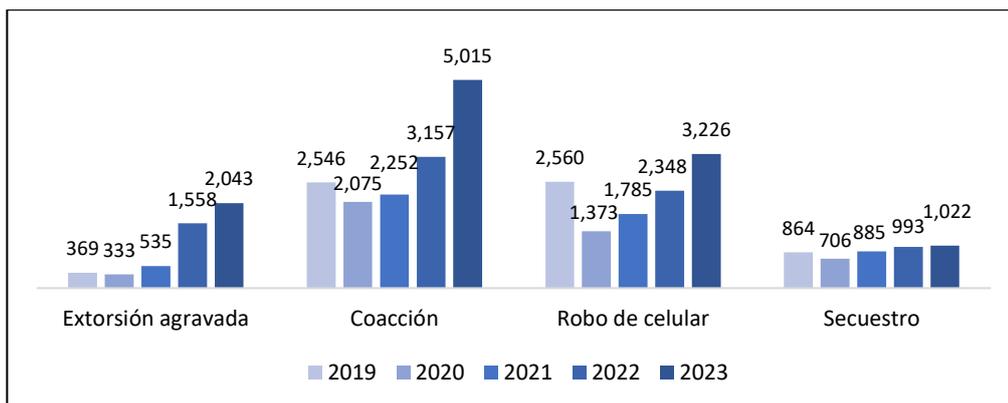
Fuente: Datacrim – Sistema Integrado de Estadísticas de la Criminalidad y Seguridad Ciudadana-INEI (<https://datacrim.inei.gob.pe/panel/mapa>).

Elaboración: Dirección General de Políticas y Regulación en Comunicaciones (DGPRC)-MTC.

Gráfico N° 1: Denuncias por comisión de delitos según modalidad registrados por la PNP a nivel nacional, 2019-2023

¹ Quinteros, V. M. (2023, 12 de noviembre). Tren de Aragua, cárceles y expansión del crimen transnacional. Ojo Público. <https://ojo-publico.com/4756/tren-aragua-carceles-y-expansion-del-crimen-transnacional>. De acuerdo con un reportaje del diario El Comercio, desde el penal de Challapalca, los líderes de la organización venezolana El Tren de Aragua enviaban instrucciones a sus subordinados fuera de la prisión a través de mensajes de audio. Uno de los implicados es Héctor Prieto Materano, alias "Mamut", uno de los 14 cabecillas de esta organización recluso en dicho centro penitenciario. Sin embargo, no es la primera vez que ocurre algo similar; según el mismo diario, "Mamut" también estuvo involucrado en un caso parecido mientras estaba recluso en el penal de Ancón I, en Lima, donde logró acceder a un teléfono celular. Por tanto, este incidente debería encender las alarmas en todos los niveles, no solo porque pone en evidencia el limitado control que ejerce la administración penitenciaria sobre la seguridad en el penal más inaccesible del país (Challapalca), sino también porque revela cómo el crimen organizado transnacional, específicamente El Tren de Aragua, opera desde las cárceles del Perú. (Fuente referida en la Exposición de Motivos N° 1688, p.4).

² Ver identificación del problema público en la Exposición de Motivos del Decreto Legislativo N° 1688.

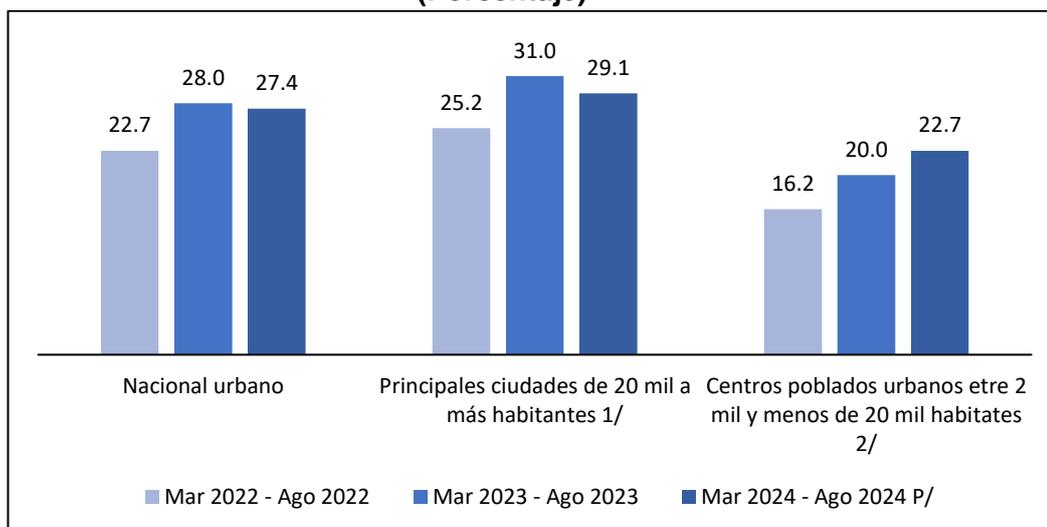


Fuente: Datacrim – Sistema Integrado de Estadísticas de la Criminalidad y Seguridad Ciudadana. INEI. (<https://datacrim.inei.gob.pe/panel/mapa>).

Elaboración: DGPRC-MTC.

En esa línea, según el Informe Técnico de Estadísticas de Seguridad Ciudadana³ (INEI, 2024), en el semestre de marzo a agosto de 2024, el 27.4% de la población de 15 años y más a nivel nacional fue víctima de algún hecho delictivo. Así también, en las principales ciudades con 20 mil o más habitantes, este porcentaje alcanzó el 29.1% de dicha población, lo que representa un incremento de 4.7 y 3.9 puntos porcentuales, respectivamente, en comparación con el mismo semestre de 2022.

Gráfico N° 2: Población urbana de 15 y más años de edad víctima de algún hecho delictivo. Semestre: Marzo – Agosto 2024 (Porcentaje)



Nota:

1/ Comprende 28 ciudades principales: 24 ciudades capitales (Arequipa, Trujillo, Ayacucho, Cajamarca, Chiclayo, Cusco, Huancayo, Huánuco, Ica, Iquitos, Piura, Pucallpa, Puno, Tacna, Abancay, Huaraz, Moquegua, Pasco, Puerto Maldonado, Tumbes, Chachapoyas, Huancavelica, Moyobamba y Lima Metropolitana (43 distritos de la Provincia de Lima) y las ciudades de Chimbote, Juliaca, Moyobamba y la Provincia Constitucional del Callao.

2/ Comprende centros poblados urbanos entre 2 mil y menos de 20 mil habitantes considerándose también capitales de distritos y ciudades que teniendo más de 20 mil habitantes no se encuentran en el grupo de ciudades priorizadas.

P/ Resultados preliminares para el año 2024.

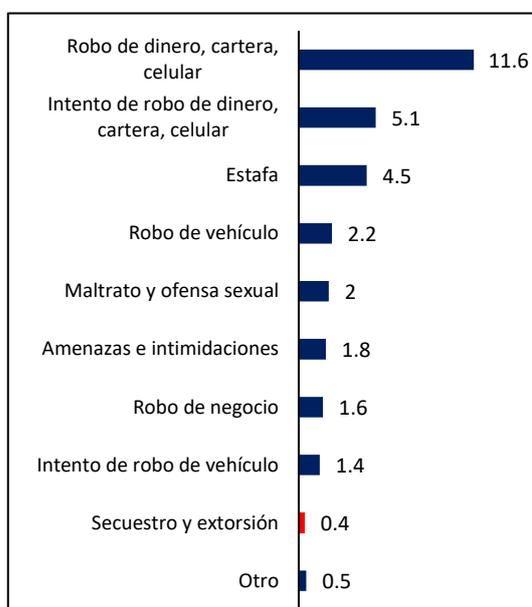
Fuente: Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024.

³ Instituto Nacional de Estadística e Informática. (2024). Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024. https://m.inei.gob.pe/media/MenuRecursivo/boletines/boletin_seguridad_2.pdf

De manera específica, en el semestre marzo a agosto de 2024, tanto a nivel nacional como en las principales ciudades de 20 mil o más habitantes, el 0.4% de la población de 15 años y más fue víctima de secuestro y extorsión. Sin embargo, aunque dichos delitos no presentan tasas tan elevadas en comparación con otros delitos, la percepción de inseguridad entre la población de 15 años y más es considerablemente mayor cuando se trata de la extorsión.

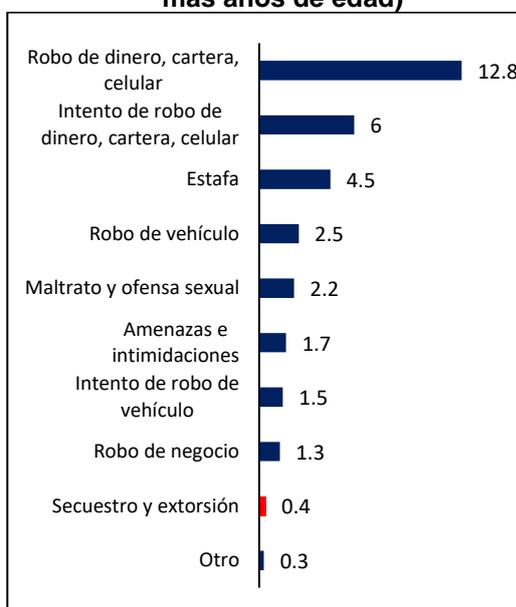
A nivel nacional, el 28.9% de esta población considera que podría ser víctima de extorsión, lo que representa un aumento de 7.5 puntos porcentuales respecto al mismo periodo de 2022. De otro lado, en las principales ciudades de 20 mil o más habitantes, el 31.0% de esta población percibe el riesgo de ser víctima de extorsión, cifra que implica un incremento de 8.3 puntos porcentuales en comparación con el mismo periodo de 2022.

**Gráfico N° 3: Tasa de víctimas por tipo de hecho delictivo, a nivel nacional
Semestre: Marzo – Agosto 2024
(Tasa por cada 100 habitantes de 15 y más años de edad)**



Fuente: Instituto Nacional de Estadística e Informática (2024). Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024.
Elaboración: DGPRC-MTC.

**Gráfico N° 4: Tasa de víctimas por tipo de hecho delictivo, en las principales ciudades de 20 mil a más habitantes
Semestre: Marzo – Agosto 2024
(Tasa por cada 100 habitantes de 15 y más años de edad)**



Fuente: Instituto Nacional de Estadística e Informática (2024). Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024.
Elaboración: DGPRC-MTC.

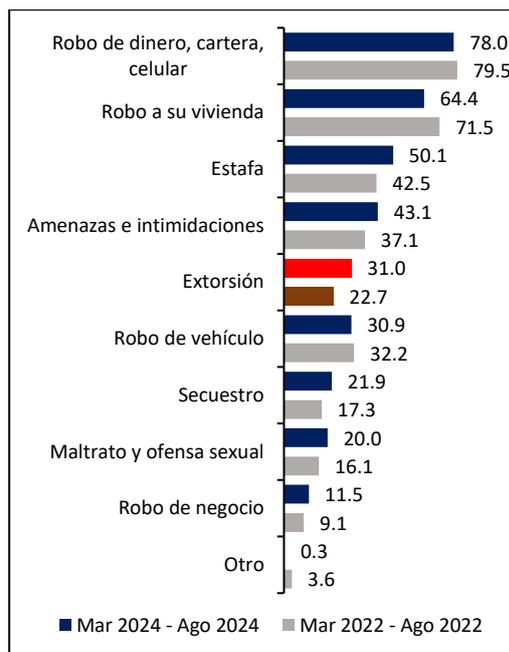
Gráfico N° 5: Población de 15 y más años de edad con percepción de inseguridad por tipo de hecho delictivo, a nivel nacional

Gráfico N° 6: Población de 15 y más años de edad con percepción de inseguridad por tipo de hecho delictivo, en las principales ciudades de 20 mil a más habitantes (Porcentaje)

(Porcentaje)



Fuente: Instituto Nacional de Estadística e Informática. (2024). Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024. Elaboración: DGPRC-MTC



Fuente: Instituto Nacional de Estadística e Informática. (2024). Informe Técnico N° 5 – Estadísticas de Seguridad Ciudadana: Marzo – Agosto 2024. Elaboración: DGPRC-MTC.

En este contexto, es fundamental reconocer que la principal actividad delictiva vinculada a los establecimientos penitenciarios y centros juveniles, es la extorsión, un delito que ha registrado un alarmante aumento del 453.7% entre 2019 y 2023. Este hecho delictivo está estrechamente asociado a los establecimientos penitenciarios debido a la disponibilidad de recursos y herramientas dentro de estos recintos que facilitan su perpetración. Entre dichos recursos destacan el mercado negro de datos personales —alimentado por la venta de información proporcionada por los usuarios a diversas empresas—, el comercio de celulares robados —que son modificados para seguir operando— y la venta fraudulenta de chips obtenidos mediante suplantación de identidad. Es así que, este complejo panorama subraya la necesidad de una intervención coordinada de actores públicos y privados, cuya participación es esencial para mitigar los factores que fomentan el fenómeno extorsivo relacionado con los establecimientos penitenciarios⁴.

Existe una clara relación entre las comunicaciones ilegales y la comisión de delitos como extorsión y secuestro desde los centros penitenciarios. Durante operativos y megaoperativos llevados a cabo por el Instituto Nacional Penitenciario (en adelante, el INPE), en algunos casos en coordinación con la PNP y el Ministerio Público, se han encontrado no solo equipos móviles y chips, sino también numerosos elementos relacionados con actividades ilícitas, especialmente extorsión mediante llamadas telefónicas. Entre estos elementos destacan vouchers, croquis de grifos, listas de nombres y números telefónicos, libretas o agendas con cuentas bancarias, y dinero en efectivo⁵.

⁴ Pereyra Colchado, G. (2022, 25 de junio). *Extorsiones desde las cárceles: con antenas ilegales evaden los bloqueadores de señal*. El Comercio. <https://elcomercio.pe/lima/seguridad/extorsiones-desde-las-carceles-con-antenas-ilegales-evaden-los-bloqueadores-de-senal-inpe-celulares-crimen-penal-castro-castro-pnp-ancon-1-noticia/>. (Fuente referida en la Exposición de Motivos N° 1688, p.14).

⁵ Diversas fuentes periodísticas han reportado estos hallazgos de actividades delictivas desde los establecimientos penitenciarios, tales como: Según la Agencia de Noticias Andina, en el operativo llevado a cabo en la cárcel de Piura se requisaron "listas con nombres y números telefónicos" que se presume estarían vinculados a delitos de extorsión.

Estos hallazgos sumados a la gran cantidad de dispositivos móviles y chips confiscados, son indicios sólidos que desde los establecimientos penitenciarios se coordinan delitos de extorsión y otras actividades criminales, por lo que esta situación no solo permite la continuidad delictiva, sino que también refuerza la estructura y operación de las organizaciones criminales dentro de los establecimientos penitenciarios consolidando su control y alcance.

Esta problemática tiene múltiples causas que contribuyen a su persistencia y complejidad, tales como los siguientes:

- **Ingreso y contrabando de dispositivos móviles:** Uno de los factores principales es el contrabando de teléfonos móviles y tarjetas SIM dentro de los centros penitenciarios y centros juveniles. Las limitadas medidas de control y seguridad en los puntos de acceso facilitan el ingreso de estos dispositivos, los cuales luego son utilizados para realizar llamadas y coordinar actividades delictivas, como se ha registrado a través de operativos policiales y notas periodísticas. Además, actos de corrupción y la falta de tecnología avanzada de detección agravan esta situación, dificultando la prevención efectiva del contrabando.

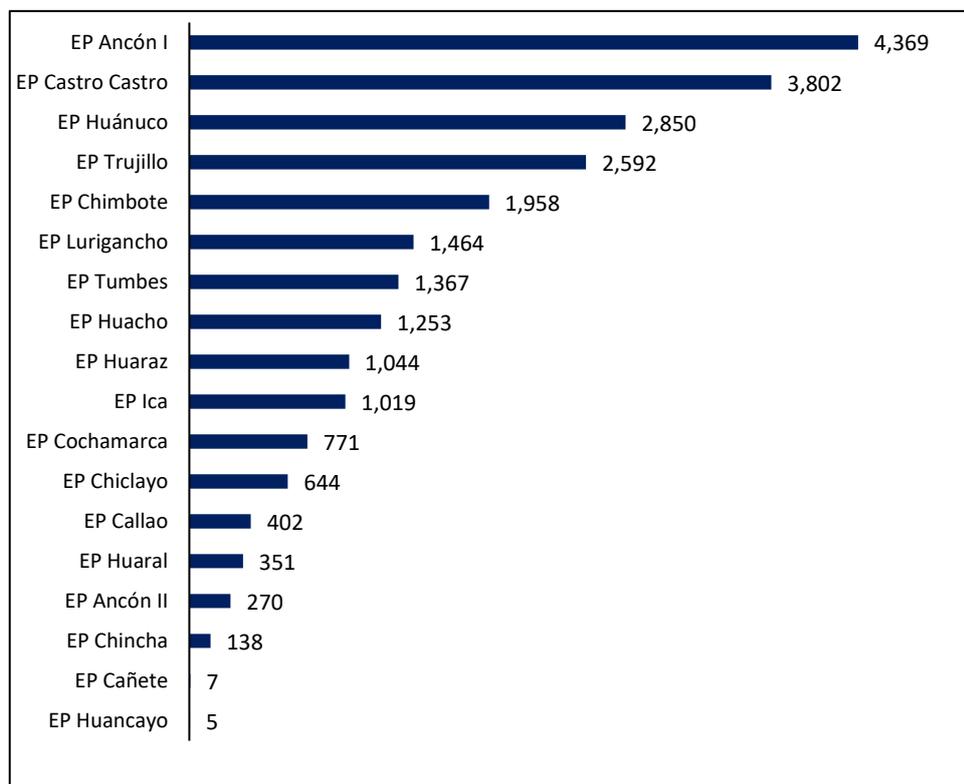
En este contexto, y según información del INPE, a pesar de la implementación de bloqueadores de señal radioeléctrica en varios establecimientos penitenciarios, se sigue registrando una considerable cantidad de incautaciones de tarjetas SIM y equipos telefónicos utilizados para realizar comunicaciones ilegales desde estos recintos.

Entre los establecimientos penitenciarios que cuentan con bloqueadores de señal, con el mayor número de incautaciones durante las requisas, se encuentran los que se muestran en el siguiente gráfico⁶.

(Andina. Agencia Peruana de Noticias. (2018, 27 de diciembre). *Requisan listas con nombres y números telefónicos en penal de Piura*. <https://andina.pe/agencia/noticia-requisan-listas-nombres-y-numeros-telefonicos-penal-piura-737353.aspx>). En el penal de Juliaca, el diario *Correo* reportó el hallazgo de evidencia vinculada a actividades de extorsión, como listas de contactos y croquis, lo cual respalda la hipótesis de la participación de los internos en estos delitos. (Correo. (2022, 14 de agosto). *Juliaca: Hallan indicios de extorsión en el penal*. <https://diariocorreo.pe/edicion/puno/juliaca-hallan-indicios-de-extorsion-en-el-penal-noticia/?ref=dc>). Así también, América Noticias informó sobre hallazgos en el penal de Ancón I donde se encontraron diversos objetos prohibidos, como un celular, un chip, un cargador artesanal, dos cables para celular y hojas de papel con anotaciones y números telefónicos. (Silva, K. (2023, 19 de octubre). *Penal Ancón I: Hallan celular y lista de teléfonos durante operativo*. América Noticias. <https://www.americatv.com.pe/noticias/actualidad/penal-ancon-hallan-celular-y-lista-telefonos-durante-operativo-n482749>). De igual manera, el diario *Perú 21*, señaló que durante una requisa en el pabellón 9 del penal Ancón I, se encontraron agendas con más de 300 números telefónicos y números de cuentas bancarias. (Perú 21. (2023, 10 de agosto). *En requisa hallan libreta con 300 números telefónicos*. <https://peru21.pe/lima/en-requisa-hallan-libreta-con-300-numeros-telefonicos-crimen-organizado-sicariato-extorsion-drogas-fiscalia-requisa-noticia/>). Por último, más recientemente, se realizó una requisa en el penal de Piedras Gordas, donde se encontraron anotaciones de números de cuentas bancarias y teléfonos de empresas, lo que aportaría evidencias que reforzarían la hipótesis de la Fiscalía sobre la habilitación de wifi dentro del penal, teoría que daría luces a la presunta comisión de delitos de extorsión desde el interior del recinto penitenciario. (Canal N. (2024, 16 de septiembre). *Reos contarían con internet en penal Piedras Gordas, según Fiscal*. <https://canaln.pe/actualidad/reos-contarian-internet-penal-piedras-gordas-segun-fiscal-n476690>). (Fuente referida en la Exposición de Motivos N° 1688, p.15, aumentada en esta nota al pie).

⁶ Gráfico desarrollado en base a la información contenida en la Exposición de Motivos del Decreto Legislativo N° 1688, considerando la Tabla N° 03, concerniente a la existencia de 18 establecimientos penitenciarios con el servicio de bloqueadores debidamente implementados (17 establecimientos penitenciarios del Contrato Innominado "Prestación de Servicios de Seguridad Tecnológica en las Prisiones" y 1 establecimiento penitenciario gestionado y administrado por el INPE, el establecimiento penitenciario de Cochamarca). (Ver las páginas 16 al 18).

Gráfico N° 7: Equipos terminales móviles y SIM Card incautados en requisas según establecimientos penitenciarios con bloqueador de señal, durante el periodo 2015 – 2023



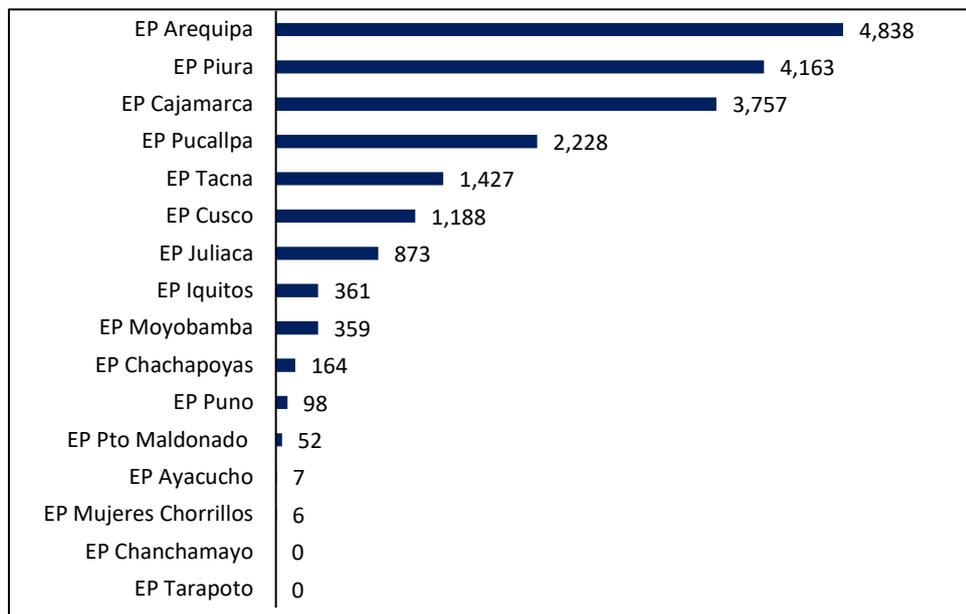
Fuente: Los datos corresponden a los partes informativos del CECOM - INPE, procesados por la DISEPE.

Elaboración: Observatorio Nacional de Política Criminal – INDAGA⁷.

Por otro lado, vista la Tabla N° 03 de la Exposición de Motivos del Decreto Legislativo N° 1688, de los 33 establecimientos penitenciarios incluidos en el Contrato Innominado de “Prestación de Servicios de Seguridad Tecnológica en las Prisiones” para la instalación de bloqueadores de señal radioeléctrica, 16 se encuentran aún en fase pre-operativa, es decir, los bloqueadores aún no están en funcionamiento. No obstante, la cantidad de tarjetas SIM y equipos terminales incautados durante las requisas en estos establecimientos no difiere significativamente de la cantidad de objetos prohibidos incautados en los centros penitenciarios que ya cuentan con bloqueadores en operación, como se muestra a continuación:

⁷ Gráfico N° 03 de la Exposición de Motivos del Decreto Legislativo N° 1688.

Gráfico N° 8: Equipos terminales móviles y SIM Card incautados en requisas según establecimientos penitenciarios con bloqueador de señal sin instalar, durante el periodo 2015 – 2023



Fuente: Los datos corresponden a los partes informativos del CECOM - INPE, procesados por la DISEPE.
Elaboración: Observatorio Nacional de Política Criminal – INDAGA⁸.

En esa misma línea, en aquellos establecimientos penitenciarios que no cuentan con sistema de bloqueo de señales radioeléctricas, se han incautado equipos terminales móviles y SIM Card, de acuerdo al siguiente detalle:

Tabla N° 2: Equipos terminales móviles y SIM Card incautados en requisas según establecimientos penitenciarios sin bloqueador de señal, en las requisas en el periodo 2015 – 2023

Nº	Establecimiento Penitenciario	Equipo móvil (IMEI)	Línea móvil (SIM)	Total
1	E.P. Juanjui	106	39	145
2	E.P. Sananguillo	59	23	82
3	E.P. Camaná	45	13	58
4	E.P. Yurimaguas	14	5	19
5	E.P. Challapallca	15	3	18
6	E.P. San Ignacio	8	5	13
7	E.P. Anexo Chorrillos	9	4	13
8	E.P. Bagua Grande	5	7	12
9	E.P. Moquegua	5	0	5
10	E.P. Mujeres Arequipa	3	1	4
11	Otros E.P.	7	9	16

Fuente: Dirección de Seguridad Penitenciaria del INPE.
Elaboración: Observatorio Nacional de Política Criminal – INDAGA⁹.

- **Uso compartido de dispositivos y rotación de SIM Cards:** La rotación frecuente de SIM cards y el uso compartido de teléfonos móviles entre

⁸ Gráfico N° 04 de la Exposición de Motivos del Decreto Legislativo N° 1688.

⁹ Tabla N° 05 de la Exposición de Motivos del Decreto Legislativo N° 1688.

internos dificultan la identificación de patrones específicos de comunicación que puedan ser rastreados por los operadores o las autoridades. Esta práctica permite a los internos evitar controles de seguridad, desdibujando la trazabilidad de las comunicaciones y facilitando la continuidad de sus actividades ilícitas sin dejar un rastro claro.

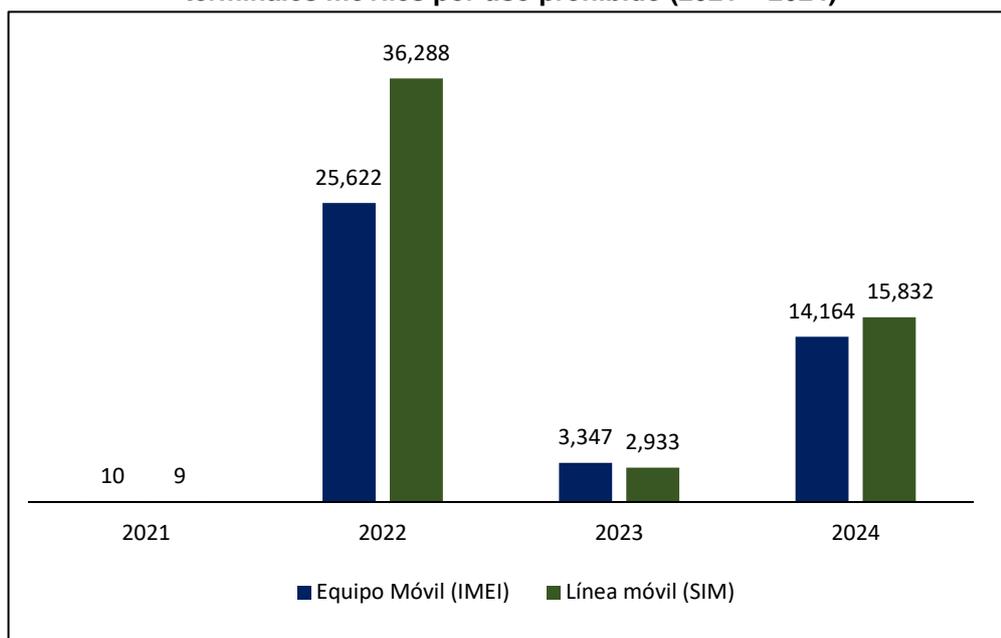
- **Normativa desactualizada:** Si bien han existido algunas disposiciones normativas sobre el control de comunicaciones en establecimientos penitenciarios, las mismas datan de hace varios años atrás, siendo que no se ha desarrollado un marco normativo específico, acorde al desarrollo tecnológico de los últimos años y que establezca obligaciones a las empresas operadoras en coordinación con las entidades competentes. Esta regulación desactualizada y poco específica ha limitado la adopción de mecanismo y/o medidas; así como, ha dificultado el ejercicio de la potestad fiscalizadora y sancionadora de las entidades competentes.

A propósito de lo anterior, de acuerdo con la información proporcionada por el OSIPTEL¹⁰, las empresas operadoras reportaron que entre 2021 y 2024, realizaron el corte de 55,062 líneas móviles y el bloqueo de 43,143 equipos terminales móviles por uso prohibido del servicio, en el marco del artículo 3 del Decreto Supremo N° 006-2011-JUS y del artículo 37 del Reglamento del Código de Ejecución Penal, aprobado por Decreto Supremo N° 015-2003-JUS.

En ese contexto, bajo un análisis desagregado año por año, se observa que, en el año 2022, se produjo un aumento exponencial en los cortes en comparación con el 2021, cuando no se registraron cortes. En 2023, el número de cortes disminuyó, pero en el 2024 se observó nuevamente un mayor incremento. Esta variación en los datos subraya la importancia de realizar una revisión exhaustiva de las medidas implementadas y evaluar su efectividad en la prevención de comunicaciones ilegales desde establecimientos penitenciarios. El gráfico a continuación ilustra este patrón, mostrando la baja cantidad de cortes en 2021, el marcado aumento en 2022, el descenso en 2023 y el repunte significativo en el 2024.

¹⁰ A través del correo electrónico de fecha 05 de noviembre de 2024.

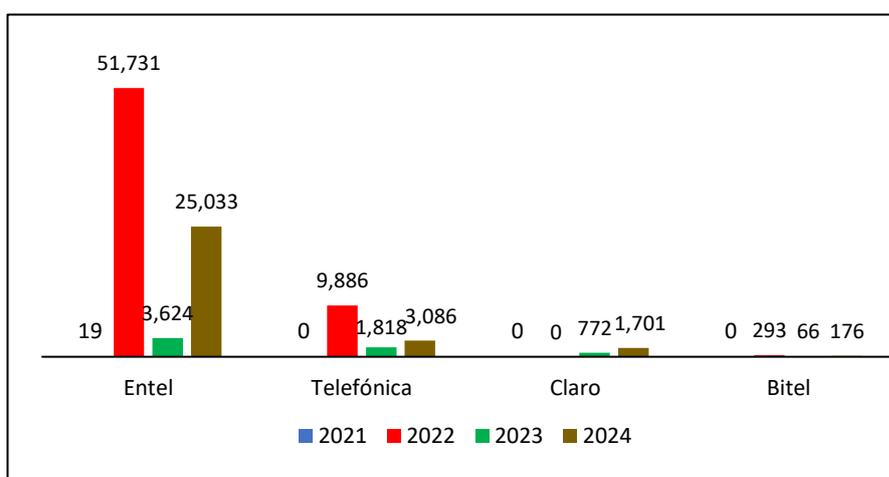
Gráfico N° 9: Número de cortes de servicios público móvil y/o equipos terminales móviles por uso prohibido (2021 – 2024)



Fuente: OSIPTEL.
Elaboración: DGPRC-MTC.

Asimismo, entre las operadoras de telecomunicaciones, Entel del Perú S.A. (en adelante, Entel) encabeza la lista en cuanto a la cantidad de cortes de servicio realizados, seguida por Telefónica del Perú S.A.A. (en adelante, Telefónica), América Móvil Perú S.A.C. (en adelante, Claro) y Viettel Peru S.A.C (en adelante, Bitel). Esta diferencia podría explicarse por varios factores ajenos al control de las empresas; sin embargo, también podría reflejar un cumplimiento deficiente de la medida de corte de servicio y/o bloqueo de equipos terminales móviles por parte de Claro y Bitel, que presentan un número de reportes considerablemente bajo, como se muestra en el siguiente gráfico.

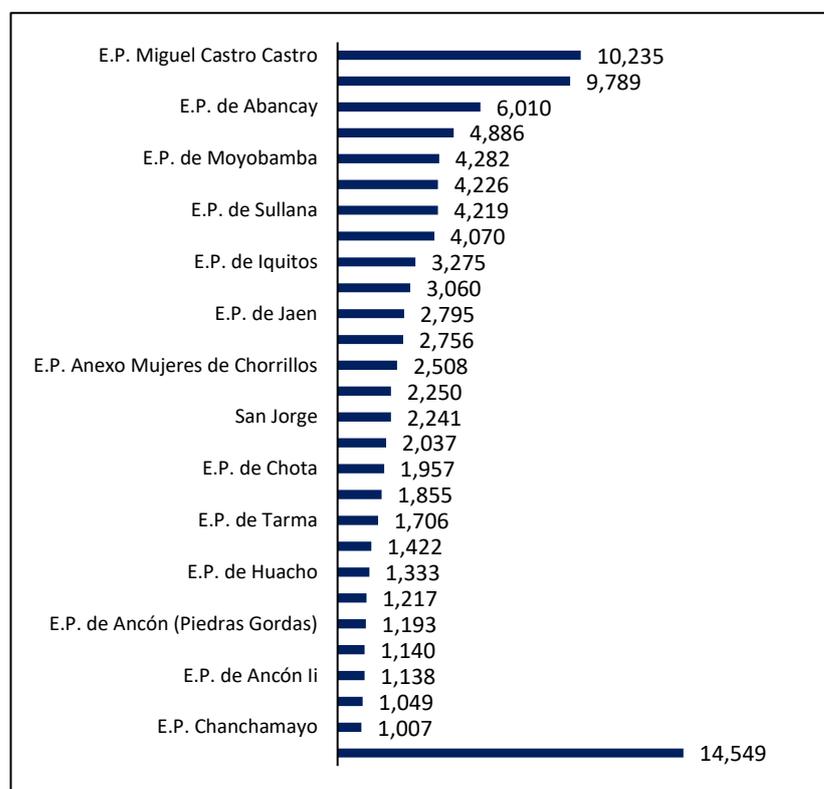
Gráfico N° 10: Número de cortes de servicios público móvil y/o bloqueo de equipos terminales móviles por uso prohibido, por operador telefónico y año 2021 – 2024



Fuente: OSIPTEL.
Elaboración: DGPRC-MTC.

Además, en el siguiente gráfico se presenta los establecimientos penitenciarios con mayor número de cortes de servicio y/o bloqueos de equipos terminales móviles.

Gráfico N° 11: Establecimientos Penitenciarios con el mayor número de cortes de servicio y/o bloqueo de equipos terminales móviles durante el periodo 2021 – 2024



Fuente: OSIPTEL.
Elaboración: DGPRC-MTC.

Aunado a lo anterior, la Tabla N° 8 de la Exposición de Motivos del Decreto Legislativo N° 1688, a través de un análisis comparativo entre los datos de celulares y SIM Card incautados por el INPE y los datos de cortes de servicio y/o bloqueo de celulares proporcionados por el OSIPTEL, sugiere la evidencia de una notable disparidad entre el número de equipos incautados y los cortes de servicio, considerando que el período de cortes abarca solo tres años (2021 a marzo de 2024), mientras que los datos del INPE cubren un periodo de nueve años (2015-2023). Asimismo, en dicha Exposición de Motivos se indica que tal diferencia sugiere varios escenarios posibles, incluyendo la presencia de factores externos que afectan la efectividad de los sistemas de bloqueo, la necesidad de incrementar las requisas ordinarias o extraordinarias, y una posible falta de cumplimiento en las acciones de corte o bloqueo por parte de las empresas operadoras¹¹.

En ese contexto, al evaluar tanto los centros penitenciarios que cuentan con sistemas de bloqueo de señales radioeléctricas como aquellos que no los tienen, se evidencia que la presencia de bloqueadores no es un factor determinante en la reducción de comunicaciones ilegales en los establecimientos penitenciarios.

¹¹ Ver en la Exposición de Motivos del Decreto Legislativo N° 1688, página 28.

Por otro lado, en relación con el problema de las comunicaciones ilegales en los Centros Juveniles, de acuerdo a lo presentado en la referida Exposición de Motivos del Decreto Legislativo N° 1688, según las encuestas realizadas a la población juvenil infractora en el II Censo Nacional de Población en estos establecimientos (2023), de un total de 1,820 adolescentes internos, 171 (9.4%) reportaron haber recibido ofrecimientos para involucrarse en actividades indebidas dentro de los centros juveniles. De estos 171 jóvenes, 54 (31.6%) señalaron que dichas actividades incluían el ingreso de celulares y chips, la venta de dispositivos móviles y la realización de llamadas ilegales. Estos datos evidencian la magnitud del problema y subrayan la urgente necesidad de implementar medidas efectivas para frenar el contrabando y el uso de dispositivos de comunicación en estos centros juveniles¹².

- **Presencia de señal radioeléctrica del servicio móvil dentro de establecimientos penitenciarios y centros juveniles:** La ubicación de muchos establecimientos penitenciarios y centros juveniles dentro o en las cercanías de zonas urbanas densamente pobladas genera que las señales del servicio móvil, destinadas a cubrir a la población general, irradien también hacia el interior de estos establecimientos, por lo que, esta cobertura no deseada se produce como consecuencia de que las estaciones base de las empresas operadoras están diseñadas para maximizar la conectividad urbana, pero sin mecanismos específicos para excluir las áreas penitenciarias, las señales alcanzan inadvertidamente dichos lugares.

Es así que, la presencia persistente de señal móvil en estos establecimientos facilita que internos y adolescentes utilicen dispositivos móviles de manera ilícita, habilitando comunicaciones ilegales que promueven actividades delictivas como extorsiones, fraudes y coordinación de crímenes desde el interior.

Por tanto, la existencia no controlada de señal radioeléctrica constituye un factor crítico que habilita la problemática de las comunicaciones ilegales en establecimientos penitenciarios, y cuya reducción es fundamental para frenarla.

Sobre la importancia de fortalecer los sistemas de bloqueo de señales radioeléctricas

Ante la problemática antes expuesta, es importante destacar que las soluciones técnicas implementadas a la fecha si bien contribuyen en la mitigación de señales radioeléctricas provenientes de los establecimientos penitenciarios, no resultan ser suficientes o se han visto desfasadas para combatir dicha problemática debido a diversas razones como pueden ser técnicas o regulatorias, ello sumado al constante desarrollo tecnológico, la poca coordinación entre los sectores involucrados y las deficientes medidas adoptadas para impedir el acceso de dispositivos móviles a estos establecimientos.

Bajo ese contexto, a continuación, se hace una breve descripción de las principales falencias identificadas de los sistemas de equipos de bloqueo o inhibición de señales implementados en los establecimientos penitenciarios del país, entre las que se incluyen:

¹² Ver en la Exposición de Motivos del Decreto Legislativo N° 1688, p.30.

a) Interferencias en la cobertura

Los sistemas de bloqueo o inhibición de señales están diseñados para interferir con las señales radioeléctricas que utilizan los teléfonos móviles para comunicarse con las antenas de telecomunicaciones. Sin embargo, su eficacia puede variar, como se describe a continuación:

- La señal de interferencia de los equipos bloqueadores en los penales puede verse mermada debido a factores como grosor de las paredes, el hormigón y las rejillas, que pueden atenuar la efectividad del bloqueador.
- Si la señal de las antenas de telecomunicaciones alcanza a los establecimientos penitenciarios y la intensidad o potencia del bloqueador no es suficiente, los teléfonos pueden seguir funcionando.

b) Avances tecnológicos

Los dispositivos móviles y las redes de telecomunicaciones están en constante evolución. Los teléfonos modernos pueden estar equipados con tecnologías de comunicación más sofisticadas (como 4G, 5G, Wi-Fi, Bluetooth, etc.), que son más difíciles de bloquear con un solo dispositivo. Además, algunos bloqueadores pueden no ser capaces de interferir con todas las frecuencias o tecnologías utilizadas por los dispositivos modernos.

c) Rango de alcance limitado

Los equipos bloqueadores de señales tienen un alcance limitado, lo que significa que solo pueden bloquear señales dentro de un área determinada. En un establecimiento penitenciario, si la cobertura del bloqueador no es lo suficientemente amplia o adecuada para cubrir toda el área, pueden quedar zonas donde las señales de telefonía aún sean accesibles.

d) Uso de tecnologías alternativas

Con la masificación de las redes móviles de banda ancha y la popularización de las plataformas o aplicaciones de mensajería instantánea, los reclusos suelen recurrir a estas tecnologías de comunicación menos detectables a través de Wi-Fi, que pueden ser más difíciles de interceptar o bloquear. Incluso si se bloquea la señal móvil, los internos pueden usar dispositivos modificados o formas alternativas de acceso a internet.

e) Mantenimiento y actualización deficiente

Los sistemas de bloqueadores o inhibidores de señales en los establecimientos penitenciarios podrían no tener el mantenimiento o actualización adecuada, lo que podría reducir su efectividad. La falta de filtros para bloqueadores que permitan interferir señales de nuevas tecnologías o bandas pueden dejar vacíos en la cobertura de las señales interferentes.

f) Comunicaciones por otros medios

Los reclusos pueden encontrar formas de evitar el bloqueo de señales, como el uso de radios o dispositivos móviles modificados que operan fuera de las

bandas de alcance de los bloqueadores. En muchos casos los reclusos hacen uso de antenas “hechizas” para la recepción de Wi-Fi, que camuflan como antenas de TV para la recepción de señales, esto sumado a que no se cuenta con una estrategia de monitoreo eficaz para detectar el uso de estos dispositivos, suele profundizar el problema.

g) Ingreso de dispositivos móviles en establecimientos penitenciarios

A pesar de los esfuerzos por bloquear las señales en establecimientos penitenciarios, las medidas adoptadas para controlar e impedir el ingreso de los dispositivos móviles son deficientes, ello sumado a la poca frecuencia de las requisas o una inadecuada estrategia de monitoreo, dificultan la labor de los sistemas de bloqueo facilitando a los reclusos el acceso a estos dispositivos para comunicarse hacia el exterior a menudo con fines delictivos.

h) Desafíos regulatorios

El uso de bloqueadores de señal en instituciones penitenciarias está limitado por regulaciones legales, toda vez que los bloqueadores pueden interferir con las comunicaciones legítimas de la población que vive en zonas aledañas o contiguas a los establecimientos penitenciarios afectando su derecho, por ejemplo, a los servicios de emergencia o al acceso a los servicios públicos de telecomunicaciones, lo que limita su uso o eficacia total en ciertas áreas.

i) Corrupción dentro de los penales

En algunos casos, la corrupción interna juega un papel clave en esta problemática, los reclusos buscan sobornar a personal de seguridad para que les permitan el acceso a teléfonos o a otros medios de comunicación, lo que facilita las actividades ilícitas desde los establecimientos penitenciarios. Esta corrupción puede dificultar aún más las operaciones de seguridad y control en los penales.

Como se puede observar, si bien los sistemas de equipos bloqueadores son una herramienta útil para el bloqueo o inhibición de señales de telefonía móvil en el interior de los establecimientos penitenciarios y así intentar frenar las comunicaciones no autorizadas, existen diversos factores técnicos, tecnológicos y operativos que pueden reducir su efectividad, haciendo que los reclusos sigan encontrando formas de eludir estos sistemas.

Estos factores representan desafíos para las autoridades penitenciarias para controlar el uso de teléfonos móviles dentro de los penales. Aunque se han implementado soluciones técnicas como los bloqueadores de señales, los reclusos siguen encontrando formas de ingresar dispositivos móviles, ello sumado a la complejidad de controlar de manera eficaz la propagación de las señales de telefonía hacia el interior de los penales, la dificultad para rastrear y ubicar los dispositivos que realizan comunicaciones no autorizadas, la falta de recursos para llevar a cabo investigaciones eficaces y la evasión de las autoridades por parte de los reclusos, a través de complejas redes de comunicación hacen que la extorsión y otras actividades delictivas desde el interior de los establecimientos penitenciarios prosperen.

5.2. Revisión de la experiencia internacional sobre medidas técnicas y regulatorias para el bloqueo de señales en establecimientos penitenciarios

Conforme a lo anteriormente expuesto, el uso de teléfonos móviles ingresados ilegalmente en los establecimientos penitenciarios con fines ilícitos como la extorsión, es una de las problemáticas más graves relacionadas con el mal uso de los servicios de telecomunicaciones y la inseguridad ciudadana, que se ha visto incrementada en los últimos años debido a la masificación de las redes de telefonía móvil y el uso no autorizado de teléfonos móviles dentro de los establecimientos penitenciarios, así como la eficacia limitada de soluciones como bloqueadores o inhibidores de señales.

Bajo ese contexto, algunos países han adoptado medidas técnicas y regulatorias alternativas o complementarias al uso de bloqueadores de señales para combatir el uso ilícito de teléfonos móviles y otras tecnologías de telecomunicaciones en los establecimientos penitenciarios. A continuación, se hace una breve revisión de las estrategias distintas a los bloqueadores de señales que se han implementado en algunos países:

Estados Unidos¹³

En Estados Unidos, la lucha contra el uso ilícito de teléfonos móviles y otras tecnologías de telecomunicaciones en establecimientos penitenciarios ha llevado a la adopción de varias medidas técnicas y regulatorias, además de los bloqueadores de señales. A continuación, se detallan algunas de las medidas más relevantes:

a) Tecnología de "Intercepción Controlada" (Managed Access Systems)

Estos sistemas permiten a las autoridades penitenciarias interceptar y gestionar las llamadas realizadas desde los teléfonos móviles dentro de las cárceles. A diferencia de los bloqueadores, que simplemente bloquean la señal, los sistemas de acceso gestionado permiten identificar, interceptar y bloquear las llamadas que no provienen de números autorizados.

Funcionamiento: El sistema crea una "zona de control" en el establecimiento penitenciario donde los teléfonos móviles pueden ser monitoreados. Solo los números previamente aprobados y registrados en una base de datos tienen acceso a las redes, mientras que el resto de las llamadas o mensajes enviados desde los teléfonos no autorizados son bloqueados o interceptados.

Regulación: Esta tecnología está regulada por la Comisión Federal de Comunicaciones (FCC) y la legislación estatal. Requiere permisos específicos para su instalación y operación, y debe cumplir con las normativas sobre privacidad y seguridad de las telecomunicaciones.

b) Colocación de Redes Privadas de Comunicaciones (Private Networks)

Algunas prisiones instalan redes privadas internas que bloquean el acceso a la red pública de telecomunicaciones, permitiendo la comunicación solo entre dispositivos autorizados dentro del recinto.

¹³ Ver norma en <https://www.law.cornell.edu/cfr/text/47/20.23>

Funcionamiento: Estas redes aisladas no permiten la conexión a la red móvil pública, y los internos pueden usar solo dispositivos que están específicamente configurados para este tipo de redes. Esto limita significativamente las posibilidades de comunicación no autorizada.

Regulación: Se requiere la coordinación con las autoridades de telecomunicaciones y puede estar sujeto a aprobaciones regulatorias, como las de la FCC, para asegurar que no interfiera con servicios públicos fuera de las instalaciones penitenciarias.

c) Tecnologías de Localización de Señales (Signal Detection and Localization)

Esta tecnología permite identificar la ubicación exacta de los teléfonos móviles en las instalaciones penitenciarias. Utiliza tecnologías de geolocalización como GPS o triangulación de señales celulares para localizar los dispositivos dentro del recinto.

Funcionamiento: Una vez que se detecta una señal de teléfono móvil, el sistema puede identificar la ubicación precisa del dispositivo, lo que permite a las autoridades penitenciarias intervenir de manera rápida y efectiva.

Regulación: Similar a los sistemas de interceptación, estas tecnologías deben cumplir con las regulaciones de privacidad y supervisión de las telecomunicaciones, y suelen ser implementadas bajo un marco de autorización judicial para asegurar que no se infrinja la privacidad de las comunicaciones legales.

d) Control de Acceso y Supervisión de Comunicaciones a través de Llamadas Monitoreadas

Los internos pueden ser autorizados a hacer llamadas, pero estas son monitoreadas y grabadas. Las llamadas pueden ser limitadas a ciertos números, y cualquier comunicación con números no autorizados es interceptada.

Funcionamiento: Las llamadas se realizan a través de sistemas que permiten a los operadores penitenciarios escuchar y grabar las conversaciones. En algunos casos, las llamadas son previamente autorizadas por los oficiales y, de ser necesario, pueden ser interrumpidas si se detecta actividad sospechosa.

Regulación: Esta medida está regulada por leyes federales y estatales que garantizan que la supervisión de las comunicaciones no infrinja los derechos constitucionales de los reclusos, como el derecho a la privacidad, aunque las autoridades suelen tener licencia para monitorear comunicaciones en contextos penitenciarios.

e) Ley Federal de Antibloqueo de Señales (Communications Act of 1934) y Enmiendas

Aunque los bloqueadores de señales están restringidos por la FCC a nivel federal debido a su potencial para interferir con las redes de telecomunicaciones públicas, existen leyes y enmiendas que permiten la implementación de tecnologías que no interfieren con los sistemas de comunicación en áreas externas a las cárceles.

La FCC establece que, en ciertos casos, las autoridades estatales pueden implementar bloqueadores o tecnologías de manejo de señales dentro de instalaciones penitenciarias bajo condiciones estrictas que eviten interferencias con el servicio público y la seguridad nacional.

Cabe indicar que la FCC en los últimos años ha autorizado el uso de diversas tecnologías de bloqueo de señales en penales, aunque se requieren permisos especiales para evitar interferencias en redes de telecomunicaciones externas. Así en 2017, la FCC aprobó una iniciativa para permitir el uso de bloqueadores de señales en establecimientos penitenciarios mediante sistemas de detección para localizar teléfonos móviles ocultos. Además, algunas prisiones experimentan con el uso de *dummy cells* para bloquear las señales de manera más dirigida y controlada.

Reino Unido¹⁴

El Reino Unido ha adoptado una serie de medidas técnicas y regulatorias para combatir este problema, garantizando al mismo tiempo el respeto a los derechos fundamentales y la seguridad pública.

a) Sistemas de Gestión de Señales (Managed Access Systems)

Uno de los enfoques más utilizados en el Reino Unido es la implementación de sistemas de gestión de acceso a señales (Managed Access Systems). Estos sistemas permiten controlar y filtrar las comunicaciones dentro de los establecimientos penitenciarios sin bloquear completamente las señales de telecomunicaciones externas.

Funcionamiento: Los sistemas de gestión de acceso funcionan mediante la identificación de teléfonos móviles dentro de las cárceles. Solo los dispositivos registrados pueden conectarse a las redes móviles internas de la prisión. Las llamadas realizadas desde teléfonos no autorizados o no registrados se bloquean o son interceptadas.

Regulación: Los sistemas de gestión de acceso deben cumplir con las regulaciones de la Ofcom (Oficina de Comunicaciones del Reino Unido) y la Autoridad Reguladora de Comunicaciones en cuanto a la interferencia con las redes externas. Estos sistemas operan bajo estrictas normativas para garantizar que no afecten a las comunicaciones fuera de los recintos penitenciarios.

b) Tecnologías de Detección de Señales

El Reino Unido también ha implementado tecnologías de detección de señales para localizar teléfonos móviles no autorizados dentro de las prisiones. Estas tecnologías permiten identificar emisiones de señales de radiofrecuencia provenientes de dispositivos de telecomunicaciones, como teléfonos móviles y otros dispositivos inalámbricos.

Funcionamiento: Las autoridades utilizan dispositivos de rastreo que pueden identificar la ubicación exacta de un teléfono móvil dentro de un establecimiento penitenciario. Estos sistemas ayudan a localizar dispositivos de manera

¹⁴ <https://www.gov.uk/government/publications/authorised-communications-controls-and-interception-policy-framework>

precisa, lo que facilita la confiscación de los teléfonos sin la necesidad de bloquear las señales de comunicación de forma generalizada.

Regulación: La Ofcom regula las tecnologías de detección de señales, asegurando que su uso no interfiera con las redes de telecomunicaciones públicas, ya que las interferencias pueden ser ilegales en el Reino Unido. Las tecnologías deben ser utilizadas exclusivamente en las instalaciones penitenciarias para evitar interferencias con las señales fuera de ellas.

c) Redes de Comunicaciones Privadas (Private Networks)

En algunos establecimientos penitenciarios, el Reino Unido ha implementado redes privadas de telecomunicaciones para permitir que los internos se comuniquen de manera controlada, sin acceder a las redes externas. Estas redes están diseñadas para que los internos puedan hacer llamadas y enviar mensajes solo dentro de la prisión, pero sin comunicación con el mundo exterior.

Funcionamiento: Estas redes internas están aisladas de las redes móviles públicas. Los internos solo pueden usar teléfonos dentro de la red interna para comunicarse con personal autorizado o con otros internos dentro del mismo establecimiento. Las comunicaciones fuera del penal solo se permiten bajo condiciones muy controladas y con la autorización de las autoridades penitenciarias.

Regulación: El uso de redes privadas está regulado por la Ofcom y debe cumplir con la legislación de telecomunicaciones vigente en el Reino Unido. Además, las autoridades penitenciarias deben garantizar que estas redes no interfieran con las comunicaciones externas y respeten la legislación en materia de protección de datos.

d) Sistemas de Acceso Controlado “Dummy Cells”

La Ley de Prisiones de 2012 impuso que las estaciones base falsas “Dummy Cells”, como los receptores IMSI, solo se podían instalar dentro de los muros de las prisiones.

Funcionamiento: La miniaturización de la tecnología ha hecho que, mientras que antes los IMSI o los receptores WiFi solo podían utilizarse en un lugar fijo, ahora pueden hacerse portátiles y estar más orientados a zonas específicas de las prisiones. Esto significa que los funcionarios de prisiones tienen un mayor control sobre dónde se vigilan los dispositivos y que las zonas fuera del complejo penitenciario, como aparcamientos, vías de acceso o zonas residenciales, no se ven afectadas.

Regulación: Esta medida está regulada por el “The Prisons Act” del año 2012¹⁵.

e) Tecnologías de Identificación Biométrica

El uso de tecnologías biométricas se ha expandido en algunos centros penitenciarios del Reino Unido para controlar el acceso de visitantes y evitar el

¹⁵ Ver norma: <https://www.legislation.gov.uk/ukpga/2012/20/contents>

ingreso de dispositivos electrónicos ilegales, como teléfonos móviles a las cárceles.

Funcionamiento: Las autoridades penitenciarias utilizan tecnologías como el reconocimiento facial, huellas dactilares y escaneo de iris para verificar la identidad de los visitantes y prevenir la introducción de dispositivos electrónicos no autorizados. Además, estas tecnologías también ayudan a rastrear a los internos y sus comunicaciones.

Regulación: La implementación de tecnologías biométricas está regulada por las leyes de protección de datos y privacidad del Reino Unido, que requieren que los datos personales de los individuos sean tratados de manera segura y conforme a la Ley de Protección de Datos de 2018. Las autoridades deben asegurarse de que el uso de esta tecnología no infrinja los derechos humanos de los reclusos ni de los visitantes.

f) Marco Regulatorio: Leyes de Telecomunicaciones y Seguridad

Ley de Comunicaciones (Communications Act 2003): Esta ley regula el uso de las telecomunicaciones en el Reino Unido, estableciendo un marco legal para las tecnologías que pueden utilizarse dentro de los establecimientos penitenciarios. La Ofcom supervisa que las tecnologías de telecomunicaciones sean utilizadas de acuerdo con esta ley, especialmente aquellas que puedan afectar las redes públicas.

Ley de Protección de Datos (Data Protection Act 2018): La ley establece cómo deben manejarse los datos personales, incluidos los datos biométricos y las grabaciones de comunicaciones. Las autoridades penitenciarias deben garantizar que el monitoreo y la recolección de datos se realicen conforme a las normas de privacidad.

Ley de Procedimiento Penal (Police and Criminal Evidence Act 1984): Esta ley establece las condiciones bajo las cuales las autoridades pueden interceptar y grabar las comunicaciones de los internos en las prisiones, asegurando que las medidas de seguridad sean legales y estén justificadas.

Asimismo, los países de la región han adoptado medidas adicionales o complementarias a las soluciones de bloqueadores con el fin de combatir las comunicaciones ilegales desde el interior de los centros penitenciarios, conforme se puede advertir en la siguiente tabla:

Tabla N° 3: Medidas adicionales o complementarias a los bloqueadores adoptadas por los países de la región

País	Normativa para el bloqueo de	Entidades responsables	Solución de bloqueo implementada	¿Qué dice la norma?	Enlace
------	------------------------------	------------------------	----------------------------------	---------------------	--------

	llamadas en las cárceles				
Colombia	Decreto 851 de 2024	Ministerio de Justicia Instituto Nacional Penitenciario (INPEC) y el Ministerio de las TIC (MinTIC) – Agencia Nacional del Espectro (ANE) (Soporte)	Restricción de señal en prisiones y bloqueo de IMEI e IMSI	Los operadores de telecomunicaciones bloquearán los equipos terminales móviles y de dispositivos relacionados, con el fin de restringir las comunicaciones no autorizadas al interior de los establecimientos penitenciarios. Para tal fin se bloquearán el IMEI y el IMSI de la tarjeta SIM de los Equipos Terminales Móviles que hayan sido identificadas estableciendo comunicaciones no autorizadas dentro de un penal. El INPEC en articulación con el Ministerio de Justicia remitirá a los Operadores la información de geolocalización de los establecimientos penitenciarios, lo que permitirá a los operadores parametrizar las acciones de identificación de comunicaciones de telefonía móvil no autorizadas en las cárceles.	https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=157638
El Salvador	Decreto 953/2015 Reglamento técnico de la Ley especial contra el delito de extorsión / 2016	Superintendencia de Electricidad y Telecomunicaciones (SIGET) Ministerio de Justicia y Seguridad Pública	Restricción de señal en las prisiones	Los Operadores de Telecomunicaciones tendrán la obligación de adoptar y aplicar los procedimientos comerciales y soluciones técnicas que sean necesarios, para	https://www.acnur.org/fileadmin/Documentos/BDL/2016/10445.pdf

				<p>evitar la prestación de los servicios de tráfico de telecomunicaciones al interior de los centros penitenciarios, granjas penitenciarias o centros de internamiento para menores. Los Operadores de Telecomunicaciones están prohibidos de brindar servicios de todo tipo de tráfico de telecomunicaciones en los espacios físicos donde están ubicados los centros penitenciarios o centros de internamiento de menores, para lo cual estarán obligados a adoptar todas las medidas técnicas que sean necesarias. Dichos espacios físicos son establecidos por la SIGET en coordinación con el Ministerio de Justicia.</p>	
Honduras	Decreto 43/2015 CONATEL – Resolución 001/2016	Comisión Nacional de Telecomunicaciones (CONATEL) Secretaría de Estado	Bloqueadores y restricción de señal en las prisiones y “Dummy Cells”	<p>Se prohíbe la prestación de Servicios de Telecomunicaciones en los Establecimientos Penitenciarios y ordena a los Operadores de telecomunicaciones a implementar medidas técnicas que bloqueen la prestación de sus servicios de telecomunicaciones, dicha prohibición se extiende a cualquier</p>	<p>https://www.acnur.org/fileadmin/Documentos/BDL/2016/10421.pdf</p>

				<p>persona natural o jurídica que no cuente con título habilitante otorgado por CONATEL, además, en el artículo 11, se establece que los Operadores de Telecomunicaciones, están obligados a actualizar las soluciones técnicas para garantizar que no se brinden servicios de telecomunicaciones en los Centros Penitenciarios.</p>	
México	<p>Lineamientos de Colaboración entre Autoridades Penitenciarias y los Concesionarios de Servicios de Telecomunicaciones y Bases Técnicas para la Instalación y Operación de Sistemas de Inhibición.</p> <p>artículo 190 de la Ley Federal de Telecomunicaciones y Radiodifusión</p>	<p>Secretaría de Seguridad Pública, Instituto Federal de Telecomunicaciones y La Conferencia Nacional del Sistema Penitenciario.</p>	<p>Bloqueadores y restricción de señal en las prisiones</p>	<p>Los concesionarios de redes públicas de telecomunicaciones, deberán cancelar o anular de manera permanente las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen, dentro del perímetro de los establecimientos penitenciarios y centros juveniles, sin que excedan en ningún caso veinte metros fuera de las instalaciones de los centros o establecimientos penitenciarios a fin de garantizar la continuidad y seguridad de los servicios a los usuarios externos.</p> <p>Los operadores deberán colaborar con el Sistema Nacional de Seguridad Pública en el monitoreo de la</p>	<p>https://dof.gob.mx/nota_detalle_popup.php?codigo=5266201</p>

				funcionalidad u operatividad de los equipos utilizados para el bloqueo permanente de las señales de telefonía celular, de radiocomunicación, o de transmisión de datos o imagen.	
Panamá	Resolución AN 6295-Telco/2013	MNOs de Ministerio de Gobierno (Dirección de Seguridad Penitenciaria) de Autoridad Nacional de Servicios Públicos (ASEP)	Restricción de señal en prisiones seleccionadas	Los operadores deben suspender y restringir las emisiones y/o señales de los Servicios de Telefonía Móvil Celular, Comunicaciones Personales e Internet para uso Público, que se preste a través de tecnologías inalámbricas, dentro del Centro Penitenciario. Delimitar el polígono de restricción que corresponde al centro penitenciario (coordenadas geográficas)	https://www.asep.gob.pa/wp-content/uploads/telecomunicaciones/resoluciones/anno_6295_telco.pdf

Elaboración: DGPRC-MTC.

Como se puede observar, varios países han adoptado medidas para combatir el uso de teléfonos móviles y otras tecnologías de telecomunicaciones en establecimientos penitenciarios además de los bloqueadores de señales. Estas soluciones son complementarias o alternativas a los bloqueadores de señales y ofrecen oportunidades para mejorar la seguridad y el control dentro de los penales, así como mitigar el mal uso de los servicios de telecomunicaciones para actividades ilícitas.

Aunque algunas de estas soluciones han demostrado que pueden ser eficientes, se enfrentan a desafíos como la evolución tecnológica y la interferencia con las redes externas, por lo que la implementación debe ser cuidadosamente controlada y ajustada según las necesidades locales.

Si bien para evitar que los internos realicen actividades delictivas desde los establecimientos penitenciarios se han adoptado diversas medidas tales como la implementación de equipos bloqueadores o interferentes, así como el fortalecimiento de las medidas tecnológicas y operativas para la detección de objetos prohibidos al momento de ingreso a los establecimientos penitenciarios y centros juveniles; la lucha contra la emisión y recepción de comunicaciones

electrónicas y telefónicas ilegales en las cárceles, dado el rendimiento insuficiente de las soluciones implementadas hasta la fecha, especialmente frente a las tecnologías en continuo desarrollo (4G, 5G y Wi-Fi), y considerando finalmente el impacto de las especificidades técnicas y arquitectónicas de los establecimientos penitenciarios en los sistemas de detección y neutralización de comunicaciones ilegales, resulta necesario implementar medidas y/o mecanismos adicionales que complementen y coadyuven a las actualmente vigentes para prevenir y combatir esta problemática asociada a los altos índices de criminalidad en nuestro país¹⁶.

De las medidas implementadas por el Estado peruano, la principal para contrarrestar la problemática ha sido el uso de bloqueadores (*jammers*), en el marco del **Contrato Innominado de “Prestación de Servicios de Seguridad Tecnológica en las Prisiones” (CIPS)** —*Contrato APP (Asociación Público Privada)*, suscrito el año 2014 entre el MINJUSDH como Contratante y la Empresa PRISONTEC S.A.C. como Prestador; así como, con intervención del INPE — para bloquear las señales radioeléctricas en treinta y tres (33) establecimientos penitenciarios, a cambio de la exclusividad en el servicio de teléfonos públicos para los internos.

El numeral 2.3 de la Cláusula Segunda del mencionado contrato establece las principales actividades o prestaciones que constituyen el objeto de los derechos y obligaciones que asumen las partes, de acuerdo con lo siguiente:

- a) La implementación de un sistema de seguridad consistente en el bloqueo o inhibición de las señales radioeléctricas de: i) los servicios públicos móviles de Telefonía Móvil Celular, Comunicaciones Personales (PCS), ii) de Canales Múltiples de Selección Automática (Troncalizado), y iii) redes inalámbricas de área local Wifi, así como otros medios de comunicaciones no permitidos en los establecimientos penitenciarios que solicite el INPE.
- b) La prestación de un servicio de telefonía fija en la modalidad de teléfonos públicos, mediante aparatos, cabinas o locutorios telefónicos, todo ello con el software necesario para su correcto funcionamiento y operación bajo condiciones de seguridad para los usuarios y destinatarios de las llamadas, con el fin de cumplir el objeto del Contrato.

Cabe indicar que el proyecto comenzó en 2017. Conforme a la Cláusula Décima del referido contrato, tendrá una vigencia de veinticinco (25) años, contados a partir de la Fecha de Cierre (ver numeral 1.3.42 del contrato).. A continuación, se detalla el estado actual de la Prestación de Servicios de Seguridad Tecnológica, en la siguiente tabla.

Tabla N° 4: Estado actual de la Prestación de Servicios de Seguridad Tecnológica en las Prisiones¹⁷

Contrato Innominado de Prestación de Servicios “Prestación de Servicios de Seguridad Tecnológica en las Prisiones” (CIPS) y Adenda N° 1 y N° 2		
N°	Etapa Pre Operativa	Etapa Operativa

¹⁶ Extraído de la Exposición de Motivos del Decreto Legislativo N° 1688, páginas 11 y 12.

¹⁷ Información remitida por la Dirección General de Asuntos Criminológicos (DGAC) del MINJUSDH, mediante correo electrónico de fecha 06 de marzo de 2025.

	Establecimiento Penitenciaria (EP)	Periodo de Estudios		Periodo Instalación de Equipos	Periodo de Puesta en Marcha	Estado	Fecha: Constancia de Inicio de Operaciones	
		Periodo de Elaboración de ETE	Periodo de Aceptación de ETE	Estado	Estado			
1	EP Cañete	Culminado	Culminado	Culminado	Culminado	En Operación	06.07.2015	
2	EP Huaral	Culminado	Culminado	Culminado	Culminado	En Operación	14.09.2015	
3	EP Callao	Culminado	Culminado	Culminado	Culminado	En Operación	31.07.2017	
4	EP Ancón II	Culminado	Culminado	Culminado	Culminado	En Operación	31.07.2017	
5	EP Chincha	Culminado	Culminado	Culminado	Culminado	En Operación	31.07.2017	
6	EP Ancón I	Culminado	Culminado	Culminado	Culminado	En Operación	31.08.2017	
7	EP Castro Castro	Culminado	Culminado	Culminado	Culminado	En Operación	25.07.2018	
8	EP Huacho	Culminado	Culminado	Culminado	Culminado	En Operación	07.11.2017	
9	EP Ica	Culminado	Culminado	Culminado	Culminado	En Operación	20.04.2018	
10	EP Trujillo	Culminado	Culminado	Culminado	Culminado	En Operación	08.02.2018	
11	EP Lurigancho	Culminado	Culminado	Culminado	Culminado	En Operación	25.03.2019	
12	EP Chiclayo	Culminado	Culminado	Culminado	Culminado	En Operación	31.05.2019	
13	EP Chimbote	Culminado	Culminado	Culminado	Culminado	En Operación	01.10.2018	
14	EP Huaraz	Culminado	Culminado	Culminado	Culminado	En Operación	11.11.2019	
15	EP Tumbes	Culminado	Culminado	Culminado	Culminado	En Operación	13.11.2020	
16	EP Huancayo	Culminado	Culminado	Culminado	Culminado	En Operación	22.07.2021	
17	EP Huánuco	Culminado	Culminado	Culminado	Culminado	En Operación	13.01.2022	
	9 penales más desde el inicio de la gestión del SM							
18	EP Cajamarca	Culminado	Culminado	Culminado	Culminado	En Operación	26.09.2024	
19	EP Pto Maldonado	Culminado	Culminado	Culminado	Culminado	En Operación	03.10.2024	
20	EP Ayacucho	Culminado	Culminado	Culminado	Culminado	En Operación	09.10.2024	
21	EP Chanchamayo	Culminado	Culminado	Culminado	Culminado	En Operación	09.10.2024	
22	EP Tacna	Culminado	Culminado	Culminado	Culminado	En Operación	16.10.2024	
23	EP Tarapoto	Culminado	Culminado	Culminado	Culminado	En Operación	18.10.2024	
24	EP Moyobamba	Culminado	Culminado	Culminado	Culminado	En Operación	25.10.2024	
25	EP Puno	Culminado	Culminado	Culminado	Culminado	En Operación	16.10.2024	
26	EP Chachapoyas	Culminado	Culminado	Culminado	Culminado	En Operación	18.10.2024	

7 penales pendientes						
27	EP Cusco	Culminado	Culminado	Culminado	En Proceso	
28	EP Muj. Chorrillos	Culminado	Culminado	Culminado	En Proceso	
29	EP Juliaca	Culminado	Culminado	Culminado	En Proceso	
30	EP Pucallpa	Culminado	Pendiente			
31	EP Iquitos	Culminado	Pendiente			
32	EP Piura	Culminado	Pendiente			
33	EP Arequipa	Culminado	Pendiente			

Elaboración: MINJUSDH.

Por otra parte, el INPE indica que aquellos establecimientos penitenciarios que no cuentan con equipos bloqueadores, a la fecha no tienen instalados otros sistemas para impedir las comunicaciones ilegales; por lo tanto, ninguna empresa tiene este servicio, a excepción del CIPS suscrito entre el MINJUSDH y PRISONTEC S.A.C. con intervención del INPE, que comprende la instalación de equipos bloqueadores en treinta y tres (33) establecimientos penitenciarios, de los cuales veintiséis (26) se encuentran instalados en etapa operativa, y tres (03) instalados en etapa pre operativa y cuatro (04) pendientes de instalación¹⁸.

De otro lado, se menciona que el INPE gestiona y administra el establecimiento penitenciario de Cochamarca que dispone del sistema de bloqueo implementado, mediante licitación pública, entre la empresa DESCA y la Oficina de Infraestructura Penitenciaria¹⁹.

Asimismo, el INPE indica que en el establecimiento penitenciario de Cochamarca fue implementado en el año 2019 un Sistema de Gestión de Llamadas el cual fue parte de un Proyecto de Inversión a cargo de la Oficina de Infraestructura Penitenciaria, el mismo que a la fecha requiere actualización por vigencia tecnológica debido a la operación de nuevas bandas de frecuencias en la que operan las empresas que prestan servicios de telefonía móvil; dicha actualización no ha sido atendida por limitaciones presupuestales²⁰.

En relación a este punto el INPE ha precisado que en el establecimiento penitenciario de Cochamarca se encuentra instalado un Sistema de Inhibición y Gestión de Llamadas; sin embargo, precisa que dicho sistema se encuentra inoperativo por falta de mantenimiento y actualización de tecnología; por lo que, no viene operando en la actualidad. La ubicación georreferenciada de dicho penal en el siguiente cuadro²¹:

Departamento	Provincia	Distrito	Dirección	X	Y	E.P.
Pasco	Pasco	Vicco	Cochamarca 19410	-76.2863	-10.8905	Cochamarca

Fuente: Unidad de Estadística INPE

De otro lado, es relevante señalar que aún no se han implementado sistemas de bloqueo de señales radioeléctricas en los centros juveniles a cargo del

¹⁸ De la información remitida por la Dirección General de Asuntos Criminológicos (DGAC) del MINJUSDH, mediante correo electrónico de fecha 06 de marzo de 2025.

¹⁹ Extraído de la Exposición de Motivos del Decreto Legislativo N° 1688, p. 18.

²⁰ Igualmente, de la información remitida por la Dirección General de Asuntos Criminológicos (DGAC) del MINJUSDH, mediante correo electrónico de fecha 06 de marzo de 2025.

²¹ Ídem.

PRONACEJ, lo que limita significativamente la capacidad para restringir las comunicaciones ilícitas en estos entornos²².

Sin perjuicio a lo expuesto, cabe mencionar que, en el marco de la lucha contra las comunicaciones ilegales en establecimientos penitenciarios y centros juveniles, se estima necesario que dichos recintos cuenten con sistemas de restricción de señales de comunicaciones, lo que permitirá que esta normativa se ejecute de manera óptima y/o eficiente, al complementarse con medidas y/o mecanismos que impidan a los internos establecer comunicaciones no autorizadas, y velar por el cumplimiento de las obligaciones establecidas a las empresas operadoras.

5.3. Medidas consideradas para la solución del problema público

5.3.1. Medidas orientadas a la restricción de señales radioeléctricas de los servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles a nivel nacional

De acuerdo con el numeral 8.1 del artículo 8 del Decreto Legislativo N° 1688, las empresas operadoras restringen las señales radioeléctricas de los servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles del país a nivel nacional, salvo excepciones por necesidades de seguridad cuando así lo determine la entidad competente en el ámbito de sus funciones y/o atribuciones. Asimismo, se indica que dicha restricción de señales radioeléctricas se realizará conforme a lo establecido en el Reglamento.

Pues bien, de las reuniones sostenidas con las empresas operadoras y con la empresa que gestiona el sistema de los equipos bloqueadores en el marco de la “Mesa técnica para implementar medidas orientadas a prevenir las comunicaciones ilegales”, se llegó a la conclusión de que es necesario una coordinación constante y fluida entre ambos actores para lograr limitar las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles y, a la vez, garantizar el acceso a los servicios de telecomunicaciones de la población aledaña a dichos lugares.

En este punto, se ha considerado la aplicación de medidas para establecimientos penitenciarios y centros juveniles, en tanto cuenten con sistemas de restricción de señales de comunicaciones. Asimismo, tratándose de centros juveniles, si bien aún no cuentan con estos sistemas, existe la posibilidad de que a futuro el Estado adopte la decisión de implementarlos, por lo que, con una mirada prospectiva, a fin de que la norma sea aplicable en el tiempo si ello ocurriera, también se ha considerado a los centros juveniles.

En primera instancia, se ha considerado establecer que la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones coordinen y acuerden los parámetros de señal y sus respectivos valores, de tal forma que se restrinjan las comunicaciones ilegales en dicho ámbito y, a su vez, no se genere afectación a los servicios públicos de telecomunicaciones de las poblaciones cercanas a estos. Dichos parámetros y sus respectivos valores acordados serán verificados por la Dirección de Fiscalización de Cumplimiento de Títulos Habilitantes en Comunicaciones (en adelante, la DFCTH) de la Dirección General de Fiscalizaciones y Sanciones en Comunicaciones del MTC (en adelante, la DGFSC) en el límite de la zona restringida y de alta seguridad.

²² Extraído de la Exposición de Motivos del Decreto Legislativo N° 1688, p. 19.

Lo antes indicado obedece a que se considera más eficiente que las partes antes mencionadas lleguen a un acuerdo, atendiendo a que ambas conocen el funcionamiento de sus redes; además, dependiendo de las particularidades de cada establecimiento penitenciario o centro juvenil, como ubicación, infraestructura, población aledaña; así como, el tipo de banda de las señales radioeléctricas que emiten las estaciones de telecomunicaciones cercanas, entre otros, que condicionan los parámetros que se deben verificar.

Es de resaltar que los parámetros que acuerden las partes deben garantizar que no progresen o no sea posible que se concreten las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, cautelando en todo momento el derecho de acceso a los servicios de telecomunicaciones de las personas que viven alrededor de dichos establecimientos.

En caso de falta de acuerdo entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones, se ha establecido que aplican los parámetros recogidos en el Protocolo Técnico que regula las condiciones de operación de los equipos bloqueadores de señales radioeléctricas y de los servicios de telecomunicaciones en los exteriores de los establecimientos penitenciarios, aprobadas mediante Resolución Ministerial Nº 954-2016-MTC/01.03 (en adelante, el Protocolo Técnico).

Ahora bien, precisamente a efectos de establecer parámetros acordes con las tecnologías móviles actuales y que contemplen la interacción entre las señales que emiten los equipos bloqueadores y las estaciones radioeléctricas, se ha considerado pertinente modificar los artículos 2 y 6 del Protocolo Técnico.

Con relación al artículo 2 del Protocolo Técnico, la referida modificación normativa contempla la extensión del ámbito de aplicación a los centros juveniles.

Asimismo, respecto al artículo 6 del Protocolo Técnico, se propone la variación de los parámetros técnicos que deben cumplir las empresas operadoras y la empresa que gestiona el sistema de restricción de señales, de acuerdo con lo siguiente:

- Numeral 6.1 del artículo 6 del Protocolo Técnico: Las empresas operadoras restringen la emisión de su señal radioeléctrica de los servicios públicos de telecomunicaciones hacia los establecimientos penitenciarios, centros juveniles y zonas restringidas y de alta seguridad, de tal forma que cumpla con los siguientes parámetros:

Tecnología	Nivel de señal
2G	RxLev < -100 dBm
3G	RSCP (Received Signal Code Power) < -100 dBm
4G	RSRP (Reference Signal Received Power) < -115 dBm
5G	SS-RSRP (Synchronization Signal Reference Power) < X0 dBm

Donde: X0 será definido por el operador, de tal manera que restrinja las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles

- Numeral 6.2 del artículo 6 del Protocolo Técnico: 6.2 Los equipos bloqueadores y los equipos de las Operadoras garantizan un nivel de relación del valor pico de la señal deseada con la señal no deseada no mayor a -7 dB, según corresponda.

En caso durante el proceso de medición no se detecte señal deseada, se toma como referencia de señal deseada -100 dBm.

- Numeral 6.3 del artículo 6 del Protocolo Técnico: Los parámetros establecidos en los numerales 6.1 y 6.2 son exigibles a partir del borde externo de la zona de intangibilidad o zona restringida y de alta seguridad, comprendiendo a toda el área de dicha zona y de los establecimientos penitenciarios y centros juveniles.

Sobre el particular, actualmente, en el numeral 6.1 del artículo 6 del Protocolo Técnico se establece que *“Los equipos bloqueadores y los equipos de las Operadoras garantizan un nivel de recepción menor o igual a -100 dBm en el límite de la Zona de Intangibilidad”*, es decir, se establece un umbral de nivel de señal, medido como RSSI.

Cabe indicar que para establecer los nuevos parámetros en el Numeral 6.1 del artículo 6 del Protocolo Técnico, se ha tomado como referencia la Norma de Requerimientos de Información Periódica, aprobada mediante Resolución de Consejo Directivo N° 00043-2022-CD/OSIPTEL, modificada mediante Resolución de Consejo Directivo N° 00151-2023-CD/OSIPTEL, que estableció dos categorías de cobertura: cobertura garantizada y capacidad adicional de red.

Así, según las referidas normas, Cobertura Garantizada se define como aquella área geográfica, determinada por la empresa operadora, donde esta ofrece el servicio móvil e internet fijo inalámbrico garantizando el cumplimiento de los valores objetivos de todos los indicadores de calidad de servicio establecidos en el Reglamento General de Calidad de los Servicios Públicos de Telecomunicaciones; mientras que, la Capacidad Adicional de red se define como aquella área geográfica que se extiende a partir del área de cobertura garantizada y donde los usuarios podrían acceder a los servicios móviles e internet fijo inalámbrico, debido a las características de propagación de las señales electromagnéticas.

De esta manera, los nuevos parámetros establecidos en el Protocolo Técnico, exigen que, en el área de los establecimientos penitenciarios, centros juveniles y las zonas restringidas y de alta seguridad, la señal de las estaciones radioeléctricas no alcance siquiera los valores de la Capacidad Adicional, de tal forma que en dichas zonas se encuentren limitadas las comunicaciones móviles.

Asimismo, de acuerdo con los nuevos valores contemplados en el Protocolo Técnico, se ha considerado que para las redes 4G (LTE) y 5G (NR) la medida de RSRP tiene mayor relevancia que la RSSI, ya que nos brinda una medida más precisa de la conectividad que tiene un dispositivo de usuario (UE) con una estación base. En efecto, los UEs censan constantemente la RSRP a fin de medir la potencia de señal de la celda a la que se encuentran registrados y de sus vecinos para poder realizar el *handover*, de ser el caso; por otro lado, el parámetro RSSI no es reportado por los UEs.

En esa misma línea, respecto a la obligación que se ha establecido en el numeral 6.2 del artículo 6 del Protocolo Técnico, cabe indicar que la relación entre la señal deseada y la señal no deseada, es transversal a todas las tecnologías móviles y además, en algunas redes de telecomunicaciones, posee una correlación con el throughput²³, por lo tanto, puede considerarse como un factor que brinda una idea sobre el acceso y/o restricción al servicio de telecomunicaciones móviles.

²³ Ghosh, A., & Ratasuk, R. (2011). *Essentials of LTE and LTE-A*. Cambridge: Cambridge University Press., pp 97 y 98. En este libro se toma como referencia el estándar 3GPP TS 36.213 (ETSI TS 136 213) para llegar a una relación aproximada entre la modulación, el CQI y el SINR en una red de telecomunicaciones LTE.

Cabe destacar que, para que las empresas operadoras cumplan los parámetros acordados con la empresa que gestiona los sistemas de restricción de señales o los establecidos en el Protocolo Técnico, de ser necesario, deben realizar las adecuaciones técnicas en sus estaciones radioeléctricas, entre otras, cambios de tilt, azimut, altura, potencia; así como, inclusive, efectuar el reemplazo de estaciones.

Asimismo, las nuevas estaciones radioeléctricas que instalen las operadoras o la implementación de nuevas tecnologías o actualizaciones sobre estaciones existentes, deben cumplir con la obligación de restricción de sus señales radioeléctricas, debiendo ceñirse a los parámetros técnicos antes mencionados.

Por otro lado, se ha planteado que la empresa operadora remita el listado de las celdas de las estaciones radioeléctricas, cuyas señales irradian hacia los establecimientos penitenciarios y centros juveniles, incluyendo la tecnología y frecuencia de operación de cada celda, ello con la finalidad de que la DFCTH cuente con la información técnica necesaria para realizar las acciones de fiscalización sobre el cumplimiento de la restricción de señales radioeléctricas. Para ello, se ha previsto un plazo de treinta (30) días calendario de publicado el reglamento.

Asimismo, dado que la red de telecomunicaciones es dinámica y se encuentra en constante cambio, la información que remita la empresa operadora se irá modificando en el tiempo y quedará desfasada para efectos de las acciones de fiscalización que se requieran realizar, por lo que se prevé que la empresa operadora informe a la DFCTH la instalación de nuevas celdas y la actualización de las existentes, cuyas señales irradian hacia los establecimientos penitenciarios y centros juveniles, dentro de los cinco (05) días hábiles de haber sido efectuados.

Aunado a lo anterior, las empresas operadoras deben resguardar los registros logs de cambios, actualizaciones y/o modificaciones de las celdas de las estaciones radioeléctricas, cuyas señales irradian hacia los establecimientos penitenciarios y centros juveniles, por un período de por treinta y seis (36) meses, con la finalidad de que se efectúe la debida supervisión y/o fiscalización por parte de la DFCTH. Para el establecimiento de dicho plazo, se ha tomado como referencia el plazo que se establece en otras normativas del sector sobre conservación de la información, tal como el previsto en el literal e) del artículo 16 de la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones – OSIPTEL y el primer párrafo de la Segunda Disposición Complementaria Final del Decreto Legislativo N° 1182, que establecen periodos similares.

Con relación a la verificación de las obligaciones estipuladas, en el Reglamento se ha previsto que en caso durante una acción de fiscalización, la DFCTH constatará que la empresa operadora no cumple con restringir su señal radioeléctrica, ya sea la acordada con la empresa que gestiona el sistema de restricción de señales o la establecida en el Protocolo Técnico, comunicará a dicha empresa, mediante el acta correspondiente, con copia a la empresa que gestiona el sistema de restricción de señales de comunicaciones, el MINJUSDH y/o al INPE, según corresponda, a efectos de que la operadora adopte las acciones para la restricción de la señal.

Para ello, se ha considerado pertinente diferenciar el plazo de cumplimiento de la restricción de señales, en función de las actividades que debe realizar la empresa operadora ya sea en campo o en gabinete. Así, se establece que la empresa operadora adopta las acciones correspondientes, en el plazo de dos (02) días calendarios, tratándose de cambios lógicos y, de cinco (05) días calendarios, tratándose cambios físicos.

Sobre el particular, se entiende por cambio lógico aquella modificación del contenido o configuración del sistema o dispositivo sin alterar su estructura física, como, por ejemplo: cambio de software, reconfiguración, actualización de parámetros, entre otros. Asimismo, se entiende por cambio físico a la modificación del hardware o de la infraestructura física, como, por ejemplo, el movimiento de antenas, agregación de dispositivos, cableado nuevo, entre otros.

Asimismo, la empresa operadora debe presentar a la DFCTH dentro de las cuarenta y ocho (48) horas siguientes a haber efectuado dichas acciones, las evidencias que demuestren el cumplimiento de la restricción de su señal radioeléctrica.

De otro lado, se debe considerar que, muchos de los establecimientos penitenciarios y centros juveniles se encuentran en, o muy cerca, de áreas urbanas y pobladas; por lo que al restringir las señales radioeléctricas hacia los mismos, se corre el riesgo de generar cierta afectación al acceso y/o calidad de los servicios de telecomunicaciones de las poblaciones aledañas; así como a la cobertura de los mismos; debido a esto, se ha considerado pertinente mantener una zona de exclusión especial, que ahora se encontrará prevista en el numeral 6.4 del artículo 6 del Protocolo Técnico y conforme a un nuevo parámetro.

De esta forma, en el caso de los establecimientos penitenciarios, dicha zona de exclusión especial, inicia desde el borde externo de la zona de intangibilidad hasta la distancia de 200 metros a su alrededor.

Cabe mencionar que, a diferencia del parámetro actualmente establecido en el Protocolo Técnico que se basaba en dBm, ahora se ha considerado conveniente establecer la zona de exclusión especial en base a una distancia específica de los establecimientos penitenciarios y centros juveniles, a fin de contar con un parámetro objetivo que permita tener certeza sobre el ámbito que comprende dicha zona.

En ese sentido, la distancia que se ha considerado para la zona de exclusión especial replica la distancia considerada para la zona restringida y de alta seguridad, toda vez que es necesario mantener un área de flexibilidad para la convivencia de las señales emitidas por las estaciones radioeléctricas y los quipos bloqueadores.

En la misma línea, en el caso de los centros juveniles, la zona de exclusión especial comprende 400 metros alrededor del perímetro de dichos centros, a fin de que guarde consistencia con la distancia considerada para los establecimientos penitenciarios.

Por tanto, la zona restringida y de alta seguridad como la zona de exclusión especial, se consideran excluidas de los parámetros de cobertura o de calidad del OSIPTEL, así como, de la verificación de obligaciones contractuales y/o administrativas aplicables.

Por otro lado, en el caso de los establecimientos penitenciarios o centros juveniles que no cuentan con sistemas de restricción de señales de comunicaciones, en la segunda disposición complementaria final se ha establecido que no resultan exigibles los parámetros establecidos en el Protocolo Técnico hasta que dichos sistemas hayan sido implementados y se encuentren operativos. Ello se debe a que, en dichos casos, no existe la posibilidad de que se llegue a un acuerdo que permita conciliar el interés de la prestación de servicios públicos de telecomunicaciones y la restricción de señales radioeléctricas, por lo que una eventual restricción de señales de comunicaciones para impedir las comunicaciones desde establecimientos penitenciarios y centros juveniles, ocasionaría un gran impacto negativo en las poblaciones aledañas a dichos recintos, considerando que estos se encuentran en zonas urbanas altamente pobladas.

No obstante, para dichos casos resultan aplicables las demás medidas previstas en el Reglamento para evitar que se concreten comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, tales como, las medidas de monitoreo de red y de uso prohibido del servicio. En ese sentido, resulta de suma relevancia que todos los establecimientos penitenciarios y centros juveniles cuenten con algún sistema de restricción de señales de comunicaciones para que las medidas establecidas en el Reglamento sean eficaces.

Finalmente, en el Reglamento se ha establecido que la empresa que gestiona el sistema de restricción de señales de comunicaciones, bajo responsabilidad, brinda a la DFCTH el acceso remoto al sistema de gestión de los equipos bloqueadores u otros sistemas instalados en los establecimientos penitenciarios y centros juveniles, según corresponda, en perfil de lectura.

Dicho acceso es relevante a fin de que la DFCTH pueda realizar las acciones de fiscalización para verificar las características de funcionamiento, bandas de frecuencia, niveles de potencia, entre otros, en el marco de sus competencias.

Asimismo, a fin de garantizar el cumplimiento de la citada obligación, se ha establecido en el Reglamento que, tratándose de la empresa que gestiona el sistema de restricción de señales de comunicaciones, dicho acceso es condición para que la DFCTH otorgue la constancia inicial de no interferencia de acuerdo con el Protocolo Técnico.

En la misma línea de ideas, se ha propuesto que el software -del sistema de gestión- de la empresa que gestiona el sistema de restricción de señales de comunicaciones, cuyo acceso brinda a la DFCTH, almacena los logs de cambios, eventos, alarmas, actualizaciones y/o modificaciones de las señales radioeléctricas, que irradian en los establecimientos penitenciarios y centros juveniles. Atendiendo a que la gestión y/u operación de los sistemas de restricción de señales de comunicaciones en establecimientos penitenciarios y centros juveniles puede estar sujeta a contratos específicos, la obligación de almacenar logs de cambios, eventos, alarmas, actualizaciones y/o modificaciones de las señales radioeléctricas, debe ser cumplida en consonancia con las condiciones, alcances y responsabilidades asumidas en dichos contratos. En ese sentido, la exigibilidad de la mencionada obligación procede únicamente en aquellos casos en que el contrato celebrado lo contemple, como parte de las prestaciones a cargo de la empresa la provisión, operación o mantenimiento de los sistemas de restricción de señales de comunicaciones.

5.3.2. Mecanismos que impidan las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles, así como que coadyuven a los sistemas y/o equipos de seguridad tecnológica implementados por las entidades competentes

De acuerdo con el numeral 8.2 del artículo 8 del Decreto Legislativo N° 1688, las empresas operadoras adoptan mecanismos que impidan las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles, así como, que coadyuven a los sistemas y/o equipos de seguridad tecnológica implementados por las entidades competentes. Asimismo, se establece que los mecanismos son establecidos en el Reglamento de dicha norma.

Al respecto, en el Reglamento se ha previsto la obligación de la empresa operadora de realizar las coordinaciones con la empresa que gestiona el sistema de restricción de señales, puesto que, como se ha indicado previamente, se considera que el acuerdo entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales es lo más eficiente para asegurar que no se concreten las comunicaciones

ilegales desde establecimientos penitenciarios o centros juveniles y, a su vez, no se genere afectación a los servicios públicos de telecomunicaciones de las poblaciones aledañas a estos.

En este contexto, cabe mencionar que, de acuerdo con las reuniones sostenidas en el marco de la “Mesa Técnica para implementar medidas orientadas a prevenir las comunicaciones ilegales”, se indicó que actualmente ciertas empresas operadoras móviles ya vienen coordinando con la empresa que gestiona los sistemas de bloqueadores sobre aspectos técnicos, lo cual facilita el bloqueo de las comunicaciones ilegales, situación que no ocurre con aquellas empresas operadoras móviles que no han mostrado predisposición para realizar tales coordinaciones.

Asimismo, en el Reglamento se ha previsto que dichas coordinaciones pueden ser por iniciativa de la empresa operadora o de la empresa que gestiona el sistema de restricción de señales, siendo que, en cualquiera de los casos, la empresa operadora debe comunicar a la DFCTH el inicio de las referidas coordinaciones.

Adicionalmente, una vez que se haya adoptado el acuerdo, la empresa operadora, comunica el acuerdo a la DFCTH y la UFSCIPS, en el plazo de cinco (05) días hábiles de haber sido adoptado, el contenido del mismo, el cual debe incluir los parámetros técnicos, físicos y lógicos establecidos para cada estación base celular que emitan señales radioeléctricas hacia los establecimientos penitenciarios y centros juveniles, así como, los parámetros técnicos, físicos y lógicos de los bloqueadores. Asimismo, cada acuerdo debe acompañarse por las pruebas de desempeño de red del entorno donde se verifique las condiciones de cobertura.

La información antes mencionada es de suma relevancia a fin de que la DFCTH pueda efectuar la verificación sobre los parámetros acordados, esto es, que los mismos efectivamente garantizan que no se pueda realizar las comunicaciones desde los establecimientos penitenciarios y centros juveniles y, a su vez, no se afecte el derecho al acceso a las telecomunicaciones de las poblaciones aledañas; así como, para realizar la supervisión del cumplimiento de los parámetros acordados.

Asimismo, se ha considerado que el acuerdo adoptado entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones también se comunique a la Unidad Funcional de Supervisión del Contrato Innominado de Prestación de Servicios (UFSCIPS), Esto permitirá que la UFSCIPS realice sus actividades de supervisión considerando dichos acuerdos y verifique su cumplimiento, garantizando así la prevención de comunicaciones ilegales desde los establecimientos penitenciarios o centros juveniles

En este punto resulta importante observar la predisposición de la empresa operadora y de la empresa que gestiona el sistema de restricción de señales de comunicaciones de ser partícipes de las coordinaciones con el ánimo de arribar a un acuerdo, lo cual que de concretarse debe informarse a la DFCTH y UFSCIPS en un plazo de cinco (05) días hábiles de haber sido adoptado, incluyendo los aspectos precisados en el Reglamento, determinándose que, cualquier modificación al acuerdo adoptado es comunicada a la DFCTH en el mismo plazo antes mencionado.

En el caso que, no se llegara a un consenso, entonces rigen tanto para la empresa operadora como para la empresa que gestiona el sistema de restricción de señales de comunicaciones, los parámetros establecidos en el Protocolo Técnico.

Asimismo, se considerará que las partes no han llegado a un acuerdo cuando hayan transcurrido treinta (30) días calendario desde el inicio de las coordinaciones sin arribar

a un común entendimiento, esto a fin de evitar que se prolongue de forma incierta dichas coordinaciones y no se cuente con parámetros claros que deben ser cumplidos por la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones.

Por otro lado, como se ha indicado previamente en la presente Exposición de Motivos, las soluciones implementadas respecto a la lucha contra las comunicaciones ilegales, a la fecha han resultado insuficientes, por lo que se estima necesario implementar medidas y/o mecanismos adicionales que complementen y coadyuven a las actualmente vigentes para prevenir y combatir esta problemática asociada a los altos índices de criminalidad en nuestro país.

Por tal motivo, en el Reglamento, se ha establecido que la empresa operadora implementa medidas de monitoreo permanente de su red de telecomunicaciones, en base a niveles de indicadores de nivel de ruido, potencia de recepción, throughput, entre otras, que coadyuvará a determinar la funcionalidad u operatividad de los sistemas de restricción de señales de comunicaciones instalados en los establecimientos penitenciarios y centros juveniles.

Es importante mencionar que, en nuestro país, el sistema de bloqueadores de señal es el único sistema de restricción con el que se cuenta en la actualidad²⁴, por lo que para lograr una restricción de las comunicaciones que se realizan desde los establecimientos penitenciarios y centros juveniles, es necesario que este sistema se encuentre operando en condiciones óptimas. Por ello, se considera que las empresas operadoras, en sus centros de gestión y monitoreo de red y a través del seguimiento de ciertos indicadores, como, por ejemplo, de nivel de ruido (SNR, SINR, etc.), potencia de recepción (uno de ellos es la potencia de banda ancha recibida – RTWP), contadores de interferencia u otros indicadores, puedan coadyuvar en el monitoreo de los equipos bloqueadores.

En ese sentido, si producto del monitoreo antes mencionado, la empresa operadora advierte parámetros inusuales, entendiéndose estos como aquellas métricas que se desvían significativamente del comportamiento o valor normal o esperado de la misma y que, por ende, pueden estar relacionadas con una falla o actividad anómala, que indique un deficiente funcionamiento u operatividad de los equipos de bloqueo, debe comunicar al MTC, al MINJUSDH y al INPE dentro de las veinticuatro horas (24) de detectada dicha situación, a fin de que adopten las acciones pertinentes dentro del marco de sus competencias.

Cabe indicar que el plazo antes mencionado, obedece a que es relevante un rápido accionar que permita prevenir que se efectúen las comunicaciones ilegales desde establecimientos penitenciarios, puesto que, si los equipos bloqueadores presentan un deficiente funcionamiento u operatividad, ello podría implicar una vulnerabilidad que posibilite la concreción de las referidas comunicaciones.

Asimismo, se propone que las empresas operadoras reporten a la DFCTH mensualmente los resultados del monitoreo realizado de cada día del mes correspondiente, a fin de que en base a la información reportada se pueda verificar el cumplimiento de la obligación.

Por otro lado, en el Reglamento se ha contemplado que la empresa operadora implemente mecanismos de monitoreo permanente de red que realicen seguimiento de los accesos y/o intentos de conexión a su red que se encuentren dentro del área de los establecimientos penitenciarios y centros juveniles.

²⁴ Excepto el sistema instalado en el establecimiento penitenciario de Cochamarca.

En este punto, se solicita que la empresa operadora obtenga información que se encuentra disponible en las herramientas de crowdsourcing y análisis de sistemas de geolocalización para identificar actividad inusual de usuarios en la red de telecomunicaciones como, por ejemplo, intentos de conexión a la red, tiempo y usos de datos en distintas tecnologías, tráfico de voz o datos, entre otros. Un caso en particular, es que puede tenerse un grupo de dispositivos en el área del penal que únicamente se conectan empleando la red de datos, mas no la red de voz.

Sobre el particular, debe tenerse en cuenta que el numeral 4.3 del artículo 4 del Decreto Legislativo N° 1182, Decreto Legislativo que regula el uso de los datos derivados de las telecomunicaciones para la identificación, localización y geolocalización de equipos de comunicación, en la lucha contra la delincuencia y el crimen organizado, estipula la obligación de los concesionarios de servicios públicos de telecomunicaciones a brindar los datos de localización, geolocalización o rastreo de manera inmediata y oportuna a la unidad especializada de la Policía Nacional del Perú.

En la misma línea, el Decreto Legislativo N° 1590, Decreto Legislativo que aprueba disposiciones para la implementación, operación y mantenimiento de la Central Única de atención de emergencias, urgencias e información mediante un número único telefónico 911 - Central 911, en el artículo 11, se enumeran las obligaciones de las empresas operadoras, entre ellas se indica que deben implementar, adecuar y/o interconectar los sistemas de geolocalización, además de obtener y compartir los datos de la geolocalización.

En base a las precitadas normas, se considera que las empresas operadoras realicen un monitoreo empleando herramientas de geolocalización a fin de identificar usuarios que hagan uso de los servicios públicos de telecomunicaciones desde el interior de los establecimientos penitenciarios y centros juveniles.

Al igual que para el caso anterior, si producto del monitoreo antes mencionado, la empresa operadora advierte parámetros inusuales que brinden indicios de acceso y/o intentos de conexión a su red dentro de los establecimientos penitenciarios o centros juveniles, debe comunicar al DFCTH, MINJUSDH, INPE y al OSIPTEL dentro de las veinticuatro (24) horas de detectada dicha situación, a fin de que tales entidades adopten las acciones pertinentes dentro del marco de sus competencias.

Cabe indicar que el plazo antes mencionado, obedece a que es relevante un rápido accionar que posibilite evitar que se efectúen las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, puesto que, si por ejemplo, existen intentos de conexión a la red de la empresa operadora, ello podría implicar que dentro del establecimiento penitenciario existen equipos terminales móviles. En este caso, la empresa operadora debe comunicar a las entidades correspondientes, a fin de que se realicen las actividades como requisas u optimización en los sistemas de restricción de señales de comunicaciones.

Asimismo, al igual que en el caso precedente, se propone que las empresas operadoras reporten a la DGFSC mensualmente los resultados del monitoreo realizado de cada día del mes correspondiente, a fin de que en base a la información reportada se pueda verificar el cumplimiento de la obligación.

Finalmente, se ha establecido que, dentro del plazo de quince (15) días hábiles de la entrada en vigencia del presente reglamento, la DFCTH, el MINJUSDH, el INPE y el OSIPTEL, establecen los medios idóneos a fin de que la empresa operadora cumpla con realizar la comunicación establecida en los numerales 6.4 y 6.6.

5.3.3. Sobre el uso prohibido del servicio

Conforme al artículo 40 del Texto Único Ordenado del Código de Ejecución Penal, aprobado mediante el Decreto Supremo N° 003-2021-JUS (en adelante, el TUO del Código de Ejecución Penal), el interno puede comunicarse periódicamente, en forma oral y escrita y en su propio idioma, con sus familiares, amigos, representantes diplomáticos, organismos e instituciones de asistencia penitenciaria.

En esa línea, el artículo 37 del Reglamento del Código de Ejecución Penal aprobado por Decreto Supremo N° 015-2023-JUS dispone que, la Administración Penitenciaria implementará la instalación de teléfonos públicos exclusivamente en cabinas con accesos comunes en los establecimientos penitenciarios, excepto en los de Régimen Cerrado Especial de máxima seguridad, estableciendo que, se encuentra prohibido por parte de los internos el uso de cualquier otro servicio de telecomunicaciones que permita la transmisión de voz y/o datos, distinto a los teléfonos públicos y locutorios instalados para tal efecto.

Asimismo, el mencionado dispositivo estipula que, las comunicaciones que se efectúen utilizando los servicios de telecomunicaciones, transgrediendo el mismo, constituyen comunicaciones ilegales no amparadas por el marco legal vigente, y dispone que está prohibido el ingreso a los establecimientos penitenciarios de equipos terminales, y sus componentes, correspondientes a los servicios de telecomunicaciones, tales como equipos celulares, satelitales, radios transceptores, y cualquier otro que permita la transmisión de voz y/o datos.

De otro lado, el artículo 161 del Reglamento del Código de Responsabilidad Penal de Adolescentes, aprobado mediante Decreto Legislativo N° 1348 aprobado por Decreto Supremo N° 004-2018-JUS, establece que, está prohibido el uso de cualquier otro servicio de telecomunicaciones que permita la transmisión de voz y/o datos, distinto a los teléfonos públicos o las cartas; así como, está prohibido el ingreso de equipos terminales y sus componentes, correspondientes a los servicios de telecomunicaciones, tales como equipos celulares, satelitales, radios transceptores y cualquier otro que permita la transmisión de voz y/o datos.

En ese marco, en aras de implementar medidas para erradicar el mal uso de los servicios de telecomunicaciones, mediante el Decreto Legislativo N° 1688, se reguló las obligaciones y sanciones administrativas para las empresas operadoras de servicios públicos de telecomunicaciones en relación con las comunicaciones ilegales en establecimientos penitenciarios y centros juveniles.

Es así como el referido decreto ha regulado obligaciones a las empresas operadoras respecto al uso no autorizado de servicios públicos de telecomunicaciones en establecimientos penitenciarios y centros juveniles, considerando que las comunicaciones que se generan desde dichos establecimientos representan una amenaza significativa para la seguridad pública, toda vez que facilitan la comisión de actos delictivos como la extorsión o estafas, entre otros.

Si bien es cierto las empresas operadoras han venido realizando la identificación y corte del servicio móvil que se vendría utilizando desde establecimientos penitenciarios, como se ha indicado previamente, existen diferencias entre la cantidad de cortes de servicio realizados por cada una de dichas empresas, lo cual podría explicarse por diversos factores ajenos al control de las mismas, pero también podría evidenciar un

cumplimiento deficiente de la medida de corte de servicio y/o bloqueo de equipos terminales móviles, lo que hace necesario una revisión de las disposiciones por uso prohibido del servicio.

Aunado a ello, también se ha identificado el uso de otros servicios públicos dentro de los establecimientos penitenciarios como el de acceso a internet fijo, a fin de realizar comunicaciones desde dichos establecimientos, lo cual no se había contemplado en la regulación precedente.

En tal sentido, el artículo 7 del Reglamento desarrolla los escenarios en los que se configura el uso prohibido de los servicios públicos de telecomunicaciones, para lo cual, se contempla que cualquier servicio de telecomunicaciones, sea de voz, datos o mensajería que sea utilizado dentro de establecimientos penitenciarios o centros juveniles, distintos de los contratados por el INPE y el PRONACEJ sea calificado como uso prohibido.

Cabe precisar que se entiende por servicios de telecomunicaciones contratados por el INPE y/o el PRONACEJ, a los que puedan contratar dichas entidades para el uso de su personal y sus propias necesidades dentro de dichos recintos; así como, también a los teléfonos públicos legalmente instalados para el uso de los internos.

Asimismo, en el Reglamento se plantea incluir el acceso a los servicios públicos de telecomunicaciones de voz, datos y mensajería no autorizados a través de conexión directa o indirecta a la red de telecomunicaciones, con la finalidad de comprender al uso del Wi-Fi dentro de los establecimientos penitenciarios y centros juveniles.

Asimismo, es preciso considerar que se considera que el uso de servicios de telecomunicaciones para extender señales de telecomunicaciones hacia centros penitenciarios o centros juveniles, a través de cualquier dispositivo que permita la conexión directa o indirecta a la red de telecomunicaciones, como por ejemplo, utilizando señales inalámbricas (señales 2G, 3G, 4G, 5G, u otras tecnologías móviles, señales WIFI, señales Bluetooth, señales satelitales, señales microondas, entre otras tecnologías inalámbricas) o señales alámbricas, configura como uso prohibido del servicio, cubriendo en este apartado, la problemática de la prestación de servicios de telecomunicaciones, entre otros, mediante la instalación de antenas ilegales, subarrendamiento del servicio del internet, Wi-Fi, los cuales pueden darse o encontrarse, dentro o fuera de la zona restringida y de alta seguridad.

Adicionalmente, conforme a lo establecido en el Decreto Legislativo N° 1688, se considera como uso prohibido de los servicios públicos de telecomunicaciones al uso de servicios públicos de telecomunicaciones en zonas restringidas y de alta seguridad para establecer o facilitar comunicaciones con fines delictivos.

Ahora bien, de conformidad con lo establecido en el artículo 3° de la Ley Marco de los Organismos Reguladores de la Inversión Privada en Servicios Públicos, aprobada mediante Ley N° 27332 y modificada en parte por la Ley N° 27631, el OSIPTEL tiene 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, y otras de carácter general referidas a intereses, obligaciones o derechos de las entidades o actividades supervisadas o de usuarios.

Asimismo, el inciso p) del artículo 25° del Reglamento General del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL, aprobado mediante Decreto Supremo N° 008-2001-PCM, establece que este Organismo en ejercicio de su función normativa tiene la facultad de dictar reglamentos o disposiciones de carácter

general que, de acuerdo a las funciones encargadas al OSIPTEL, sea necesario para cumplir con sus fines.

Por ello, corresponde que el OSIPTEL en el marco de sus competencias apruebe los criterios que las empresas operadoras utilizan para proceder al respectivo corte del servicio y/o bloqueo del equipo terminal.

Asimismo, considerando que el Osiptel ha establecido previamente los criterios que actualmente se vienen aplicando para el corte del servicio móvil por uso prohibido, por tanto, corresponde que proceda a actualizar dichos criterios dadas las nuevas circunstancias, como el uso del servicio de acceso fijo a internet, que se han venido presentando desde la entrada en vigencia del Decreto Supremo N° 006-2011-JUS.

De otro lado, el artículo 22° del Reglamento General del OSIPTEL, aprobado mediante Decreto Supremo N° 008-2001-PCM, señala que, para el cumplimiento de sus objetivos, el OSIPTEL cuenta con la función supervisora. Asimismo, el artículo 36° del Reglamento General indica que la función supervisora permite verificar el cumplimiento de las obligaciones legales, contractuales o técnicas por parte de las empresas operadoras y demás empresas o personas que realizan actividades sujetas a su competencia; además, a través de la misma, se puede comprobar el cumplimiento de cualquier mandato o resolución emitida por el OSIPTEL o de cualquier otra obligación que se encuentre a cargo de dichas entidades supervisadas.

Por ello, dado que el Osiptel es el organismo competente para fiscalizar a las empresas operadoras prestadoras de los servicios públicos, corresponde que, en el marco de sus competencias, proceda a emitir los criterios que estas deben aplicar para la detección del uso prohibido, buscando que se dé cumplimiento a lo previsto en el Reglamento, pero a su vez salvaguardando el derecho de los posibles usuarios afectados.

En tal sentido, los criterios que deberá aprobar el Osiptel deben considerar no solo el procedimiento para efectuar el corte del servicio y/o bloqueo del equipo terminal, sino también el procedimiento para que se pueda realizar la respectiva reactivación y/o desbloqueo del equipo terminal. En efecto, si bien los criterios a establecerse tendrán como finalidad identificar el uso prohibido, es posible que, en algunos casos estos criterios no se sigan adecuadamente por parte de las empresas operadoras, de modo que se afecten a usuarios que no estarían realizando uso del servicio dentro del mismo establecimiento penitenciario, debiendo las empresas operadoras en estos casos proceder con la reactivación del servicio y desbloqueo respectivos.

Cabe indicar que la información de detalle de los criterios a aprobarse para proceder al corte del servicio y/o bloqueo del equipo terminal, será puesta en conocimiento directamente a las empresas operadoras, considerando que en el artículo 16° del Decreto Supremo N° 021-2019-JUS, que aprobó el Texto Único Ordenado de la Ley N° 2780, Ley de Transparencia y Acceso a la Información Pública, se indica que se considera reservada la información que tiene por finalidad prevenir y reprimir la criminalidad en el país y cuya revelación puede entorpecerla y, ello comprende los planes de seguridad de establecimientos penitenciarios. Por tanto, la información de los criterios que apruebe el Osiptel y que deben concurrir para que las empresas operadoras procedan al corte del servicio y/o bloqueo del equipo terminal, tendrá la clasificación de reservada.

Por otro lado, se ha contemplado establecer una obligación a ser cumplida por la empresa operadora, referida a que si mediante el uso de mecanismos de monitoreo permanente, detecte accesos y/o intentos de conexión a la red móvil dentro de los establecimientos penitenciarios o centros juveniles, debe efectuar el corte del servicio

público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo de manera inmediata, de acuerdo a los criterios que apruebe el OSIPTEL para tal efecto.

Sobre el particular, la obligación antes mencionada está relacionada a lo establecido en el numeral 6.5 del artículo 6 del Proyecto de Reglamento, el cual dispone que la empresa operadora debe implementar mecanismos de monitoreo permanente de red, tales como, a través de herramientas de crowdsourcing y análisis de sistemas de geolocalización que realicen seguimiento de los accesos y/o intentos de conexión a su red, de los equipos terminales que se encuentren dentro del área de los establecimientos penitenciarios y centros juveniles. En ese sentido, si en base a dicho monitoreo detecta intentos de conexión a su red desde los establecimientos penitenciarios o centros juveniles, efectúa el corte del servicio público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo de manera inmediata.

Asimismo, el OSIPTEL aprobará los criterios bajo los cuales se realizará la aplicación de la mencionada medida.

Considerando que el uso prohibido constituye una conducta ilícita realizada por los internos de los establecimientos penitenciarios o centros juveniles, resulta probable que el mismo se lleve a cabo con fines igual de delictivos, como extorsión, suplantación de identidad, entre otros. Por tanto, corresponde advertir a los usuarios que reciben estas comunicaciones, a fin de evitar que –por desconocimiento– del origen de este tipo de comunicaciones se vean afectados.

En ese sentido, este mecanismo de alerta permite a los abonados tomar las precauciones del caso, en el marco de la seguridad ciudadana; siendo que se transparenta la naturaleza de la llamada y brinda al receptor la oportunidad de tomar decisiones informadas, reduciendo así la posibilidad de involucrarse en comunicaciones ilícitas o no deseadas.

Del mismo modo, dado el origen ilícito de este tipo de comunicaciones, resulta necesario que la PNP y al INPE tengan conocimiento de aquellos servicios y equipos que reciben una gran cantidad de comunicaciones que constituyen uso prohibido, por lo que se dispone que las empresas operadoras brinden un reporte mensual al respecto.

Cabe indicar que, similares medidas se vienen implementando en otros países, como se cita a continuación:

- **Argentina:** Mediante la resolución 36/2005 publicada el 28.02.2005 obliga a los prestadores del servicio telefónico a informar por medio de un mensaje grabado que se está recibiendo llamadas provenientes de las dependencias del servicio penitenciario en forma previa al inicio de la comunicación²⁵.

La referida medida se sustentó en la proliferación de los denominados “secuestros virtuales”, y tuvo la finalidad de desalentar maniobras delictivas mediante el uso de tarjetas de telefonía prepago a través de llamadas realizadas desde establecimientos penitenciarios. Se consideró que dicha medida no resultaba arbitraria pues no vulnera el derecho a la privacidad del interno, toda vez que su permanencia en prisión ha sido dispuesta por un juez competente y por lo tanto “no reviste carácter secreto, ni genera obligación del Estado Nacional de ocultar tal circunstancia”²⁶.

²⁵ <https://www.argentina.gob.ar/normativa/nacional/resoluci%C3%B3n-36-2005-104125/texto>

²⁶ <https://www.diariojudicial.com/news-49925-advertencia-para-evitar-ilicitos-desde-carceles>

- **Estado Unidos:** En este país, los internos solo pueden hacer llamadas mediante cobro revertido. Las normas de la Comisión Federal de Comunicaciones -FCC exigen que, cuando una persona privada de su libertad realiza una llamada de cobro revertido, cada proveedor de servicios debe identificarse ante la persona que recibe la llamada antes de conectarla. Asimismo, el proveedor de servicios debe permitir al receptor de la llamada telefónica dar término a la misma, antes de realizar la conexión, sin ningún costo²⁷.
- **México:** La Ley Federal de Telecomunicaciones y Radiodifusión de los Estados Unidos Mexicanos (LFTR)²⁸ establece que las empresas de telecomunicaciones deben conservar un registro y control de comunicaciones que se realicen desde cualquier tipo de línea que utilice numeración propia o arrendada, bajo cualquier modalidad, que permitan identificar con precisión los siguientes datos: Nombre, denominación o razón social y domicilio del suscriptor; así como los datos necesarios para rastrear e identificar el origen y destino de las comunicaciones de telefonía móvil: número de destino, modalidad de líneas con contrato o plan tarifario, como en la modalidad de líneas de prepago; entre otros.

Asimismo, esta información puede ser requerida por la autoridad competente en los términos que establezcan las leyes, conforme lo dispuesto en la referida Ley Federal de Telecomunicaciones y Radiodifusión.

En atención a lo expuesto, queda claro que la obligación de las empresas operadoras de alertar a los abonados sobre posibles comunicaciones ilegales, se encuentra alineada con las medidas de seguridad que deben considerarse en el uso de servicios públicos de telecomunicaciones.

5.3.4. Solicitud de datos relacionados a los equipos terminales móviles encontrados en establecimientos penitenciarios o en centros juveniles

El artículo 15 del Decreto Legislativo N° 1688 establece la obligación de las empresas operadoras de brindar el acceso a la información de servicios móviles asociados a equipos terminales móviles y SIM Card incautados en requisas en establecimientos penitenciarios y centros juveniles, conforme se cita a continuación:

“Artículo 15. Acceso a la información de servicios móviles asociados a equipos terminales móviles y SIM Card incautados en requisas en establecimientos penitenciarios y centros juveniles

Las empresas operadoras, a solicitud del Ministerio Público, del Instituto Nacional Penitenciario o de la Policía Nacional del Perú, deben proporcionar la información sobre datos de titularidad del equipo terminal móvil y del abonado asociado a la tarjeta SIM Card, así como el reporte de llamadas entrantes y salientes realizadas a través de dichos objetos prohibidos incautados durante las requisas en establecimientos penitenciarios o centros juveniles, conforme al procedimiento establecido en el Reglamento.”

En ese sentido, en el capítulo IV del Reglamento se ha desarrollado el acceso a la información de servicios móviles asociados a equipos terminales móviles encontrados en establecimientos penitenciarios o en centros juveniles, es decir, se reglamenta lo dispuesto en el referido artículo 15 del Decreto Legislativo N° 1688, con la finalidad de

²⁷ https://www.fcc.gov/sites/default/files/servicio_telefonico_en_centros_penitenciarios.pdf

²⁸ <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFTR.pdf>

que el acceso a la referida información se realice de manera celer y eficaz, acorde al ordenamiento jurídico vigente.

Respecto del artículo 14 del reglamento del Decreto Legislativo N° 1688

El numeral 14.1 del artículo 14 del Reglamento establece las entidades públicas y sus dependencias específicas que se encuentran legitimadas para solicitar a las empresas operadoras de servicios públicos de telecomunicaciones la información que se señala en el artículo 15 del Decreto Legislativo N° 1688 relacionada a los equipos terminales móviles encontrados en centros penitenciarios o centros juveniles.

En ese sentido, se establece que el Ministerio Público o la unidad especializada de la PNP, indistintamente, pueden solicitar a las empresas operadoras los siguientes datos relacionados a los equipos terminales móviles encontrados en establecimientos penitenciarios o centros juveniles, siempre que constituya un medio necesario para la investigación penal:

- a) Datos de titularidad del equipo terminal móvil y del abonado asociado a la tarjeta SIM Card.
- b) Reporte de llamadas entrantes y salientes realizadas a través de dichos objetos.

Es importante resaltar que se reconoce la legitimidad del Ministerio Público para solicitar la referida información a las empresas operadoras, en tanto que este tiene la calidad de titular de la acción penal; en ese sentido, es responsable de dirigir las investigaciones penales que podrían llevarse a cabo en atención a haber encontrado un equipo terminal móvil en un centro penitenciario.

Así, por ejemplo, dentro del Título XVIII del Código Penal que establece los delitos contra la administración pública, encontramos el artículo 368-A, el cual tipifica el delito de *“Ingreso indebido de equipos o sistema de comunicación, fotografía y/o filmación en centros de detención o reclusión”* el cual es cometido por *“el que ingresa, intenta ingresar o permite el ingreso a un centro de detención o reclusión, equipos o sistema de comunicación, fotografía y/o filmación o sus componentes que permitan la comunicación telefónica celular o fija, radial, vía internet u otra análoga del interno, así como el registro de tomas fotográficas, de video, o proporcionen la señal para el acceso a internet desde el exterior del establecimiento penitenciario”* y puede ser reprimido con pena privativa de libertad no menor de cuatro ni mayor de seis años; asimismo, el artículo 368-D tipifica la *“Posesión indebida de teléfonos celulares o, armas, municiones o materiales explosivos, inflamables, asfixiantes o tóxicos en establecimientos penitenciarios”*, estableciendo que si el agente posee, porta, usa o trafica con un teléfono celular o fijo o cualquiera de sus accesorios que no esté expresamente autorizado, la pena privativa de libertad será no menor de tres ni mayor de ocho años.

Por otro lado, se reconoce la legitimidad de la Unidad especializada de la PNP para solicitar datos relacionados a los equipos terminales móviles encontrados en establecimientos penitenciarios o centros juveniles debido a que conforme al Decreto Legislativo N° 1182, dicha unidad es la que actualmente desempeña el papel de punto focal con las empresas operadoras para que estas permitan el acceso a datos derivados de las telecomunicaciones, los cuales son usados por las unidades a cargo de la investigación policial que así lo requieren.

Dicha medida permite hacer un uso eficiente del manejo de la información pues busca aprovechar que actualmente, la Unidad especializada de la PNP, cuenta con mecanismos de coordinación celeres para solicitar a las empresas operadoras datos derivados de las telecomunicaciones, así como para recibir dicha información. En

específico las referidas solicitudes las realiza a través de correos electrónicos institucionales o medios idóneos convenidos (conforme el artículo 4 del Decreto Legislativo N° 1182). Además, debe tenerse en cuenta que la Unidad especializada de la PNP actualmente recibe el reporte de los datos identificatorios de teléfonos móviles o dispositivos electrónicos de naturaleza similar cuyas llamadas proceden de establecimientos penitenciarios en atención a lo dispuesto en el numeral 13.2 del artículo 13 del Decreto Legislativo N° 1688.

Por otro lado, el numeral 14.2 del artículo 14 del Reglamento, establece que la Dirección de Seguridad Penitenciaria del INPE, puede solicitar a las empresas operadoras los datos señalados en el numeral 14.1 respecto de los equipos terminales móviles encontrados en establecimientos penitenciarios en el marco de lo dispuesto en los artículos 68 y 69 del Reglamento del Código de Ejecución Penal, aprobado con Decreto Supremo N° 015-2003-JUS.

Dicha medida se encuentra alineada al marco regulatorio vigente respecto a las acciones de registro o revisión que realiza el INPE en establecimientos penitenciarios, el cual se encuentra regulado en los artículos 68 y 69 del Reglamento del Código de Ejecución Penal, aprobado con Decreto Supremo N° 015-2003-JUS; en ese sentido, la propuesta normativa trata de que se respeten las actuales reglas que buscan garantizar la transparencia y objetividad en dichas revisiones y el consecuente decomiso de objetos prohibidos como los equipos terminales móviles²⁹, conforme se procede a detallar:

- El artículo 68 del Reglamento del Código de Ejecución Penal establece que la autoridad penitenciaria podrá ordenar las revisiones de rutina, por lo menos una vez por semana, en los ambientes que ocupa el interno, las que se realizarán con presencia del director o subdirector, del jefe de seguridad y del personal de tratamiento; éstos participarán como observadores. Además, que terminada la diligencia, se levantará un acta suscrita por las autoridades antes señaladas, donde consten los objetos prohibidos que se hayan encontrado, los mismos que serán puestos a disposición del Ministerio Público, PNP u Oficina Regional del INPE, según corresponda, dentro de las 24 horas. Asimismo, un ejemplar del acta será entregada al director de la Oficina Regional.
- Además, el artículo 69 del Reglamento del Código de Ejecución Penal establece que los registros o revisiones súbitas o extraordinarias, cuando la necesidad o circunstancias así lo requieran, se realizarán con la presencia obligatoria del representante del Ministerio Público y, de ser el caso, con el apoyo de la PNP. Concluidos éstos, se informará inmediatamente al director general de la Dirección Regional.

En esta línea, el artículo 150 del Reglamento General de Seguridad del INPE, aprobado con Resolución Presidencial N° 003-2008-INPE-P, establece que los teléfonos celulares decomisados en los establecimientos penitenciarios “*serán remitidos por las direcciones regionales a la Dirección de Seguridad Penitenciaria, quién coordinará con la Policía Nacional del Perú para la correspondiente investigación del registro de llamadas y recibidas.*” En ese sentido, resulta coherente que sea dicha dirección la legitimada para solicitar a las empresas operadoras los datos señalados en el numeral 14.1 respecto de los equipos terminales móviles encontrados en establecimientos penitenciarios.

²⁹ Conforme el anexo 9 del Reglamento General de Seguridad del INPE, aprobado con Resolución Presidencial NO 003-2008-INPE P, y modificado con Resolución de Presidencia N° 98-2012-INPE/P, los “Teléfonos celulares y cualquier accesorio y/o complemento que facilite su uso, como baterías, cargadores y chips, asimismo, cualquier equipo terminal y sus componentes que faciliten la telecomunicación y/o transmisión de voz” constituyen artículo prohibidos para el ingreso a un establecimiento penitenciario.

Respecto del artículo 15 del Reglamento y su séptima disposición complementaria final

El numeral 15.1 del artículo 15 del Reglamento, establece que el Ministerio Público, la unidad especializada de la PNP, o la Dirección de Seguridad Penitenciaria del INPE, cursa la solicitud a la que hace referencia el artículo anterior a las empresas operadoras, a través del correo electrónico institucional u otro medio idóneo convenido. A su vez, la séptima disposición complementaria final establece que, en un plazo no mayor de sesenta (60) días hábiles, dichas entidades, previa coordinación con las empresas operadoras, elaboran y aprueban los protocolos para el mejor acceso de los datos señalados en el numeral 14.1 del artículo 14.

Dicha medida tiene por objeto dotar de celeridad a la presentación de solicitudes de acceso a información de equipos terminales encontrados en establecimientos penitenciarios o centros juveniles, permitiendo que se realicen acciones de coordinación entre las entidades públicas legitimadas y las empresas operadoras que permitan su presentación a través de correos electrónicos, u otro medio acordado entre estos, por ejemplo el acceso a las plataformas de datos de las empresa operadoras u otros medios disponibles consensuados de manera conjunta.

El numeral 15.2 del artículo 15 del Reglamento establece los requisitos que deben acompañar las entidades públicas legitimadas a las solicitudes para acceder a información de terminales móviles encontrados en establecimientos penitenciarios o centros juveniles, los cuales son:

- El Acta de decomiso de Artículos Prohibidos, pues conforme los artículos 68 y 69 del Reglamento del Código de Ejecución Penal, en concordancia con el artículo 148 del Reglamento General de Seguridad del INPE, el personal del Centro Penitenciario decomisa los artículos prohibidos que haya encontrado, y levanta el Acta correspondiente con las autoridades que participan en dicha diligencia.

Dicha acta debe ser acompañada a la solicitud de información que se presenten a las empresas operadoras, pues permite identificar que efectivamente se trata de datos relacionados a equipos encontrados en establecimientos penitenciarios, acción que podría constituir el delito de “ingreso indebido de equipos o sistema de comunicación, fotografía y/o filmación en centros de detención o reclusión” (artículo 368-A del Código Penal); “posesión indebida de teléfonos celulares o, armas, municiones o materiales explosivos, inflamables, asfixiantes o tóxicos en establecimientos penitenciarios” (artículo 368-D del Código Penal), y que por ende constituyen datos que no se encuentran protegidos por el derecho al secreto de las telecomunicaciones.

Sobre el particular, el objeto de protección del derecho fundamental al secreto de las comunicaciones³⁰ es “proteger el proceso de comunicación en sí, y la expectativa de confidencialidad³¹ que se genera cuando una persona utiliza para

³⁰ Al respecto, el Tribunal Constitucional ha señalado que en atención al numeral 10 del artículo 2 de la Constitución Política, “Toda persona tiene derecho a que sus comunicaciones y documentos privados sean adecuadamente protegidos, así como a que las mismas y los instrumentos que las contienen, no puedan ser abiertas, incautadas, interceptadas o intervenidas sino mediante mandamiento motivado del juez y con las garantías previstas en la ley” (STC 01058-2004-AA/TC fundamento 18)

³¹ El Magistrado Carlos ramos Nuñez en su voto recaído en al STC 05532-2014-PA/TC señala que la doctrina de la “expectativa razonable de privacidad (*reasonable expectation of privacy*)”, la cual fue elaborada por la Corte Suprema Federal de los Estados Unidos en el caso *Katz vs. U.S* (1967), y que tiene un origen más remoto en el conocido trabajo de los juristas Warren y Brandeis titulado “The right to Privacy” [Warren y Brandeis. *The Right to Privacy*. Harvard Law Review, vol. IV, Nro. 5, de 15 de diciembre de 1890]. Esta doctrina, desarrollada inicialmente para evaluar las actuaciones

comunicarse un determinado medio técnico” (STC 03599-2010-PA/TC fundamento 8 del voto del magistrado Eto Cruz)³²; sin embargo, los datos señalados en el numeral 14.1 del artículo 14 del Reglamento se encuentran relacionados a comunicaciones realizadas con terminales móviles ingresados indebidamente en centros penitenciarios y no pueden generar en los reclusos una “expectativa de confidencialidad” pues se trata de una actividad ilegal que puede constituir un delito, máxime si se tiene en cuenta la finalidad de dichas comunicaciones, pues conforme se señaló en la Sentencia de Casación 1356-2019-/AREQUIPA, “La existencia de equipos de comunicación telefónica en poder de los internos, les permite alterar la tranquilidad pública desde el interior del propio establecimiento penitenciario –o, con mayor amplitud, de centros de detención o reclusión en general–, con la planificación de actos delictivos, extorsiones, amedrentamientos y demás acciones que ponen en zozobra a la ciudadanía.”

Por lo tanto, los datos señalados en el numeral 14.1 del artículo 14 del Reglamento (registro de llamadas, titularidad del equipo o del servicio) no se encuentran protegidos por el derecho al secreto de las comunicaciones y por ende no requieren de autorización judicial previa para ser revelados.

- Los datos que permitan identificar el equipo terminal móvil y la tarjeta SIM Card encontrados en el establecimiento penitenciario o centro juvenil.

Por su parte el numeral 15.3 del artículo 15 del presente reglamento, establece que las empresas operadoras están obligadas a conservar los datos señalados en el numeral 14.1 del artículo 14 del presente reglamento por treinta y seis (36) meses en un sistema de almacenamiento electrónico. La entrega de dichos datos se realiza dentro de los siete (7) días calendario siguientes de realizada la solicitud

Dicha medida se encuentra alineada a lo dispuesto en el primer párrafo de la Segunda Disposición Complementaria Final del Decreto Legislativo N° 1182, que establece similar periodo, forma de almacenamiento y plazo de entrega de los datos derivados de telecomunicaciones por parte de las empresas operadoras, y tiene por objetivo garantizar la celeridad de la entrega de información para que las entidades públicas legitimadas puedan desarrollar sus funciones de manera idónea, ya sea para la persecución del delito (en el caso de la PNP y el Ministerio Público) o para mantener el principio de autoridad, orden y disciplina dentro del centro penitenciario (en el caso del INPE).

5.3.5. Sobre el régimen de fiscalización a cargo del MTC

Conforme al segundo párrafo del numeral 239.1 del artículo 239 del Texto único Ordenado de la Ley 27444, aprobado mediante Decreto Supremo N° 004-2019-JUS (en adelante, TUO de la LPAG), *“solamente por Ley o Decreto Legislativo puede atribuirse la actividad de fiscalización a las entidades”*.

de los órganos de persecución penal y las formas de obtención de la prueba, fue con posterioridad trasladada a otros ámbitos, y ha sido empleada, entre otros organismos, por el Tribunal Europeo de Derechos Humanos para analizar posibles vulneraciones del derecho a la vida privada o familiar [ver, entre otros, Halford v. United Kingdom, Copland v. United Kingdom].

³² En esta misma línea el TC señaló que *“El concepto de “secreto” e “inviolabilidad” de las comunicaciones y documentos privados, desde esa perspectiva, comprende a la comunicación misma, sea cual fuere su contenido y pertenezca o no el objeto de la comunicación al ámbito de lo personal, lo íntimo o lo reservado. De manera que se conculca el derecho tanto cuando se produce una interceptación de las comunicaciones, es decir, cuando se aprehende la comunicación dirigida a terceros, como cuando se accede al conocimiento de lo comunicado, sin encontrarse autorizado para ello”*. (STC 2863-2002-AA/TC fundamento 3)

En línea con la precitada disposición, el artículo 16 del Decreto Legislativo N° 1688, otorga al MTC la potestad fiscalizadora respecto de las obligaciones derivadas del artículo 8 del Capítulo I, Título II de dicha norma.

En este contexto, corresponde considerar que el artículo 5 de la LOF del MTC dispone que el MTC tiene, entre otras **funciones rectoras**, formular, planear, dirigir, coordinar, ejecutar, fiscalizar, supervisar y evaluar la política nacional y sectorial bajo su competencia, aplicable a todos los niveles de gobierno; así como, dictar normas y lineamientos técnicos para la adecuada ejecución, supervisión y evaluación de las políticas, la gestión de los recursos del sector, así como para el otorgamiento y reconocimiento de derechos, **la sanción, la fiscalización y ejecución coactiva en materias de su competencia.**

Por su parte, el artículo 2 del ROF del MTC, establece que, el MTC ejerce jurisdicción en el ámbito nacional, regional y local, **como ente rector del sector Transportes y Comunicaciones**, en el marco de sus competencias exclusivas y compartidas que le otorga la ley, comprendiendo, la competencia exclusiva en infraestructura y servicios de comunicaciones y la competencia compartida en promoción de la infraestructura de telecomunicaciones y el planeamiento de los servicios de telecomunicaciones de alcance regional.

Dicho reglamento establece las siguientes competencias y funciones del órgano de línea:

“Artículo 164.- Dirección General de Fiscalizaciones y Sanciones en Comunicaciones

La Dirección General de Fiscalizaciones y Sanciones en Comunicaciones es el órgano de línea responsable de la conducción de los actos y diligencias correspondientes a la fiscalización del cumplimiento de las normas y de los títulos habilitantes en la prestación de servicios y actividades de comunicaciones; y, a la sanción, en caso de su incumplimiento; así como, al control del uso del espectro radioeléctrico. Depende del Despacho Viceministerial de Comunicaciones”.

El artículo 166 del ROF del MTC, establece que son unidades orgánicas de la DGFSC las siguientes: la Dirección de Fiscalizaciones de Cumplimiento de Normativa en Comunicaciones, la Dirección de Fiscalizaciones de Cumplimiento de Títulos Habilitantes en Comunicaciones, y la Dirección de Sanciones en Comunicaciones.

Atendiendo a dicha potestad, facultades y funciones, en el Capítulo V del Reglamento se han desarrollado las disposiciones sobre la facultad fiscalizadora del MTC para verificar el cumplimiento de las obligaciones establecidas en el capítulo II del Reglamento.

De esta manera, en el artículo 16 del Reglamento se han incluido disposiciones generales sobre las acciones de fiscalización a ser realizadas por el MTC, en el marco del Reglamento.

Así, en el numeral 16.1 se establece que las acciones de fiscalización que realice el MTC, a través de la DGFSC, son el conjunto de actuaciones cuyo objeto es verificar el cumplimiento de las obligaciones establecidas en el Reglamento. Además, en el numeral 16.2 se indica que las acciones de fiscalización se realizan con comunicación previa o de forma inopinada; así como, en el numeral 16.3, se señala que pueden ejecutarse de manera presencial o remota. De este modo, los diferentes tipos de fiscalización podrán ser ejecutados por el MTC, dependiendo de las necesidades

particulares de la obligación cuyo cumplimiento se busca constatar, así como, los elementos y/o componentes que serán objeto de verificación.

Asimismo, en el numeral 16.4 del artículo 16 del Reglamento se ha establecido que el MTC puede coordinar o solicitar la cooperación del MINJUSDH, INPE, PRONACEJ, la PNP, la empresa que gestiona el sistema de restricción de señales de comunicaciones, el OSIPTEL, entre otras entidades, a fin de que las mismas otorguen las facilidades, cooperación y/o garantías necesarias para que el MTC realice las acciones de fiscalización, sobre todo en las que involucre el resguardo de la integridad física del personal de fiscalización de la DFCTH.

Dicha disposición es de suma relevancia considerando que las referidas entidades están involucradas ya sea en la administración y gestión de los establecimientos penitenciarios, centros juveniles, el sistema de restricción de señales, la fiscalización de las empresas operadoras y/o en el mantenimiento de la seguridad pública, respectivamente, por lo cual, dependiendo del objeto de la fiscalización y el lugar donde esta se realice, el MTC podrá requerir el apoyo de las mismas para realizar las pruebas técnicas y asegurar un resultado adecuado en las verificación del cumplimiento de las obligaciones, así como para salvaguardar la integridad del personal fiscalizador de la DFCTH, considerando que las comunicaciones ilegales desde los establecimientos penitenciarios y centros juveniles podrían estar vinculados a bandas u organizaciones criminales con cierto interés en frustrar las acciones de fiscalización.

En el numeral 16.5 se ha establecido que en todo lo no contemplado en dicho capítulo, rige lo establecido en el Reglamento de Fiscalización y Sanción en la Prestación de Servicios y Actividades de Comunicaciones de Competencia del Ministerio de Transportes y Comunicaciones, aprobado mediante Decreto Supremo N° 028-2019-MTC (en adelante, Reglamento de Fiscalización y Sanción del MTC) o norma que la sustituya.

Sobre el particular, es preciso considerar que actualmente el Reglamento de Fiscalización y Sanción del MTC regula el ejercicio de las funciones de fiscalización y de sanción en la prestación de los servicios de comunicaciones y las actividades conexas que son de competencia del MTC, por lo que las disposiciones correspondientes al Capítulo V del Reglamento deben ser entendidas de manera sistemática y concordada con el mencionado reglamento.

Con relación a las fiscalizaciones con comunicación previa a la empresa operadora, en el artículo 17 del Reglamento se prevé que dicha comunicación se realice con una anticipación no menor a tres (03) días hábiles, indicando determinada información como el objeto de la fiscalización, el lugar donde se efectuará las acciones de fiscalización (en caso de ser presencial), los sistemas de gestión o desarrollos tecnológicos (en caso de ser remota), la fecha y hora de su realización, entre otros datos.

Por su parte, con relación a las fiscalizaciones inopinadas, estas serán realizadas dependiendo del objeto de fiscalización y con la finalidad de garantizar un resultado exitoso que permita conocer fehacientemente el estado del cumplimiento de la obligación.

Para tal efecto, se ha establecido que ante dicho tipo de fiscalizaciones, las empresas operadoras tienen la obligación de permitir al MTC el acceso inmediato e ininterrumpido a las instalaciones y/o sistemas que se requiera fiscalizar, no pudiendo alegar ausencia de personal, problemas de gestión interna, entre otros, que impidan realizar la fiscalización.

De otra parte, en el artículo 19 del Reglamento se ha previsto la obligación de la DGFSC de programar la ejecución de acciones de fiscalización a las empresas operadoras para verificar el cumplimiento de las obligaciones a su cargo, las cuales deben ejecutarse periódicamente, por lo menos de forma trimestral, periodicidad que se ha considerado adecuada para un monitoreo frecuente sobre el estado de cumplimiento de dichas obligaciones y, dependiendo de los resultados, poder adoptar las medidas que contribuyan a mantener el cumplimiento de las obligaciones.

En el artículo 20 del Reglamento se han estipulado, de forma enunciativa, algunas obligaciones de las empresas operadoras en cuanto a las acciones de supervisión; entre ellas, la obligación de acompañar al personal fiscalizador, cuando este lo requiera, a las fiscalizaciones que se realicen; brindar todas las facilidades y cooperar para la realización de las verificaciones técnicas que fueran necesarias durante las acciones de fiscalización; proporcionar toda la información, conforme a la solicitud que efectúa la autoridad fiscalizadora; permitir el acceso del personal fiscalizador a sus instalaciones, cuando sea requerido por esta; suscribir el acta correspondiente en aquellos casos en los que intervengan y las demás que establezca el marco normativo aplicable.

Cabe mencionar que las obligaciones antes mencionadas se encuentran alineadas con las obligaciones establecidas en el numeral 5.1 del artículo 5 del Reglamento de Fiscalización y Sanción del MTC.

Por otro lado, en el Reglamento se ha establecido las acciones de fiscalización culminan con la suscripción del acta de fiscalización que dejan constancia del desarrollo de las mismas, de acuerdo a las formalidades que se establece en el Reglamento de Fiscalización y Sanción del MTC o norma que la sustituya.

5.3.6. Sobre el régimen sancionador a cargo del MTC

El numeral 1 del artículo 248 del TUO de la LPAG consagra el Principio de Legalidad en materia sancionadora, según el cual sólo por norma con rango de ley cabe atribuir a las entidades la potestad sancionadora y la consiguiente previsión de las consecuencias administrativas que a título de sanción son posibles de aplicar a un administrado.

En mérito a lo antes dispuesto, el artículo 16 del Decreto Legislativo N° 1688 otorga al MTC la potestad sancionadora respecto de las obligaciones derivadas del Capítulo I, Título II de dicha norma. Asimismo, se establece que las infracciones se clasifican en leves, graves y muy graves, las cuales se tipifican en el Reglamento. Además, se ha estipulado que las infracciones son sancionadas, de acuerdo a las escalas de multas establecidas en la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL o norma que sustituya dicha escala de multas. En el caso de infracciones leves, se puede aplicar la sanción de amonestación escrita o multa, y para las infracciones graves y muy graves aplica la sanción de multa.

Sobre el particular, en la exposición de motivos del Decreto Legislativo N° 1688 se indica lo siguiente: *“...se advierte que gran parte de estas normas de mandato carecen de aplicabilidad por razones técnicas, y principalmente, por la falta de potestad sancionadora de la entidad competente frente a su incumplimiento. Esta última situación amerita emitir una norma con rango de Ley que otorgue de forma expresa al MTC y al OSIPTEL facultades fiscalizadoras y sancionadoras respecto a las diferentes obligaciones atribuibles a las empresas operadoras, vinculadas a las diferentes normas sobre comunicaciones ilícitas desde establecimientos penitenciarios y centros juveniles”.*

De acuerdo con el precitado texto, una de las falencias del marco normativo previo al Decreto Legislativo N° 1688, es que, si bien se establecía ciertas obligaciones a las empresas operadoras para evitar que se realicen llamadas ilegales desde establecimientos penitenciarios, no se había dotado a las entidades competentes, de la potestad sancionadora para la tipificación de infracciones y sanciones que aseguren la observancia de dichas obligaciones.

Considerando lo antes mencionado, en el Reglamento se han tipificado las infracciones y la calificación de las mismas, ante el incumplimiento de las obligaciones establecidas en los artículos 5 y 6 de dicho reglamento, con la finalidad de garantizar su cumplimiento por parte de las empresas operadoras, de acuerdo con lo siguiente:

- **Por incumplimiento de los numerales 5.1, 5.2 y 5.4 del artículo 5 del Reglamento:**

“La empresa operadora que no cumpla con restringir la emisión de su señal radioeléctrica de los servicios públicos de telecomunicaciones hacia los establecimientos penitenciarios y centros juveniles, conforme a lo establecido en los numerales 5.1 y 5.2 del artículo 5 del presente reglamento.

Asimismo, la empresa operadora que instale nuevas estaciones radioeléctricas o implemente nuevas tecnologías o actualizaciones sobre estaciones existentes, incumpliendo lo dispuesto en el numeral 5.4 del artículo 5 del presente reglamento.”

Esta infracción está referida al incumplimiento por parte de la empresa operadora de la obligación de restringir su señal radioeléctrica conforme a los parámetros establecidos en el Reglamento, considerando que de no existir un adecuado control de la señal radioeléctrica que se emite hacia los establecimientos penitenciarios y centros juveniles, se podría dificultar el bloqueo de la misma y/o posibilitar que se realicen las comunicaciones desde dichos ámbitos.

Asimismo, esta infracción también comprende el incumplimiento por parte de la empresa operadora de la obligación de instalar nuevas estaciones radioeléctricas o nuevas tecnologías; así como, realizar actualizaciones sobre estaciones existentes, sin cumplir con la restricción de la señal radioeléctrica conforme a lo previsto en el Reglamento, puesto que, si la empresa operadora realiza las adecuaciones técnicas en su infraestructura para cumplir con restringir su señal radioeléctrica y no realiza lo propio con las nuevas estaciones que pueda instalar o las actualizaciones tecnológicas que efectúe, se incrementa el riesgo de que concreten las comunicaciones desde establecimientos penitenciarios y centros juveniles.

La calificación de “*muy grave*” se sustenta en la relevancia de la obligación cuyo cumplimiento se busca asegurar puesto que, de no realizarse una restricción de la señal radioeléctrica hacia los establecimientos penitenciarios y centros juveniles, se favorece a la realización de comunicaciones ilegales desde dichos ámbitos, poniendo así en riesgo a la ciudadanía en general.

De este modo, la referida calificación obedece a la necesidad de disuadir esta conducta y desincentivar que la empresa operadora no se ciña a los parámetros acordados con la empresa que gestiona el sistema de restricción de señales radioeléctricas o los previstos en el Protocolo Técnico, los cuales son relevantes que se cumplan para evitar que se concreten las referidas comunicaciones ilegales.

- **Por incumplimiento del numeral 6.1 del artículo 6 del Reglamento:**

“La empresa operadora que se niegue a realizar las coordinaciones o muestre resistencia para realizar dichas coordinaciones, según lo establecido en el numeral 6.1 del artículo 6 del presente Reglamento.”

Esta infracción está referida a la negativa de la empresa operadora de realizar las coordinaciones con la empresa que gestiona el sistema de restricción de señales o a la resistencia para lograr la finalidad de tales coordinaciones.

Como se ha señalado en la presente exposición de motivos, se considera que es más eficiente que la empresa operadora y la empresa que gestiona los sistemas de restricción de señales coordinen y acuerden los parámetros técnicos de las estaciones que irradian hacia los establecimientos penitenciarios y centros juveniles, así como, de los equipos bloqueadores, considerando las particularidades de cada caso para así evitar que se concreten llamadas desde dichos ámbitos y a su vez no se genere afectación a los usuarios de las zonas cercanas a los mismos.

En ese sentido, resulta de suma importancia incentivar que la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones, realicen las coordinaciones necesarias orientadas a llegar a un acuerdo que permitirá que precisamente que ambas partes cumplan parámetros técnicos que, por un lado, evitará las comunicaciones desde los establecimientos penitenciarios y centros juveniles, reduciendo a su vez el riesgo de afectación a los servicios públicos de telecomunicaciones de las poblaciones aledañas a los establecimientos penitenciarios y centros juveniles.

Nótese en este punto que, si bien a falta de acuerdo aplican los parámetros técnicos establecidos en el Protocolo Técnico, lo más idóneo o eficiente para la finalidad de la norma es lograr que se llegue a un acuerdo entre las mencionadas empresas, por lo cual, es necesario disuadir cualquier acción renuente a realizar las coordinaciones orientadas a arribar a dicho acuerdo.

Ahora bien, cabe aclarar que no constituye infracción la falta de acuerdo entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales, sino la renuencia de la empresa operadora de efectuar tales coordinaciones lo que podría evidenciarse a través de la falta de respuestas o respuestas que muestren una resistencia a llegar un acuerdo.

Cabe mencionar que la calificación de grave obedece a que es importante propiciar las coordinaciones antes mencionadas bajo el entendido de que a través de las mismas se llegará a resultados más eficientes, que no solo evitarán que se concreten las comunicaciones ilegales, sino también que se mitigue el riesgo de afectación a las poblaciones aledañas a los establecimientos penitenciarios y centros juveniles.

- **Por incumplimiento del numeral 6.3 del artículo 6 del Reglamento:**

“La empresa operadora que no implemente medidas de monitoreo de su red de telecomunicaciones para coadyuvar a determinar la funcionalidad u operatividad de los sistemas de restricción de señales de comunicaciones instalados en los establecimientos penitenciarios y centros juveniles, según lo establecido en el numeral 6.3 del artículo 6 del presente reglamento.”

Esta infracción está referida al incumplimiento de la empresa operadora de implementar medidas de monitoreo de su red de telecomunicaciones, según los indicadores señalados en el numeral 6.3 del artículo 6 del Reglamento, los cuales precisamente coadyuvarán a conocer el estado de operación de los equipos bloqueadores, siendo por ello relevante que la empresa operadora se ciña a la citada obligación.

Cabe mencionar que la calificación de grave obedece a que es importante desincentivar esta conducta y evitar que la empresa operadora no realice el monitoreo de su red para advertir situaciones inusuales de la operación de los equipos bloqueadores que podrían reflejar la vulnerabilidad en la seguridad y por ende posibilitar que se concreten las comunicaciones ilegales desde los establecimientos penitenciarios y centros juveniles.

- **Por incumplimiento del numeral 6.4 del artículo 6 del Reglamento:**

“La empresa operadora que no cumpla con advertir los parámetros inusuales que indique un deficiente funcionamiento u operatividad de los equipos de bloqueo, según lo establecido en el numeral 6.4 del artículo 6 del presente Reglamento.”

Esta infracción está referida al incumplimiento de la empresa operadora de comunicar o alertar al MTC, MINJUSDH e INPE, cuando -como resultado del monitoreo de su red- advierta parámetros inusuales que indiquen un funcionamiento deficiente de los equipos bloqueadores.

De esta manera, la calificación de “grave” se sustenta en la necesidad de desincentivar el accionar de la empresa operadora de no comunicar dentro de las veinticuatro (24) horas de detectada tales situaciones, lo cual no coadyuvaría a que las mencionadas entidades, según sus competencias, puedan realizar las verificaciones correspondientes y, de ser el caso, adoptar las acciones que eviten una eventual falencia en la operación de los referidos equipos bloqueadores y con ello prevenir la realización de comunicaciones ilegales.

- **Por incumplimiento del numeral 6.5 del artículo 6 del Reglamento:**

“La empresa operadora que no implemente mecanismos de monitoreo de red que realicen seguimiento de los accesos y/o intentos de conexión a su red que se encuentren dentro del área de los establecimientos penitenciarios y centros juveniles, según lo establecido en el numeral 6.5 del artículo 6 del presente reglamento.”

Esta infracción está referida al incumplimiento de la empresa operadora de implementar mecanismos de monitoreo permanente de su red de telecomunicaciones, según lo dispuesto en el numeral 6.5 del artículo 6 del Reglamento, los cuales precisamente permitirán identificar actividad inusual de usuarios en la red de telecomunicaciones como, por ejemplo, intentos de conexión a la red, tiempo y usos de datos en distintas tecnologías, tráfico de voz o datos, entre otros.

Cabe indicar que la calificación de grave se debe a que es importante desincentivar esta conducta y evitar que la empresa operadora no realice el monitoreo permanente de su red para advertir situaciones anómalas en el acceso y/o intentos de conexión a su red dentro de los establecimientos penitenciarios y centros juveniles.

- **Por incumplimiento del numeral 6.6 del artículo 6 del Reglamento:**

“La empresa operadora que no cumpla con advertir los parámetros inusuales que brinde indicios de acceso y/o intentos de conexión a su red dentro de los establecimientos penitenciarios y centros juveniles, según lo establecido en el numeral 6.6 del artículo 6 del presente reglamento.”

Esta infracción está referida al incumplimiento de la empresa operadora de comunicar o alertar al MTC, MINJUSDH e INPE, cuando -como resultado del monitoreo de su red- advierta indicios de acceso y/o intentos de conexión a su red dentro de los establecimientos penitenciarios y centros juveniles.

De esta manera, la calificación de “grave” se sustenta en la necesidad de desincentivar el accionar de la empresa operadora de no comunicar dentro de las veinticuatro (24) horas de detectada tales situaciones, lo cual no coadyuvaría a que las mencionadas entidades, según sus competencias, puedan realizar las verificaciones correspondientes y, de ser el caso, adoptar las acciones que eviten que se realicen llamadas desde los establecimientos penitenciarios o centros juveniles.

- **Por incumplimiento del numeral 6.7 del artículo 6 del Reglamento:**

“La empresa operadora que incumpla con presentar el detalle de las medidas y mecanismos que implementará en cumplimiento de las obligaciones contenidas en los numerales 6.3 y 6.5, conforme a lo establecido en el numeral 6.7 del artículo 6 del presente reglamento.”

Esta infracción está referida al incumplimiento por la empresa operadora de comunicar el detalle de las medidas y mecanismos de monitoreo que ha de implementar para cumplir las obligaciones contenidas en los numerales 6.3 y 6.5. del artículo 6 del Reglamento, puesto que los criterios utilizados para los monitoreos de red, pueden diferir entre una empresa y otra, además de abarcar más de un indicador, por lo que se considera relevante que las empresas operadoras realicen dicha comunicación.

Cabe mencionar que la calificación de grave se debe a que es importante desincentivar esta conducta y evitar que la empresa operadora no comunique qué medidas o mecanismos implementará, pues de ser así, la DGFSC se verá imposibilitada de verificar y constatar la observancia de esta obligación y, por ende, de garantizar su cumplimiento.

- **Por incumplimiento del artículo 20 del Reglamento:**

“La empresa operadora que no cumpla una o más de las siguientes obligaciones en el marco de la actividad de fiscalización, conforme a lo establecido en los literales a), b), c), d) y e) del artículo 20 del presente reglamento, respectivamente:

- i) Acompañar al personal fiscalizador, cuando este lo requiera, a las fiscalizaciones que se realicen;*
- ii) Brindar todas las facilidades y cooperar para la realización de las verificaciones técnicas que fueran necesarias durante las acciones de fiscalización;*
- iii) Proporcionar toda la información, conforme a la solicitud que efectúa la autoridad fiscalizadora;*
- iv) Permitir el acceso del personal fiscalizador a sus instalaciones y sistemas, cuando sea requerido por esta; o, suscribir el acta correspondiente en aquellos casos en los que intervengan.”*

Esta infracción está referida al incumplimiento de la empresa operadora de las obligaciones vinculadas a permitir y facilitar que el MTC ejerza su potestad fiscalizadora, según lo estipulado en el artículo 20 del Reglamento.

En ese sentido, la calificación de grave se debe a que se trata de disuadir cualquier conducta obstruccionista de las acciones de fiscalización, siendo importante que se concreten las acciones de fiscalización para verificar y constatar el cumplimiento de las obligaciones estipuladas en el presente Reglamento.

- **Por incumplimiento del numeral 6.8 del artículo 6 del Reglamento:**

“La empresa operadora que incumpla con remitir el reporte mensual, según lo establecido en el numeral 6.8 del artículo 6 del presente reglamento.”

Esta infracción está referida al incumplimiento de la empresa operadora de remitir los reportes mensuales sobre el monitoreo de su red de telecomunicaciones, obligación cuya observancia es importante para permitir al MTC la verificación del cumplimiento de las obligaciones estipuladas en los numerales 6.3, 6.4, 6.5 y 6.6 del artículo 6 del Reglamento, referidas a los mecanismos o medidas de monitoreo de red que deben efectuar las empresas operadoras; así como, las comunicaciones que las mismas deben realizar al MTC a partir de las situaciones advertidas producto de dicho monitoreo.

Cabe mencionar que la tipificación de leve obedece a que la obligación de remisión de reportes no está referida directamente al cumplimiento de una obligación sustancial para evitar las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles.

- **Por incumplimiento del numeral 5.5 del artículo 5 del Reglamento:**

“La empresa operadora que incumpla con remitir el listado de estaciones radioeléctricas que emiten señales hacia los establecimientos penitenciarios y centros juveniles, incluyendo la tecnología de cada estación, así como, que incumpla con informar la instalación de nuevas estaciones o la actualización en la tecnología de las mismas, de acuerdo a lo establecido en el numeral 5.5 del artículo 5 del presente reglamento”.

Esta infracción está referida al incumplimiento de la empresa operadora de remitir el listado de estaciones radioeléctricas que emiten señales hacia los establecimientos penitenciarios y centros juveniles, incluyendo la tecnología de cada estación; así como, al incumplimiento de la empresa operadora de informar la instalación de nuevas estaciones que emiten señales radioeléctricas hacia los establecimientos penitenciarios y centros juveniles y las actualizaciones en la tecnología de dichas estaciones, dentro de los cinco (05) días hábiles de haber sido efectuados, conforme con lo establecido en el numeral 5.5. del artículo 5 del Reglamento.

Cabe mencionar que la tipificación de leve obedece a que la obligación de remisión de información no está vinculada directamente al cumplimiento de una obligación sustancial para evitar las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles.

5.3.7. Incentivos para la empresa operadora

Sobre el particular, el Reglamento contiene los siguientes incentivos para las empresas operadoras:

Zona de Exclusión Especial

Al respecto en el Proyecto de Reglamento se contempla la “zona de exclusión especial” lo que se concibe en la situación fáctica que por lo general los establecimientos penitenciarios y centros juveniles se encuentran o colindan con áreas urbanas; por lo que, se corre el riesgo de afectar el acceso y/o calidad de los servicios de telecomunicaciones de las poblaciones aledañas asentadas en mencionados recintos.

Cabe señalar que la “zona de exclusión especial” actualmente existe en el numeral 6.2 del artículo del Protocolo Técnico³³, y en el Proyecto de Reglamento se ha considerado precisarlo y comprender no sólo a los establecimientos penitenciarios sino también a los centros juveniles. Es así que, en el numeral 6.4 del artículo 6 del Protocolo Técnico se modifica lo concerniente a la “zona de exclusión especial”³⁴, según el detalle siguiente:

- En el caso de los establecimientos penitenciarios, dicha zona inicia desde el borde externo de la zona restringida y de alta seguridad y se extiende hasta la distancia de 200 metros a su alrededor.
- En el caso de los centros juveniles, dicha zona comprende 400 metros alrededor del perímetro de dichos centros.

En ese sentido, para los establecimientos penitenciarios se dispone que la distancia que se ha considerado para la “zona de exclusión especial” replica la distancia considerada para la zona restringida y de alta seguridad, toda vez que es necesario mantener un área de flexibilidad para la convivencia de las señales emitidas por las estaciones radioeléctricas y los quipos bloqueadores.

Para los centros juveniles, la “zona de exclusión especial” comprende 400 metros alrededor del perímetro de dichos centros, a fin de que guarde consistencia con la distancia considerada para los establecimientos penitenciarios.

Por tanto, en la “zona de exclusión especial” se considera excluida de los parámetros de cobertura o de calidad del OSIPTEL, así como, de la verificación de obligaciones contractuales y/o administrativas aplicables.

Exoneración de responsabilidad

En el artículo 13 del Proyecto de Reglamento, se dispone la exoneración de responsabilidad por el corte de servicio público móvil y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo a pesar de no haberse realizado un uso prohibido, conforme a lo siguiente:

³³ “(...) 6.2 Se establece una zona de exclusión especial, la misma que inicia desde el borde externo de la Zona de Intangibilidad hasta la distancia donde se verifique niveles de recepción igual a -95 dBm. Esta zona, se considera excluida de los parámetros de cobertura o de calidad del OSIPTEL, así como de la verificación de obligaciones contractuales y/o administrativas aplicables.
 (...)”

³⁴ Ver la Única Disposición Complementaria Modificatoria del Proyecto de Reglamento.

“Cuando la empresa operadora que lleve a cabo el corte del servicio público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo, a pesar de no haberse realizado un uso prohibido, no incurrir en responsabilidad frente al abonado, usuario o arrendatario de servicios públicos de telecomunicaciones, siempre que haya actuado de conformidad con los criterios y procedimientos establecidos en la normativa correspondiente del OSIPTEL.”

Al respecto, considerando que existe un margen de error en la aplicación por parte de la empresa operadora de los criterios de uso prohibido del servicio, dado que, si bien estos brindan indicios razonables de que una llamada se realiza desde un establecimiento penitenciario o centro juvenil, no garantizan al cien por ciento dicha situación, por lo que, atendiendo a ello, se ha previsto la exoneración de responsabilidad de la empresa operadora en caso realice el corte de servicio público móvil y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo a pesar de no haberse realizado un uso prohibido.

5.3.8. Sobre la gestión de los sistemas de restricción de señales de comunicaciones en establecimientos penitenciarios y centros juveniles

Una de las medidas que se plantea en la segunda disposición complementaria y final del Reglamento está referida al establecimiento de obligaciones a cargo de la entidad y/o empresa que gestiona sistemas de restricción señales de comunicaciones.

Sobre el particular, es importante considerar que cuando se alude a sistemas de restricción de señales de comunicaciones, se hace referencia a equipos bloqueadores o inhibidores de señales radioeléctricas u otros sistemas de control de acceso, detección y/o bloqueo de comunicaciones instalados -o que pudieran instalarse a futuro- de manera directa por el Estado o a través de alguna empresa privada, en establecimientos penitenciarios o centros juveniles para garantizar que no se concreten las comunicaciones ilegales desde el interior de estos.

De este modo, se plantean requisitos, características y/o funcionalidades mínimas que deben cumplir los referidos sistemas, tales como los siguientes:

- Impedir y/o restringir cada una de las señales radioeléctricas utilizadas para servicios de telecomunicaciones al interior de dichos recintos, independientemente de la tecnología y el tipo de banda de frecuencia empleadas.
- Impedir y/o restringir las comunicaciones ilegales al interior de dichos recintos, independientemente de la tecnología, medio utilizado, tipo de servicio, entre otros.
- Permitir una configuración independiente por cada banda.
- Contar con un sistema de control y/o monitoreo remoto.
- Cumplir el marco normativo vigente y las normas, protocolos o lineamientos que las entidades competentes emitan sobre los sistemas de restricción de señales de comunicaciones.

Cabe mencionar que las características o funcionalidades mínimas antes indicadas, están orientadas a que los sistemas de restricción de señales de

comunicaciones se adapten a la evolución y cambios tecnológicos; así como, a los diferentes mecanismos que puedan ser utilizados para concretar las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, tomando en cuenta que el sector de las telecomunicaciones es bastante dinámico y exige una continua adaptación a dichos cambios, puesto que, de no hacerlo, se corre el riesgo de que tales sistemas queden desfasados en el tiempo y no cumplan la finalidad para la que fueron implementados.

Ahora bien, cabe precisar que en el caso de los contratos sobre sistemas de restricción de señales de comunicaciones que se encuentran suscritos a la fecha de publicación del presente reglamento, las disposiciones antes mencionadas rigen siempre que los términos contractuales así lo permitan. No obstante, para los contratos que pudieran suscribirse a futuro, se considera que los mencionados sistemas deben cumplir con las disposiciones antes mencionadas.

5.3.9. Sobre el objetivo de reducir progresivamente el número de comunicaciones ilegales

Al respecto, se tiene como objetivo reducir progresivamente el número de comunicaciones ilegales realizadas a través de dispositivos no autorizados desde el interior de los establecimientos penitenciarios y centros juveniles, alcanzando una reducción acumulada del 90% al año 2030.

Para alcanzar dicho objetivo, se han establecido mecanismos regulatorios claros y efectivos que permitan restringir el uso indebido de los servicios públicos de telecomunicaciones en estos establecimientos, contribuyendo a eliminar una de las principales vías para la comisión de delitos desde el interior, por lo que, de esta manera, se busca fortalecer la seguridad pública, mejorar la capacidad de control institucional y alinear la intervención con los objetivos de política pública en materia de seguridad ciudadana.

A fin de medir el progreso hacia el objetivo, se ha definido el siguiente indicador:

“Porcentaje de reducción de comunicaciones ilegales realizadas a través de dispositivos no autorizados desde establecimientos penitenciarios y centros juveniles”.

Este indicador permitirá evaluar de manera anual la disminución en el número de cortes de servicio público móvil y bloqueos de equipos terminales móviles por uso prohibido, así como en la cantidad de equipos terminales incautados durante los operativos de requisa. Es así que, el indicador constituirá una medida indirecta de la reducción de las comunicaciones ilegales, permitiendo un seguimiento sistemático y verificable del cumplimiento del objetivo planteado.

Fórmula:

$$\text{Reducción porcentual anual} = \left(\frac{NCI_{t-1} - NCI_t}{NCI_{t-1}} \right) \times 100\%$$

Donde:

NCI_t = Número total de comunicaciones ilegales detectadas en el año t.

NCI_{t-1} = Número total de comunicaciones ilegales detectadas en el año anterior.

Número total de comunicaciones ilegales detectadas:

- Número de cortes de servicio público móvil por uso prohibido.
- Número de bloqueos de equipos terminales móviles.
- Número de terminales incautados en requisas oficiales.

Frecuencia de medición: Anual.

Fuente de verificación:

- Reporte anual del OSIPTEL sobre cortes de servicio móvil y bloqueos de equipos terminales por uso prohibido.
- Reporte oficial del INPE sobre terminales móviles incautados durante requisas.
- Responsable del indicador: Ministerio de Justicia y Derechos Humanos (MINJUSDH). (Coordinando con OSIPTEL e INPE para consolidar la información).

Logros esperados:

2025	2026	2027	2028	2029	2030
Línea base	75%	80%	85%	88%	90%

Cabe resaltar que, como parte del proceso de identificación de indicadores para medir el objetivo, se evaluaron diversas alternativas que permitieran medir el impacto del proyecto normativo, incluyendo indicadores como la reducción porcentual de llamadas al 111 por presuntos casos de extorsión y la reducción porcentual de denuncias registradas por extorsión. No obstante, se concluyó que estos indicadores presentan una alta sensibilidad a factores exógenos como campañas mediáticas, cambios en la cultura de denuncia, entre otros elementos estacionales, lo cual podría generar una alta volatilidad y dificultar la medición objetiva y constante del impacto real de la norma. En cambio, el indicador seleccionado, permite un seguimiento más directo, técnico y verificable de las intervenciones establecidas en el reglamento, al estar sustentado en datos reportados por entidades competentes como OSIPTEL e INPE, asegurando una medición más robusta y alineada con los resultados esperados del proyecto normativo.

5.3.10. Análisis sobre la necesidad, viabilidad y oportunidad de la norma

a) Análisis de necesidad de la norma

La necesidad del Reglamento se sustenta en que para que las disposiciones establecidas en el Decreto Legislativo N° 1688 sean aplicables y, por ende, se cumpla su finalidad, es necesario su desarrollo a través de medidas específicas y concretas que precisamente serán estipuladas en su reglamento.

Asimismo, tómesese en cuenta que en la segunda disposición complementaria final del Decreto Legislativo N° 1688 se encargó al MTC en coordinación con el OSIPTEL, la aprobación del reglamento de dicha norma, inclusive, en su primera disposición complementaria final se ha supeditado la entrada en vigencia de sus capítulos I y II del Título II, el Título III y la Única Disposición Complementaria Derogatoria, a la publicación de su reglamento, siendo por tanto, imperativo que el MTC dé cumplimiento de dicha disposición.

En atención a ello, en el Reglamento se desarrollan las obligaciones que deberán ser cumplidas para prevenir y/o mitigar la problemática de las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles; así como, se tipifican las infracciones y sanciones aplicables ante el incumplimiento de las mismas, lo cual precisamente garantiza su cumplimiento.

De este modo, a través del Reglamento se contribuirá con la seguridad nacional en el ámbito del orden interno, orden público y seguridad ciudadana, evitando que los internos establezcan comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, lo cual, a su vez, coadyuvará a disminuir la comisión de ilícitos penales vinculados al uso de los servicios de telecomunicaciones, como el fraude, la extorsión, sicariato, secuestro, criminalidad organizada, entre otros, y la gestión del contrabando, como el tráfico ilícito de drogas y de armas de fuego.

b) Análisis de viabilidad de la norma

El Reglamento resulta viable, toda vez que su elaboración se realiza en el marco de lo dispuesto en el Decreto Legislativo N° 1688, siendo esta norma la que precisamente dispone la emisión de dicho reglamento.

Asimismo, las disposiciones del Reglamento se han formulado acorde al marco normativo vigente, tal como lo dispuesto en la Constitución Política del Perú, el TUO de la Ley de Telecomunicaciones, el TUO del Reglamento de la Ley de Telecomunicaciones, la LOF del MTC, entre otras normas, según lo desarrollado en la presente exposición de motivos en las secciones III. Antecedentes y IV. Marco jurídico y las habilitaciones en cuyo ejercicio se dicta.

Asimismo, las medidas establecidas se consideran factibles de ser aplicadas técnicamente, además de ser las más eficientes dada la situación actual de la problemática relacionada a las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, los costos que les corresponde asumir a los actores involucrados y los diferentes factores que influyen en dicha problemática.

En ese sentido, resulta viable que se emita el Reglamento para desarrollar las disposiciones contenidas en el Decreto Legislativo N° 1688.

c) Análisis de oportunidad de la norma

La emisión del Reglamento se considera oportuna puesto que, como mencionamos previamente, en la segunda disposición complementaria final del Decreto Legislativo N° 1688 se encargó al MTC en coordinación con el OSIPTEL, la aprobación del Reglamento de dicha norma, otorgando para ello un plazo de ciento ochenta (180) días calendarios, por lo que resulta imperioso la emisión del mencionado proyecto normativo, a fin de que las disposiciones del referido decreto legislativo puedan ser aplicables.

Asimismo, dado que la problemática de las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles acarrea distintos perjuicios para el orden interno, orden público y seguridad ciudadana, urge la adopción de medidas orientadas a prevenir, controlar y/o mitigar la misma, por lo que es oportuna la emisión del Reglamento que precisamente contiene disposiciones dirigidas a enfrentar la mencionada problemática.

VI. Propuesta normativa

Artículo 1 del Reglamento del Decreto Legislativo N° 1688:

Este artículo contiene el objeto del Reglamento, el cual consiste en desarrollar las disposiciones contenidas en el Decreto Legislativo N° 1688, en consideración a lo establecido en la Segunda Disposición Complementaria Final del mencionado Decreto Legislativo, para su cumplimiento por parte de los sujetos pasivos de su ámbito de aplicación.

Artículo 2 del Reglamento del Decreto Legislativo N° 1688:

Este artículo comprende la finalidad del Reglamento del Decreto Legislativo N° 1688, la cual es prevenir, mitigar y/o controlar la problemática de las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, que permiten delitos tales como: extorsión, fraude, secuestros; entre otros, siendo ello, un mal latente que involucra una lucha contra la inseguridad ciudadana³⁵.

Artículo 3 del Reglamento del Decreto Legislativo N° 1688:

Este artículo comprende las definiciones y abreviaturas que son aplicables en el Reglamento.

Con relación a las abreviaturas se tiene a los órganos de línea o entidades involucradas en el ámbito de aplicación de la normativa como: la **DFGSC** (Dirección General de Fiscalizaciones y Sanciones en Comunicaciones del MTC), **DFCTH** (Dirección de Fiscalización de Cumplimiento de Títulos Habilitantes en Comunicaciones), la **DSANC** (Dirección de Sanciones en Comunicaciones), el **INPE** (Instituto Nacional Penitenciario), el MTC (Ministerio de Transportes y Comunicaciones), el **MINJUSDH** (Ministerio de Justicia y Derechos Humanos), el **MININTER** (Ministerio del Interior), el **OSIPTEL** (Organismo Supervisor de la Inversión Privada en Telecomunicaciones), la **PNP** (Policía Nacional del Perú) y el **PRONACEJ** (Programa Nacional de Centros Juveniles), **UFSCIPS** (Unidad Funcional de Supervisión del Contrato Innominado de Prestación de Servicios).

Con relación a las definiciones se establecen los siguientes términos:

- (i) **Azimut**, es el ángulo que se mide en el plano horizontal, desde un punto de referencia fijo (el norte) en sentido horario, hasta la proyección del eje de radiación de la antena. Se expresa en grados sexagesimales de 0° a 360°.
- (ii) **Empresa(s) que gestiona(n) el sistema de restricción de señales de comunicaciones**, son la(s) persona(s) natural(es) o jurídica(s) responsable (s) de la instalación y/u operación de equipos bloqueadores o inhibidores de señales radioeléctricas, u otros sistemas de control de acceso, detección y/o bloqueo de

³⁵ Ejemplos de esta problemática, se refieren las noticias o notas periodísticas siguientes: **Ojo Público (12 de noviembre de 2023). Quinteros, V. “Tren de Aragua, cárceles y expansión del crimen transnacional”**. El autor señala que, según un reportaje del diario *El Comercio*, desde el E.P. Challapallca, los líderes de la organización de origen venezolano El Tren de Aragua enviaban directivas a sus huéspedes en el exterior a través de mensajes de audio. El caso compromete a Héctor Prieto Materano, alias “Mamut”, uno de los 14 líderes de la organización reclusos en dicho penal. Pero no era la primera vez; según el mismo diario, “Mamut” habría estado involucrado en un hecho similar en el penal de Ancón I, en Lima, donde también pudo acceder a un teléfono celular. Precisa que, este caso debe encender las alarmas a todo nivel, no solo por exponer el limitado control que ejerce la administración penitenciaria sobre la seguridad del penal más inaccesible del país (E.P. Challapallca), sino por revelar la forma en que el crimen organizado transnacional, concretamente El Tren de Aragua, opera desde las cárceles del Perú. Ver en: <https://ojo-publico.com/4756/tren-aragua-carceles-y-expansion-del-crimen-transnacional>

Desde el penal Ancón I cabecillas de bandas coordinaban extorsiones. Delitos agravados. Cabecillas de bandas reclusos en esta cárcel coordinaban también secuestros y asesinatos. Señal de internet salía desde una casa vecina. Ingeniero cobraba servicio a los reclusos (06 de octubre de 2024). Ver en: <https://larepublica.pe/sociedad/2024/10/06/desde-el-penal-ancon-i-cabecillas-de-bandas-coordinaban-extorsiones-411160>

comunicaciones instalados en establecimientos penitenciarios o centros juveniles para impedir las comunicaciones ilegales desde el interior de estos.

En caso una entidad pública tuviera a su cargo directamente la instalación y/u operación de los equipos indicados en el párrafo precedente, se entiende para todos los efectos del presente reglamento que cuando se alude a Empresa(s) que gestiona(n) el sistema de restricción de señales de comunicaciones, se hace referencia a la mencionada entidad.

- (iii) **Empresa(s) operadora(s)**, son la(s) persona(s) natural(es) o jurídica(s) que cuenta(n) con concesión, autorización o registro para prestar o explotar uno o más servicios públicos de telecomunicaciones.
- (iv) **Herramientas de crowdsourcing**, Son plataformas o aplicaciones que permiten obtener datos de un gran número de personas (generalmente por internet), se soportan en el uso que las personas hagan de dichas aplicaciones o plataformas.
- (v) **Log(s)**, archivo o sistema de registros cronológicos donde se documenta eventos, cambios o la actividad que se realiza en un sistema de red.
- (vi) **Protocolo Técnico**, el marco que regula las condiciones de operación de los equipos bloqueadores de señales radioeléctricas y de los servicios de telecomunicaciones en los exteriores de los establecimientos penitenciarios, aprobado mediante Resolución Ministerial N° 954-2016-MTC/01.03 o norma que la sustituya, Se establece en la modificatoria de su artículo 6 que los parámetros de señales radioeléctricas de los equipos de telecomunicaciones de las operadoras y de los equipos bloqueadores, resultan aplicables a los centros juveniles.
- (vii) **Sistema(s) de geolocalización**, son sistemas que emplean tecnologías capaces de determinar la ubicación geográfica de un objeto o dispositivo en tiempo real y/o dentro de un área específica delimitada, mediante el uso de uno o más métodos de posicionamiento o técnicas de análisis de datos, tales como redes de telefonía móvil, redes Wi-Fi, Sistema de Posicionamiento Global (GPS), sistemas globales de navegación por satélite (GNSS), técnicas de aprendizaje automático (machine learning), análisis de grandes volúmenes de datos (big data), entre otros.
- (viii) **Sistema(s) de restricción de señales de comunicaciones**, son sistemas de equipos bloqueadores o inhibidores de señales radioeléctricas, u otros sistemas de control de acceso, detección y/o bloqueo de comunicaciones instalados dentro o fuera de establecimientos penitenciarios o centros juveniles para impedir las comunicaciones ilegales desde el interior de estos.
- (ix) **Throughput**, es la tasa efectiva de transferencia de datos expresada en bits por segundo (bps), representa la capacidad útil de canal de transmisión.

Artículo 4 del Reglamento del Decreto Legislativo N° 1688:

Este artículo concierne a las entidades públicas y privadas sujetas al ámbito de aplicación del Reglamento del Decreto Legislativo N° 1688 como: (i) la(s) empresa(s) operadora(s) que son los agentes centrales que coadyuvarán al cumplimiento del objetivo del marco normativo; (ii) la(s) empresa(s) que gestionan el sistema de restricción de señales de comunicaciones que son actores involucrados en la lucha contra las comunicaciones ilegales en los establecimientos penitenciarios y en los centros juveniles; así como, (iii) las entidades inmersas en el Sector Comunicaciones, en el Sistema Penitenciario Nacional y al Sistema Nacional de Reinserción Social, que implica las autoridades que gestionen, supervisen y/o fiscalicen el desarrollo de la aplicación del Decreto Legislativo N° 1688.

Artículo 5 del Reglamento del Decreto Legislativo N° 1688:

Este artículo desarrolla el numeral 8.1 del artículo 8 del Decreto Legislativo N° 1688 que establece, las empresas operadoras restringen las señales radioeléctricas de los servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles del país a nivel nacional, salvo excepciones por necesidades de seguridad, previéndose que la restricción de señales radioeléctricas se realiza conforme a lo establecido en su Reglamento.

En ese contexto, en el numeral 5.1 del artículo 5, se dispone que, *“De acuerdo con el numeral 8.1 del artículo 8 del Decreto Legislativo, la empresa operadora restringe la emisión de su señal radioeléctrica de los servicios públicos de telecomunicaciones hacia los establecimientos penitenciarios y centros juveniles, salvo excepciones por necesidades de seguridad cuando así lo determine la entidad competente en el ámbito de sus funciones y/o atribuciones, cautelando que no se afecte el derecho de acceso a los servicios públicos de telecomunicaciones de las poblaciones aledañas.”*

Al respecto, este postulado implica el mandato que la empresa operadora limite o reduzca sus señales radioeléctricas³⁶, previéndolo que no se afecte el acceso a los servicios públicos de telecomunicaciones de los ciudadanos que coexisten en la periferia de mencionados espacios de reinserción social.

Así pues, el numeral 5.2 del artículo 5, se considera que, en los establecimientos penitenciarios y centros juveniles rigen los aspectos y/o parámetros acordados entre la empresa operadora y la empresa que gestiona dichos sistemas, de acuerdo con lo establecido en el mismo Reglamento, puesto que, la situación fáctica es que la red móvil implica una señal dinámica no estática, y depende, del desarrollo y/o evolución de las tecnologías a través de las cuales prestan los servicios públicos de telecomunicaciones las empresas operadoras, así como, de factores de infraestructura o ubicación geográfica en que se encuentren los establecimientos penitenciarios y los centros juveniles, para que haya un equilibrio entre las empresas que gestionan los sistemas de restricción de señales de comunicaciones y las empresas operadoras, y no se afecte en desmedida el acceso a los servicios públicos de telecomunicaciones de las poblaciones aledañas, siendo que, a falta de acuerdo entre ambas partes, según lo dispuesto en el marco normativo, rigen los parámetros de señales radioeléctricas establecidos en el Protocolo Técnico³⁷.

Por otra parte, en los numerales 5.3 y 5.4 del artículo 5, se especifica condiciones para el cumplimiento de los numerales 5.1 y 5.2. En esa línea, se prevé que, la empresa operadora debe realizar las adecuaciones técnicas necesarias en sus estaciones radioeléctricas; entre otras, cambios de tilt, azimut, altura, potencia, así como, de ser necesario, se efectúe el reemplazo de estaciones; y en el caso, la empresa operadora instalen nuevas estaciones radioeléctricas o implementen nuevas tecnologías o actualizaciones sobre sus estaciones existentes, cumplen con las disposiciones previstas en los numerales 5.1 y 5.2, respectivamente.

Con relación al numeral 5.5. del artículo 5, se ha estipulado que la empresa operadora dentro de los treinta (30) días calendario de publicado el reglamento, remite a la DFCTH el listado de las celdas de las estaciones radioeléctricas, cuyas señales irradian hacia los establecimientos penitenciarios y centros juveniles, incluyendo la tecnología y frecuencia de operación de cada celda. Asimismo, la empresa operadora informa a la DFCTH la instalación de nuevas celdas y la actualización de las existentes, cuyas

³⁶ Conforme a la Real Academia Española la palabra restringir se define como: 1. tr. Ceñir, circunscribir, reducir a menores límites, y 2. tr. Apretar, constreñir, restringir. Ver en: <https://dle.rae.es/restringir>

³⁷ Casuística considerada de la evaluación técnica realizada por el MTC y de las reuniones sostenidas con las empresas operadoras y con la empresa que gestiona el sistema de los equipos bloqueadores (Prisontec S.A.C.) en el marco de la “Mesa técnica para implementar medidas orientadas a prevenir las comunicaciones ilegales”.

señales irradian hacia los establecimientos penitenciarios y centros juveniles, dentro de los cinco (05) días hábiles de haber sido efectuados.

Para el efecto, las empresas operadoras deben resguardar los registros logs de cambios, actualizaciones y/o modificaciones de las celdas de las estaciones radioeléctricas, cuyas señales irradian hacia los establecimientos penitenciarios y centros juveniles, por un período de treinta y seis (36) meses contabilizados desde que se realicen las mencionadas acciones, con la finalidad de que se efectúe la debida supervisión y/o fiscalización por parte de la DFCTH.

Por su parte, en el numeral 5.6, se establece que en caso la DFCTH advierta que la empresa operadora no cumple con restringir su señal radioeléctrica, conforme a lo establecido en los numerales precedentes, comunica a esta, mediante el acta correspondiente, con copia a la empresa que gestiona el sistema de restricción de señales de comunicaciones, el MINJUSDH y/o el INPE, según corresponda, a efectos de que la operadora adopte las acciones correspondientes que garanticen y demuestren la restricción de la señal, sin perjuicio de la responsabilidad administrativa que le corresponda asumir.

Para ello, se ha considerado pertinente diferenciar el plazo de cumplimiento de la restricción de señales, en función de las actividades que debe realizar la empresa operadora ya sea en campo o en gabinete. Así, se establece que la empresa operadora adopta las acciones correspondientes, en el plazo de dos (02) días calendarios, tratándose de cambios lógicos y, de cinco (05) días calendarios, tratándose cambios físicos.

Para acreditar las acciones realizadas, la empresa operadora presenta a la DFCTH dentro de las cuarenta y ocho (48) horas siguientes a haber efectuado las acciones correspondientes, las evidencias que demuestren el cumplimiento del numeral 5.2 del presente artículo, sin perjuicio de la facultad fiscalizadora que le corresponde a la DFCTH.

Con relación al numeral 5.7 del artículo 5, se contempla que la empresa que gestiona el sistema de restricción de señales de comunicaciones, bajo responsabilidad, brinda a la DFCTH el acceso remoto al sistema de gestión de los equipos bloqueadores u otros sistemas instalados en los establecimientos penitenciarios y centros juveniles, según corresponda, en perfil de lectura, a fin de que permita realizar las acciones de fiscalización para verificar las características de funcionamiento, bandas de frecuencia, niveles de potencia, entre otros, en el marco de sus competencias.

Para el inicio del acceso antes mencionado, la empresa que gestiona el sistema de restricción de señales de comunicaciones, brinda las credenciales correspondientes en el plazo de tres (03) días hábiles contados desde la entrada en vigencia del presente reglamento.

Para el caso de la empresa que gestiona el sistema de restricción de señales de comunicaciones, este acceso es condición para que la DGFSC otorgue la constancia inicial de no interferencia de acuerdo con el Protocolo Técnico, medida que se ha considerado para fortalecer la lucha contra las comunicaciones ilegales desde el interior de establecimientos penitenciarios y centros juveniles, y teniendo en cuenta que conforme al artículo 4 del Decreto Legislativo N° 1688, este marco normativo se aplica también para las entidades privadas que participen o estén vinculadas al Sistema Penitenciario Nacional y al Sistema Nacional de Reinserción Social.

Finalmente, se establece que el software del sistema de gestión de la empresa que gestiona el sistema de restricción de señales de comunicaciones, cuyo acceso brinda a la DFCTH, almacena los logs de cambios, eventos, alarmas, actualizaciones y/o modificaciones de las señales radioeléctricas, que irradian en los establecimientos penitenciarios y centros juveniles, acorde a lo dispuesto en el contrato que haya suscrito para la gestión y/u operación de los sistemas de restricción de señales de comunicaciones, según corresponda.

Respecto al numeral 5.8 del artículo 5, se establece una zona de exclusión donde la empresa operadora se encuentra excluida de responsabilidad según lo establecido en el Protocolo Técnico, en consideración que las señales de la red móvil son de índole dinámica y es factible que por factores externos o se corre el riesgo de generar cierta afectación al acceso y/o calidad de los servicios de telecomunicaciones de las poblaciones aledañas.

Artículo 6 del Reglamento del Decreto Legislativo N° 1688:

Este artículo desarrolla el numeral 8.2 del artículo 8 del Decreto Legislativo N° 1688, el cual establece que las empresas operadoras adoptan mecanismos que impidan las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles, así como que coadyuven a los sistemas y/o equipos de seguridad tecnológica implementados por las entidades competentes.

En el numeral 6.1 del artículo 6 se precisa que, la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones, coordinan los aspectos técnicos necesarios, a fin de que no se concreten las comunicaciones ilegales desde establecimientos penitenciarios o centros juveniles y, a su vez, no se genere afectación a los servicios públicos de telecomunicaciones de las poblaciones aledañas a estos. Las coordinaciones antes mencionadas pueden ser iniciadas por cualquiera de las referidas empresas.

Para tal efecto, la empresa operadora comunica a la DFCTH el inicio de las coordinaciones con la empresa que gestiona el sistema de restricción de señales de comunicaciones y la empresa operadora.

Con este mecanismo se pretende evitar que concreten comunicaciones ilegales desde los establecimientos penitenciarios y centros juveniles, propendiendo a que no se afecten las poblaciones aledañas, se procura garantizar que se efectúen las coordinaciones la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones para afianzar la eficacia de los sistemas y/o equipos de seguridad tecnológica,

Con relación al numeral 6.2 del artículo 6, se determina que producto de las coordinaciones entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones se debe llegar a un acuerdo entre ambas partes, conciliando los parámetros la señal radioeléctrica involucrada, entre otros aspectos, lo cual debe ser informado al detalle por la empresa operadora a la DFCTH y la UFSCIPS en un plazo de cinco (05) días hábiles de haber sido adoptado acompañado por las pruebas de desempeño de red del entorno donde se verifique las condiciones de cobertura. Asimismo, cualquier modificación al acuerdo adoptado es comunicada a la DFCTH y la UFSCIPS en el mismo plazo antes mencionado.

En caso la empresa operadora no comunique a la DFCTH el mencionado acuerdo o sus modificaciones, para todo efecto, se considerará que rigen los parámetros establecidos en el Protocolo Técnico o los parámetros inicialmente acordados, respectivamente.

Se entiende que no se ha llegado a un acuerdo entre la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones, luego de transcurrido treinta (30) días calendario de iniciadas las coordinaciones, por lo tanto, la empresa operadora y la empresa que gestiona el sistema de restricción de señales de comunicaciones, deberán aplicar los parámetros establecidos en el Protocolo Técnico.

En los numerales 6.3 al 6.8 del artículo 6, se establece que la empresa operadora implemente lo siguiente: (1) medidas de monitoreo permanente de su red de telecomunicaciones, en base a niveles de indicadores de nivel de ruido, potencia de recepción, throughput, entre otros, que coadyuvará a determinar la funcionalidad u operatividad de los sistemas de restricción de señales de comunicaciones instalados en los establecimientos penitenciarios y centros juveniles; y, (2) mecanismos de monitoreo permanente de red, entre otras, a través de herramientas de crowdsourcing, así como análisis de sistemas de geolocalización que realicen seguimiento de los accesos y/o intentos de conexión a su red que se encuentren, que realicen seguimiento de los accesos y/o intentos de conexión a su red que se encuentren dentro del área de los establecimientos penitenciarios y centros juveniles.

En el contexto de los mencionados mecanismos, se contempla que en el plazo de veinticuatro (24) horas, la empresa operadora comunique lo siguiente:

- (a) Si producto de la implementación de las referidas medidas de monitoreo, se advierte parámetros inusuales que indique un deficiente funcionamiento u operatividad de los equipos de bloqueo, comunicar al MTC, MINJUSDH e INPE, a fin de que adopten las acciones pertinentes dentro del marco de sus competencias.
- (b) Si producto de la implementación de los mecanismos de monitoreo, se advierte parámetros inusuales que brinde indicios de acceso y/o intentos de conexión a su red dentro de los establecimientos penitenciarios y centros juveniles, comunicar al OSIPTEL, MTC, MINJUSDH e INPE, a fin de que se adopten las acciones pertinentes dentro del marco de sus competencias.

Se estima prudente que en el plazo de treinta (30) días calendario de la entrada en vigencia del Reglamento, la empresa operadora presenta a la DFCTH, el detalle de las referidas medidas y mecanismos de monitoreo, para el buen desarrollo de la facultad de supervisión y fiscalización del MTC.

En esa misma línea, se prevé que la empresa operadora remita un reporte mensual a la DGFSC, hasta el quinto día hábil de cada mes, que contenga información del mes inmediato anterior sobre los registros obtenidos y alertas generadas producto de los referidos monitoreos, según los formatos contenidos en el Anexo del presente Reglamento.

Finalmente, en el numeral 6.9 se prevé que dentro del plazo de quince (15) días hábiles de la entrada en vigencia del reglamento, la DGFSC, el MINJUSDH y el INPE comunican a las empresas operadoras móviles los medios idóneos a fin de que dichas empresas cumplan con realizar la comunicación establecida en los numerales 6.4 y 6.6, lo cual debe ser comunicado a la empresa operadora.

Artículo 7 del Reglamento del Decreto Legislativo N° 1688:

Sobre el particular, este artículo se encuentra como parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros

juveniles, comprendiendo que el uso prohibido del servicio público de telecomunicaciones corresponde a:

- El uso de servicios públicos de telecomunicaciones en establecimientos penitenciarios o centros juveniles, distintos a los contratados por el MINJUSDH, el INPE y/o el PRONACEJ, incluyendo este supuesto, el uso de los servicios públicos de telecomunicaciones de voz, datos y/o mensajería, distintos a los contratados por el INPE y el PRONACEJ, a través de cualquier dispositivo que permita la conexión directa o indirecta a la red de telecomunicaciones dentro de los establecimientos penitenciarios o centros juveniles; así como, a los servicios de telecomunicaciones distintos a los prestados por las empresas operadoras que permiten el acceso a dichas conexiones.
- El uso de servicios públicos de telecomunicaciones en zonas restringidas y de alta seguridad para establecer o facilitar comunicaciones con fines delictivos.

Artículo 8 del Reglamento del Decreto Legislativo N° 1688:

Este artículo se encuentra inmerso como desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, el cual contempla que, el OSIPTEL aprueba las normas que establezcan los criterios que las empresas operadoras utilicen para determinar el uso prohibido de un servicio público de telecomunicaciones, disponiendo que dichos criterios y cualquier modificación que realice el OSIPTEL, sean comunicados a las empresas operadoras, previo a su aplicación. Asimismo, se establece que la empresa operadora que, mediante el uso de mecanismos de monitoreo permanente, detecte accesos y/o intentos de conexión a la red móvil dentro de los establecimientos penitenciarios o centros juveniles, debe efectuar el corte del servicio público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo de manera inmediata, de acuerdo a los criterios que apruebe el OSIPTEL para tal efecto.

Artículo 9 del Reglamento del Decreto Legislativo N° 1688:

Este artículo también es parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, mediante el cual, se regula que la empresa operadora procede al corte del servicio y/o el bloqueo del equipo terminal, cuando corresponda, conforme al procedimiento aprobado por el OSIPTEL, y se dispone que dentro de las veinticuatro (24) horas de realizado el corte del servicio y/o bloqueo del equipo terminal, las empresas operadoras comuniquen al OSIPTEL y al MINJUSDH, la siguiente información: (1) nombres y apellidos del abonado afectado; (2) número del servicio público de telecomunicaciones afectado; (3) número de Serie Electrónica (Electronic Serial Number - ESN, International Mobile Equipment Identity - IMEI, u otro equivalente) que identifica el equipo terminal bloqueado; y, (4) las causales que motivaron el corte del servicio y bloqueo del equipo terminal, información remitida para su conocimiento y se tomen las medidas, según corresponda, en el marco de sus competencias y funciones, respectivamente; y, (5) otros parámetros a ser definidos por el OSIPTEL.

Artículo 10 del Reglamento del Decreto Legislativo N° 1688:

Del mismo modo, este artículo forma parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 referido al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, a través del cual, se regula los mecanismos de alerta, contemplando un mensaje de alerta a sus abonados por parte de la empresa operadora, cuando aquellos reciban comunicaciones que se encuentren en alguno de los supuestos de uso prohibido del servicio público de telecomunicaciones, disponiéndose que el mecanismo utilizado para el envío de mensaje de alerta, así como, el contenido del mensaje, es aprobado por el OSIPTEL.

Artículo 11 del Reglamento del Decreto Legislativo N° 1688:

Este artículo también es parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, concerniente al reporte de servicios con alto índice de mensajes de alerta, estableciéndose que, las empresas operadoras remitan a la PNP y al INPE, dentro del plazo que OSIPTEL establezca, el listado de servicios públicos móviles, así como los IMEI de los equipos terminales móviles u otros dispositivos de naturaleza similar, que registren un índice elevado de emisión de advertencias, lo que se estima para el seguimiento y levantamiento de información, a fin de que se tomen las acciones y/o medidas que ameriten; según corresponda, en el ámbito de sus competencias y funciones, respectivamente.

Artículo 12 del Reglamento del Decreto Legislativo N° 1688:

Del mismo modo, este artículo forma parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 referido al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, mediante el cual, se regula lo concerniente a la reactivación del servicio público móvil y/o desbloqueo de equipo terminal móvil o terminal inalámbrico fijo por corte por presunto uso prohibido, estipulando que, la empresa operadora que haya procedido en forma injustificada al corte del servicio y/o bloqueo del equipo terminal por un presunto uso prohibido del servicio, debe proceder a reactivar el servicio y/o desbloquear el equipo terminal del abonado en un plazo máximo de veinticuatro (24) horas, plazo inmediato que se concibe para no causar una mayor afectación o malestar al abonado, máxime si no correspondía realizar dicho corte y/o bloqueo.

En ese contexto, se dispone que aquello resulta aplicable, en los casos que el abonado en un plazo no mayor de cinco (5) días hábiles luego de realizado el corte del servicio por uso prohibido, se acerque a la oficina o centro de atención de la empresa operadora portando el equipo terminal bloqueado y el SIM Card asociado al servicio cortado, cuestionando el referido corte, o cuando tenga un pronunciamiento favorable en el procedimiento de reclamo establecido por el OSIPTEL, previo procedimiento necesario, para verificar y/o corroborar un corte y/o bloqueo que no debió realizarse.

En el mencionado artículo, también se prevé que, la empresa operadora debe comunicar estos hechos al OSIPTEL y al MINJUSDH, dentro de los cinco (5) días hábiles del mes siguiente a la reactivación del servicio público móvil y/o desbloqueo del equipo terminal, conteniendo la siguiente información: (i) nombres y apellidos del abonado, (ii) número y tipo de documento legal de identificación del abonado, (iii) número del servicio afectado, (iv) número de serie (NS) del equipo terminal, y (v) fecha y hora de la reactivación del servicio y desbloqueo del equipo terminal, para el control y/o seguimiento, según corresponda.

Cabe señalar que esta disposición, se encuentra prevista actualmente en el numeral 2.4 del Anexo 8 sobre suspensión, corte y terminación de los servicios públicos de telecomunicaciones de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones aprobada por Resolución de Consejo Directivo N° 172-2022-CD/OSIPTEL, siendo esta, asimilada en el Reglamento del Decreto Legislativo N° 1688, y una disposición de índole similar, se encontraba contemplada en el artículo 6 del Decreto Supremo N° 006-2011-JUS, Decreto Supremo que modifica el Reglamento del Código de Ejecución Penal (en adelante, el Decreto Supremo N° 006-2011-JUS), artículo que fue derogado en la Única Disposición Complementaria Derogatoria del Decreto Legislativo N° 1688.

Artículo 13 del Reglamento del Decreto Legislativo N° 1688:

Este artículo también es parte del desarrollo del Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al uso prohibido de servicios públicos de telecomunicaciones en los establecimientos penitenciarios y centros juveniles, que regula la exoneración de responsabilidad por el corte de servicio público móvil y/o el bloqueo del equipo terminal móvil o terminal fijo inalámbrico³⁸.

En este dispositivo se prevé que, las empresas operadoras que lleven a cabo el corte del servicio público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo, a pesar de no haberse realizado un uso prohibido, no incurrirán en responsabilidad frente al abonado, usuario o arrendatario de servicios públicos de telecomunicaciones, siempre y cuando, hayan actuado de conformidad con los criterios y procedimientos establecidos en la normativa correspondiente que emita para el efecto, el OSIPTEL, y se determina la prohibición de que se efectúe cualquier cobro por el periodo en el que el servicio público de telecomunicaciones estuvo con corte, por parte de la empresa operadora, como un lineamiento de ecuanimidad para los abonados que se hayan o se encuentren afectados por un corte y/o bloqueo que no le correspondía.

Artículos 14 y 15 del Reglamento del Decreto Legislativo N° 1688:

Dichos dispositivos desarrollan el Capítulo II del Título II del Decreto Legislativo N° 1688 concerniente al acceso a la información de equipos terminales móviles y SIM Card incautados en requisas.

En ese contexto, se contempla las autoridades que pueden solicitar datos relacionados a los equipos terminales móviles encontrados en establecimientos penitenciarios o en centros juveniles, siendo las siguientes³⁹:

- (i) El Ministerio Público, o la unidad especializada de la PNP, indistintamente; autoridades competentes para la persecución del delito, siempre constituya un medio necesario para la investigación penal.
- (ii) La Dirección de Seguridad Penitenciaria del INPE, respecto de los equipos terminales móviles encontrados en establecimientos penitenciarios en el marco de lo dispuesto en los artículos 68 y 69 del Reglamento del Código de Ejecución Penal aprobado con Decreto Supremo N° 015-2003-JUS.

³⁸ Al respecto, se señala que en el artículo 4 del Decreto Supremo N° 006-2011-JUS se establecía, la exclusión de responsabilidad de las empresas operadoras cuando se corte el servicio y/o se bloquee el equipo terminal móvil, en caso de uso prohibido, estipulando que, en caso las empresas operadoras procedan al corte del servicio público móvil y/o bloqueo del equipo terminal móvil no obstante no haberse realizado un uso prohibido del servicio, éstas no incurrirán en responsabilidad siempre que hayan procedido de conformidad con los criterios y el procedimiento establecidos en la correspondiente directiva; sin perjuicio de lo dispuesto en el artículo 6 del referido Decreto Supremo, siendo este artículo derogado en la Única Disposición Complementaria Derogatoria del Decreto Legislativo N° 1688.

³⁹ Artículo 14 del Reglamento del Decreto Legislativo N° 1688.

Los datos relacionados a los equipos terminales móviles encontrados en establecimientos penitenciarios o en centros juveniles, que se pueden solicitar, son los siguientes:

- a) Datos de titularidad del equipo terminal móvil y del abonado asociado a la tarjeta SIM Card.
- b) Reporte de llamadas entrantes y salientes.

Asimismo, se contempla los requisitos y plazos de atención con relación al acceso a la información de equipos terminales y Sim Card incautados en requisas, previéndose lo siguiente⁴⁰:

- (1) El Ministerio Público, la unidad especializada de la PNP, o la Dirección de Seguridad Penitenciaria del INPE, cursan la solicitud materia del caso, a la empresa operadora, a través del correo electrónico institucional u otro medio idóneo convenido.
- (2) Se debe adjuntar a la referida solicitud, únicamente, el Acta de Decomiso de Artículos Prohibidos, y los datos que permitan identificar el equipo terminal móvil y la tarjeta SIM Card encontrados en el establecimiento penitenciario o centro juvenil.
- (3) La entrega de dichos datos se realiza dentro de los siete (7) días calendario siguientes de realizada la solicitud.
- (4) La empresa operadora está obligada a conservar los referidos datos por treinta y seis (36) meses en un sistema de almacenamiento electrónico⁴¹.

Artículos 16 al 23 del Reglamento del Decreto Legislativo N° 1688:

Dichos dispositivos desarrollan el Título III del Decreto Legislativo N° 1688 referido a la potestad fiscalizadora y sancionadora del MTC.

En ese ámbito, el artículo 16 del Reglamento del Decreto Legislativo N° 1688 regula las acciones de fiscalización que realice el MTC a través de la DFCTH, el artículo 17 contempla la solicitud de fiscalizaciones con comunicación previa, el artículo 18 comprende las fiscalizaciones inopinadas, el artículo 19 prevé la programación de las acciones de fiscalización, el artículo 20 regula las obligaciones de las empresas operadoras, y el artículo 21 establece la firma del acta de fiscalización.

Por su parte, los artículos 22 y 23 del Reglamento del Decreto Legislativo N° 1688, regulan la potestad sancionadora del MTC y se determina la tipificación de infracciones.

Artículos 24 y 25 del Reglamento del Decreto Legislativo N° 1688:

Dichos dispositivos desarrollan el Título III del Decreto Legislativo N° 1688 referido a la potestad fiscalizadora y sancionadora del OSIPTEL.

Sobre el particular, el artículo 76 del TUO de la Ley de Telecomunicaciones establece que el OSIPTEL, 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.

Asimismo, el artículo 1 de la Ley de Desarrollo de las Funciones y Facultades del OSIPTEL – Ley N° 27336, establece que, es objeto de esta Ley, definir y delimitar las facultades del OSIPTEL, para supervisar y sancionar a las personas naturales o

⁴⁰ Artículo 15 del Reglamento del Decreto Legislativo N° 1688.

⁴¹ Ver su fundamento técnico de dichos articulados en el numeral 5.3.3 de la presente Exposición de Motivos.

jurídicas que prestan servicios públicos de telecomunicaciones, en lo que respecta a su competencia; y, establecer las instancias competentes para los respectivos procedimientos administrativos.

El artículo 40 del Reglamento General del OSIPTEL dispone que, la función fiscalizadora y sancionadora permite al OSIPTEL imponer sanciones y medidas correctivas a las empresas operadoras y demás empresas o personas que realizan actividades sujetas a su competencia por el incumplimiento de las normas aplicables, de las regulaciones y de las obligaciones contenidas en los contratos de concesión.

Asimismo, mediante la Resolución de Consejo Directivo N° 00229-2021-CD/OSIPTEL, se aprobó la Metodología para el Cálculo para la Determinación de Multas en los Procedimientos Administrativos Sancionadores tramitados ante el OSIPTEL.

En ese ámbito, los artículos 24 y 25 del Reglamento regula la potestad fiscalizadora y sancionadora del OSIPTEL, y se tipifican las infracciones bajo el ámbito de competencia y funciones del OSIPTEL, respectivamente.

Primera Disposición Complementaria Final del Reglamento del Decreto Legislativo N° 1688:

Se considera disposiciones y/u obligaciones con relación a la gestión de los sistemas de restricción de señales de comunicaciones en establecimientos penitenciarios y centros juveniles, en aras de salvaguardar una eficiente lucha contra las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles, y equilibrar la sinergia de los actores y elementos involucrados para prevenir o mitigar dicha problemática:

En ese ámbito, se comprende que, los sistemas de restricción de señales de comunicaciones implementados en los establecimientos penitenciarios y centros juveniles, como mínimo cumplen con los siguientes requisitos: (1) Impedir y/o restringir cada una de las señales radioeléctricas utilizadas para servicios de telecomunicaciones al interior de dichos recintos, independientemente de la tecnología y el tipo de banda de frecuencia empleadas; (2) Permitir una configuración independiente por cada banda; (3) Contar con un sistema de control y/o monitoreo remoto; y, (4) Cumplir el marco normativo vigente y las normas, protocolos o lineamientos que las entidades competentes emitan sobre los sistemas de restricción de señales de comunicaciones.

En ese contexto, la entidad y/o empresa que se encuentra a cargo del sistema de restricción de señales de comunicaciones, realiza las actualizaciones tecnológicas que fueran necesarias, teniendo en cuenta que la red de voz y/o datos es dinámica y evolutiva con el paso del tiempo.

Cabe tener en cuenta que, en caso de los contratos sobre sistemas de restricción de señales de comunicaciones que se encuentran suscritos a la fecha de publicación del Reglamento, las disposiciones previstas rigen siempre que los términos contractuales así lo permitan, con la finalidad de no transgredir los actos jurídicos celebrados en su oportunidad.

Segunda Disposición Complementaria Final del Reglamento del Decreto Legislativo N° 1688:

En esta disposición se establece que, en el caso de los establecimientos penitenciarios o centros juveniles que no cuentan con sistemas de restricción de señales de comunicaciones, no resultan exigibles los parámetros establecidos en el Protocolo

Técnico hasta que dichos sistemas hayan sido implementados y se encuentren operativos.

Tercera Disposición Complementaria Final del Reglamento del Decreto Legislativo N° 1688:

En esta disposición se establece que el MTC se encuentra facultado, mediante resolución ministerial, a modificar o reemplazar el contenido del Protocolo Técnico que regula las condiciones de operación de los equipos bloqueadores de señales radioeléctricas y de los servicios de telecomunicaciones en los exteriores de los establecimientos penitenciarios, aprobado mediante Resolución Ministerial N° 954-2016-MTC/01.03.

Cuarta Disposición Complementaria Final del Reglamento del Decreto Legislativo N° 1688:

En esta disposición se establece que el MTC se encuentra facultado a aprobar mediante resolución ministerial protocolos técnicos adicionales y necesarios referidos a sistemas de restricción de señales de comunicaciones u otros sistemas que posteriormente puedan ser implementados para prevenir, mitigar y/o controlar las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles.

Quinta Disposición Complementaria Final del Reglamento del Decreto Legislativo N° 1688

En esta disposición, se establece que la empresa operadora puede solicitar al MINJUSDH información sobre el listado de los establecimientos penitenciarios y centros juveniles, incluyendo las ubicaciones, perímetros y coordenadas. Asimismo, el MINJUSDH remite la información antes mencionada dentro del plazo de cinco (05) días hábiles de recibida la solicitud.

Dicha disposición permitirá a las operadoras contar con información fehaciente sobre los establecimientos penitenciarios y centros juveniles para la adecuada aplicación de las obligaciones y medidas establecidas en el Reglamento.

Sexta Disposición Complementaria Final: se otorga un plazo no mayor de sesenta (60) días hábiles desde la entrada en vigencia del presente reglamento, para que el OSIPTEL apruebe los criterios que la empresa operadora utiliza para realizar el corte del servicio público de telecomunicaciones y/o el bloqueo del equipo terminal móvil o terminal inalámbrico fijo en el marco del uso prohibido; así como, cuando detecte accesos y/o intentos de conexión a la red móvil dentro de los establecimientos penitenciarios o centros juveniles, el procedimiento para el corte del servicio y/o bloqueo del equipo terminal móvil o terminal inalámbrico fijo, el mecanismo utilizado para el envío de mensaje de alerta; así como, el contenido del mensaje.

Séptima Disposición Complementaria Final: se otorga un plazo no mayor de sesenta (60) días hábiles desde la entrada en vigencia del presente reglamento, para que el Ministerio Público, la unidad especializada de la PNP, la Dirección de Seguridad Penitenciaria del INPE, previa coordinación con las empresas operadoras, para la elaboración y aprobación de los protocolos para el mejor acceso de los datos.

Octava Disposición Complementaria Final: se otorga un plazo no mayor de sesenta (60) días hábiles desde la entrada en vigencia del presente reglamento, para que el MTC actualice el Anexo del Protocolo de Medición del Protocolo Técnico que regula las condiciones de operación de los equipos bloqueadores de señales radioeléctricas y de

los servicios de telecomunicaciones en los exteriores de los establecimientos penitenciarios, aprobado mediante Resolución Ministerial N° 954-2016-MTC/01.03.

Única Disposición Complementaria Modificatoria del Reglamento del Decreto Legislativo N° 1688:

En este apartado se modifica los artículos 2 y 6 del Protocolo Técnico que contiene el ámbito de aplicación del mismo, así como, los parámetros técnicos de las señales radioeléctricas de los equipos de telecomunicaciones de las operadoras y de los equipos bloqueadores, respectivamente.

Cabe señalar que, en esta modificatoria se comprende no solo a los establecimientos penitenciarios, se incluye a los centros juveniles, en razón al objeto del Decreto Legislativo N° 1688.

Única Disposición Complementaria Transitoria del Reglamento del Decreto Legislativo N° 1688:

En mencionadas disposiciones se contemplan los siguientes plazos:

Única Disposición Complementaria Transitoria: se establece un plazo no mayor de noventa (90) días calendario desde la entrada en vigencia del presente reglamento, para que las empresas operadoras, las entidades públicas y las empresas que gestionan el sistema de restricción de señales de comunicaciones, dentro del ámbito de aplicación del presente reglamento, se adecúen al cumplimiento de las obligaciones y disposiciones de esta norma.

VII. Análisis de impactos cuantitativos y/o cualitativos de la norma

Esta sección aborda la identificación de las ventajas y desventajas de cada alternativa de solución, seguida de un análisis detallado de los costos y beneficios asociados; así como, concluye con un análisis multicriterio que nos permite seleccionar con mayor efectividad la alternativa más adecuada, después de haber evaluado cada una de las alternativas:

Alternativa 1: Instalación de celdas dummy

Esta alternativa técnica corresponde a una configuración específica de las estaciones base, diseñada para "engañar" al dispositivo móvil del usuario.

En la práctica, el dispositivo del usuario se conecta a una estación base cuya configuración impide la transmisión de información, lo que puede resultar en mensajes como "Red Ocupada" o en la imposibilidad de acceder a cualquier servicio de comunicación. Para implementar esta solución, se requiere instalar una red de celdas distribuidas que asegure una cobertura óptima del área del establecimiento penitenciario o centro juvenil, esto debe realizarse por cada operador, tecnología y banda de frecuencias; dichas celdas deben estar configuradas de tal modo que no sea posible acceder a ningún servicio a través de ellas; además, es necesario reducir al mínimo posible la cobertura de las estaciones base externas (que sí brindan acceso a los servicios de telecomunicaciones) de tal forma que ningún dispositivo pueda conectarse a ellas desde el interior del establecimiento penitenciario o centros juveniles.

Esta alternativa presenta las siguientes ventajas y desventajas:

	Estado	Operadores de telecomunicaciones	Población
--	---------------	---	------------------

Ventajas	<ul style="list-style-type: none"> • Reducción de actividades delictivas como la extorsión. • Permite una mayor seguridad pública. • Minimiza la inversión pública al transferir los costos de implementación a los operadores de telecomunicaciones. 	<ul style="list-style-type: none"> • Cumplimiento normativo al prevenir las comunicaciones ilegales. • Reducción de tráfico ilegal en sus redes. • Permite restringir comunicaciones ilegales. 	<ul style="list-style-type: none"> • Aumento de la seguridad pública al reducir la incidencia de extorsiones y delitos organizados.
Desventajas	<ul style="list-style-type: none"> • Costos de supervisión y monitoreo. 	<ul style="list-style-type: none"> • Costos significativos de instalación, operación y mantenimiento de las celdas dummy. • Necesidad de ajustes técnicos y monitoreo constante con el fin de evitar el bloqueo de usuario en las áreas cercanas a los establecimientos penitenciarios y centros juveniles. 	<ul style="list-style-type: none"> • Riesgo de no poder acceder a los servicios de telecomunicaciones en áreas cercanas a los establecimientos penitenciarios y centros juveniles.

Asimismo, a continuación se detallan los costos y beneficios de implementar esta alternativa.

Para el Estado:

Beneficios:

- Reducción de actividades delictivas debido a que la instalación de celdas dummy ayuda a reducir las comunicaciones ilegales, mitigando las extorsiones y otros delitos coordinados desde los establecimientos penitenciarios o centros juveniles.
- Mayor seguridad pública, lo que alivia la carga sobre el sistema de justicia.
- Optimización de recursos públicos de seguridad, debido a una menor necesidad de intervenciones externas para bloquear dispositivos ilegales al interior de los establecimientos penitenciarios o centros juveniles, por lo que el Estado puede asignar estos recursos de manera más eficiente a otras áreas de seguridad.

Costos:

- Mayores costos de supervisión y monitoreo, debido a que se deberán destinar recursos a la regulación y supervisión de la implementación y operación de las celdas dummy, asegurando que las operadoras de telecomunicaciones cumplan con las normas y que las celdas operen adecuadamente en los establecimientos penitenciarios y centros juveniles sin afectar áreas vecinas.

Para las empresas operadoras:

Beneficios:

- Fomenta el cumplimiento normativo debido a que la implementación de las celdas dummy permite a los operadores cumplir con prevenir las comunicaciones ilegales en establecimientos penitenciarios y centros juveniles.
- Menor afectación de servicios de telecomunicaciones debido a que las celdas dummy se configuran para evitar bloqueo de usuarios en zonas aledañas, minimizando quejas y costos de restituir los servicios.
- Reducción de comunicaciones ilegales en la red de las empresas operadoras, lo que genera que la población retome la confianza en el uso de los servicios públicos de telecomunicaciones, por lo que las operadoras pueden ofrecer servicios adicionales de forma segura.

Costos:

- Mayor inversión inicial, dado que la instalación de celdas dummy requiere una inversión significativa en cuanto a la instalación de equipos, infraestructura y tecnología especializada, que varía dependiendo de la cobertura y la cantidad de establecimientos.
- Alta complejidad de coordinación y requiere múltiples soluciones para cada operador, banda y tecnologías.
- Mayores costos de operación y mantenimiento, debido a que se necesitará una optimización de red de manera continua, siendo realizada de forma individual por cada establecimiento penitenciario y centro juvenil, así como, la supervisión técnica para asegurar la eficacia de su solución.
- Solo aplica a redes móviles celulares.
- No incluye el bloqueo de tecnologías como WiFi o comunicaciones satelitales, ni proporciona datos que faciliten las labores de inteligencia de las entidades competentes en temas de seguridad.
- Debido al reto técnico de limitar la cobertura de las estaciones base externas, existe el riesgo de zonas ciegas donde se podría acceder a los servicios comerciales de comunicaciones desde el interior de los establecimientos penitenciarios o centros juveniles.
- Riesgo de afectar áreas fuera de los límites del establecimiento penitenciario, lo que podría bloquear el acceso a servicios de comunicación para usuarios autorizados.

Para la población:

Beneficios:

- Mayor seguridad, debido a que la población se beneficia directamente de la reducción de actividades delictivas organizadas desde establecimientos penitenciarios o centros juveniles, como la extorsión, de esta manera se incrementa la seguridad y tranquilidad.

Costos:

- Posibles bloqueos en áreas adyacentes a los establecimientos penitenciarios y centros juveniles, por lo que existe el riesgo de que, sin un ajuste preciso, las celdas dummy afecten a los usuarios en zonas cercanas a estos establecimientos.

Alternativa 2: Sistema de detección

Esta alternativa se basa en la instalación de equipamiento que permite localizar, rastrear e identificar dispositivos de comunicaciones inalámbricas dentro de los establecimientos penitenciarios y centros juveniles.

Algunos de estos equipos advierten la generación de señales de radiofrecuencia y determinan una localización aproximada para facilitar el proceso de incautación de los dispositivos; otros más avanzados, conocidos como IMSI Catcher permiten capturar información de identidad del dispositivo (por ejemplo, identificación del dispositivo o IMEI, e identificación de la SIM Card o IMSI), facilitando su inclusión en listas de bloqueo de operadores comerciales (similar a las listas negras usadas para reportar terminales robados) y estimar la localización del mismo para su incautación.

Dado que estos dispositivos no requieren, necesariamente, generar transmisiones de alta potencia, el riesgo de interferir con los servicios de comunicación fuera de los límites del establecimiento penitenciario y centros juveniles es considerablemente menor en comparación con otras soluciones.

Esta alternativa presenta las siguientes ventajas y desventajas:

	Estado	Operadores de telecomunicaciones	Población
Ventajas	<ul style="list-style-type: none"> • Reducción de actividades delictivas como la extorsión. • Permite una mayor seguridad pública. • Minimiza la inversión pública al transferir los costos de implementación a los operadores de telecomunicaciones 	<ul style="list-style-type: none"> • Cumplimiento normativo al prevenir las comunicaciones ilegales. • Reducción de tráfico ilegal en sus redes. • Permite restringir comunicaciones ilegales. • Permite la identificación de usuario, servicio, destinatario y localización. 	<ul style="list-style-type: none"> • Aumento de la seguridad pública al reducir la incidencia de extorsiones y delitos organizados.
Desventajas	<ul style="list-style-type: none"> • Costos de supervisión y monitoreo. 	<ul style="list-style-type: none"> • Altos costos de instalación, operación y mantenimiento del sistema de detección. 	<ul style="list-style-type: none"> • Riesgo (bajo) de bloqueos en áreas cercanas a los establecimientos y centros juveniles.

Asimismo, a continuación, se detallan los costos y beneficios de implementar esta alternativa.

Para el Estado:

Beneficios:

- Reducción de delitos coordinados desde el interior de los establecimientos penitenciarios y centros juveniles, puesto que se permite la localización aproximada que reduce significativamente el uso de dispositivos móviles para actividades delictivas.
- Mayor seguridad pública y, por ende, se alivia la carga sobre el sistema de justicia.
- Bajo riesgo de interferencia: Como el sistema no implica emisión de señal de alta potencia, minimiza la posibilidad de interferir con las comunicaciones en áreas aledañas, reduciendo los costos asociados a rectificar interferencias.
- Facilidad en la incautación de dispositivos, debido a la capacidad de ubicar dispositivos lo que facilita las operaciones de incautación y limita el uso de estos equipos en actividades ilícitas.

Costos:

- Mayores costos de coordinación, supervisión y monitoreo, debido a que el Estado deberá coordinar con los operadores la implementación y operación del sistema, lo cual puede requerir inversión en personal y capacitación para supervisar el uso de estos sistemas y garantizar su efectividad.
- Costos por la actualización tecnológica para el monitoreo. Esto debido a que la dependencia de un sistema tecnológico de alta precisión implica que el Estado debe mantenerse actualizado y ajustarse a las mejoras en tecnología de detección para garantizar un control eficaz de las comunicaciones ilegales.

Para las empresas operadoras:

Beneficios:

- Menor interferencia en la red, puesto que, al no requerir transmisiones de alta potencia, los operadores reducen el riesgo de interferencia en sus redes, manteniendo la calidad de servicio para los usuarios fuera de los centros penitenciarios y evitando posibles quejas y reclamos.
- Reducción de uso ilegal de la red, debido a que los detectores permiten identificar y bloquear dispositivos utilizados en actividades ilegales sin afectar la red en general, lo que mejora la eficiencia operativa.
- Facilita el cumplimiento normativo, dado que, al implementar esta solución, los operadores cumplen con las normativas de seguridad y evitan posibles sanciones por el Estado.

Costos:

- Altos costos de implementación, dado que los operadores asumen los costos de adquisición e instalación de equipos y detectores avanzados, como IMSI Catchers, así como los gastos de configuración y mantenimiento periódico del sistema de detección en los establecimientos penitenciarios y centros juveniles.

- Altos costos operativos continuos, puesto que los operadores deberán gestionar el sistema, realizar ajustes y supervisar su operación, lo cual implica un gasto continuo en infraestructura y recursos humanos especializados.
- Costos de actualización, toda vez que el operador debe actualizar continuamente el sistema, lo que implica costos administrativos y tecnológicos adicionales.

Para la población:

Beneficios:

- Mayor seguridad ciudadana, ya que la detección y bloqueo de dispositivos ilegales reduce las actividades delictivas coordinadas desde los establecimientos penitenciarios y centros juveniles, mejorando la seguridad y tranquilidad de la población.
- Menor riesgo de conectividad afectada, dado que, el sistema no necesariamente emite señales de alta potencia, por lo que la población en áreas cercanas a los establecimientos penitenciarios o centros juveniles puede continuar usando sus servicios de telecomunicaciones con menor riesgo de sufrir interrupciones e interferencias.
- Genera confianza en los servicios de telecomunicaciones.

Costos:

- Posible riesgo de que la población de zonas aledañas a los establecimientos penitenciarios o centros juveniles sufran el bloqueo en el acceso a servicios de comunicaciones, aunque en menor proporción que otras alternativas técnicas disponibles.

Alternativa 3: Propuesta regulatoria

Esta alternativa conlleva la propuesta regulatoria que presenta las siguientes ventajas y desventajas:

	Estado	Operadores de telecomunicaciones	Población
Ventajas	<ul style="list-style-type: none"> • Fortalecimiento de la seguridad pública. • Expectativa de reducción de delitos de extorsión. • Minimización de inversión directa en restringir las señales radioeléctricas. • Mayor control y coordinación. 	<ul style="list-style-type: none"> • Facilita el cumplimiento normativo -de acuerdo a las exigencias regulatorias- evitando sanciones. • Las acciones de monitoreo incrementan una mayor confianza en las comunicaciones por parte de los usuarios. • Impulsa la reducción de afectación de servicios mediante la coordinación entre los 	<ul style="list-style-type: none"> • Aumento en la seguridad, ya que se espera reducir los delitos de extorsión y otros crímenes organizados desde los establecimientos penitenciarios y centros juveniles, mejorando la tranquilidad y seguridad. • Permite un mayor control de la conectividad en zonas aledañas,

		<p><i>stakeholders</i> de la red de telecomunicaciones y la ejecución de los ajustes técnicos que optimizan el funcionamiento de la red en zonas aledañas a los establecimientos penitenciarios y centros juveniles, minimizando quejas y reclamos de usuarios.</p>	<p>evitando afectación en el servicio.</p>
Desventajas	<ul style="list-style-type: none"> • Costos de supervisión y monitoreo de cumplimiento de la restricción de señales por parte de las empresas operadoras de telecomunicaciones en establecimientos penitenciarios y centros juveniles. 	<ul style="list-style-type: none"> • Costos de adecuaciones técnicas, optimización, monitoreo permanente de red y generación de reportes. • Reemplazo de la ubicación de su infraestructura, en caso ello fuera necesario, para la restricción de señales radioeléctricas. 	<ul style="list-style-type: none"> • Riesgo de afectación de servicios en zonas aledañas a los establecimientos penitenciarios y centros juveniles.

A continuación, se presentan los costos y beneficios de la presente alternativa:

Para el Estado:

Beneficios:

- Reducción de comunicaciones ilegales desde los establecimientos penitenciarios y centros juveniles, dado que, al minimizar las actividades delictivas coordinadas desde estos establecimientos, se fortalece la seguridad pública, lo cual reduce el costo social y económico de delitos como la extorsión y el fraude.
- Optimización de recursos públicos de seguridad, debido a una menor necesidad de intervenciones externas para bloquear dispositivos ilegales al interior de los establecimientos penitenciarios o centros juveniles, por lo que el Estado puede asignar estos recursos de manera más eficiente a otras áreas de seguridad.

Costos:

- Costos de supervisión y monitoreo, debido a que el MTC tendrá que establecer sistemas de supervisión y monitoreo, así como capacitar a personal para el monitoreo de las restricciones en las señales.
- Costos administrativos y tecnológicos, ya que, al tener acceso remoto al sistema de gestión de los equipos bloqueadores instalados en los establecimientos penitenciarios, así como tener la necesidad de supervisar la eficacia de los sistemas de bloqueo, se podrían incurrir en algunos costos administrativos y tecnológicos.

Para las empresas operadoras:

Beneficios:

- Permite cumplir la normativa regulatoria, debido a que la implementación de estas medidas permite a los operadores cumplir con las exigencias legales y evitar sanciones o multas que podrían impactar negativamente en su operación y reputación.
- Protección de infraestructura y calidad de servicio, ya que, al implementar mecanismos de monitoreo de red, los operadores pueden detectar y mitigar el uso ilegal de sus servicios, protegiendo su infraestructura y optimizando la calidad del servicio en áreas aledañas a los establecimientos penitenciarios y centros juveniles.
- Facilita la reducción de interferencias, puesto que, con un monitoreo y ajuste de sus estaciones, en caso sea necesario, los operadores pueden reducir interferencias que afectan a las zonas aledañas, lo cual mejora la experiencia del usuario y minimiza quejas y reclamos.

Costos:

- Adecuaciones técnicas en infraestructura, ya que, los operadores deberán realizar ajustes como cambios en el tilt, azimut, altura y potencia de sus estaciones radioeléctricas y, de ser necesario, el reemplazo de estaciones radioeléctricas, lo cual implica algunos costos de ingeniería y adquisición de nuevos equipos, si es necesario.
- Implementación y mantenimiento de nuevos procedimientos de monitoreo, ya que, los operadores deben implementar nuevos mecanismos de monitoreo continuo en sus redes y reportar al MTC, MINJUSHD e INPE cuando detecten situaciones inusuales, lo que puede implicar algunos costos en infraestructura y personal técnico.
- Elaboración de reportes periódicos, toda vez que, se tiene la obligación de presentar informes al MTC sobre las medidas y monitoreo de red, lo cual puede agregar algunos costos administrativos y logísticos a sus operaciones.

Para la población:

Beneficios:

- Mayor seguridad ciudadana, como consecuencia de la reducción de actividades delictivas provenientes de comunicaciones ilegales, lo que contribuye a la seguridad de la población, disminuyendo la exposición a riesgos de extorsión y otros delitos.
- Preservación de la calidad del servicio, dado que, al establecer un sistema que controla y ajusta el impacto de las señales radioeléctricas, la conectividad de las zonas aledañas presentaría menor riesgo de interrupciones por parte de los equipos bloqueadores.
- Fomenta la confiabilidad en el sistema de telecomunicaciones, ya que, como consecuencia de la implementación de medidas de monitoreo y restricción de señales radioeléctricas por parte de las empresas operadoras hacia los

establecimientos penitenciario y centros juveniles, se garantiza que la infraestructura de telecomunicaciones opere de manera estable y segura, incrementando la confianza de los usuarios en los servicios.

Costos:

- Posibles afectaciones en la conectividad en áreas aledañas, ya que, si los ajustes técnicos en la red no se calibran correctamente, podría haber problemas de conexión en las áreas cercanas a los establecimientos penitenciarios y centros juveniles.

Análisis Multicriterio

Por consiguiente, con la finalidad de evaluar las tres alternativas propuestas y dado que esta evaluación abarca una serie de aspectos tanto cuantitativos como cualitativos, siendo estos últimos particularmente no siempre posibles de medir, resulta apropiado utilizar el Análisis Multicriterio⁴². Este método permite identificar y seleccionar la alternativa que, en su conjunto, logre el mayor puntaje de evaluación y ofrezca los mayores beneficios netos según los criterios establecidos.

En base a ello, para la evaluación del análisis multicriterio se consideran los siguientes criterios:

Efectividad de la intervención: Este criterio evalúa la capacidad de cada alternativa para alcanzar el objetivo fundamental de promover la innovación tecnológica y reducir las brechas de infraestructura y acceso a servicios de telecomunicaciones. Dada su importancia fundamental en la selección de una alternativa, este criterio representará el 50% de la ponderación total. El propósito principal es determinar cuán efectivamente cada alternativa resuelve los problemas planteados, con un enfoque particular para evitar que las zonas aledañas se vean perjudicadas en su conectividad, otorgándose un mayor puntaje a aquella alternativa que mejor alcance los objetivos planteados.

Costo para las empresas: Este criterio considera, cuál de las alternativas genera o facilita ahorros en costos de inversión y regulación para las empresas, así como, los costos directos e indirectos que las empresas tendrán que asumir para cumplir con las regulaciones propuestas por cada alternativa. Obteniendo un puntaje mayor aquella alternativa que genere una menor carga financiera para las empresas o mayores ahorros para el cumplimiento normativo. En esa línea, este criterio tendrá un peso de 25% de la medida a implementar.

Costo regulatorio: Este criterio se enmarca en evaluar cuál de las alternativas genera menores costos de supervisión y fiscalización relacionadas al cumplimiento de las

⁴² El análisis multicriterio, es una metodología que permite la elección de la mejor alternativa, a partir de la ponderación y agregación de diferentes criterios de evaluación, que son el reflejo de la valoración que se ha otorgado a la forma en que cada alternativa pretende resolver el problema.

Una vez definidos los criterios y ponderaciones, se procede a calificar cada alternativa asignándoles un puntaje ordinal. Posteriormente, se realiza la suma ponderada de estas calificaciones y se obtiene el total para cada alternativa. Finalmente, se elige la alternativa que obtenga el mayor puntaje ponderado como la mejor opción:

$$Max \left[V_i = w_1V_{i1} + w_2V_{i2} + \dots + w_nV_{in} = \sum_{j=1}^n w_jV_{ij} \right]$$

Donde w_n es la ponderación asignada al criterio n y V_{in} es la calificación o puntaje otorgado por el criterio n a la alternativa de solución i .

(Esta referencia comprende lo señalado en las "Metodologías para la evaluación de impactos del AIR Ex Ante").

regulaciones impuestas. En otras palabras, este criterio busca evaluar cuál de las alternativas conlleva menores costos operativos y de gestión para el Estado, buscando eficiencia en la utilización de recursos públicos y agilidad en los procesos regulatorios. En esa línea, este criterio tendrá un peso de 25% de la medida a implementar.

Escala de criterios de evaluación

+3	+2	+1	0	-1	-2	-3
Alta mejora respecto al escenario base.	Mejora moderada respecto al escenario base.	Ligera mejora respecto al escenario base.	No presenta un cambio sustancial en efectividad o costos con respecto al escenario base.	Ligera desmejora respecto al escenario base.	Desmejora moderada respecto al escenario base.	Importante desmejora respecto al escenario base.
-----	-----	-----	-----	-----	-----	-----
-	-	----	---	--	--	---
Ahorros importantes frente al escenario base	Ahorros moderados frente al escenario base	Ligero ahorro frente al escenario base		Ligero incremento de costos respecto a escenario base	Incremento moderado de costos respecto a escenario base	Importante incremento de costos respecto a escenario base

Fuente: Informe N° 00110-GPRC/2020-OSIPTTEL.

Valoración de las alternativas

A partir de los criterios metodológicos expuestos, se evaluará el puntaje a asignar a las dos *alternativas distintas al statu quo* (para efectos de este análisis consideramos el *statu quo* como el escenario base donde no se implementa ninguna acción), con el fin de atender la problemática.

Criterio	Alternativa 1	Alternativa 2	Alternativa 3
Efectividad	<p>La instalación de celdas dummy proporciona una buena solución para restringir y/o bloquear comunicaciones ilegales en áreas específicas dentro de los establecimientos penitenciarios y centros juveniles. Las celdas emulan estaciones base y captan las conexiones de dispositivos cercanos, evitando que las llamadas y conexiones ilegales se transmitan fuera del área controlada.</p> <p>No obstante, esta alternativa tiene limitaciones en cuanto a la precisión del bloqueo y el riesgo de afectar a la población que vive en zonas aledañas, por lo que esta posibilidad de bloqueo limita la efectividad general de la alternativa para mantener el acceso a los servicios de</p>	<p>La implementación de un sistema de detección empleando equipos avanzados, como los IMSI Catchers, es altamente efectiva para identificar y rastrear dispositivos ilegales dentro de los establecimientos penitenciarios y centros juveniles, ya que estos dispositivos permiten capturar información específica de los dispositivos, como el IMEI y el IMSI. De esta manera, se facilita su inclusión en listas de bloqueo sin necesidad de interferir con la señal general de telecomunicaciones en las zonas aledañas a los establecimientos penitenciarios y centros juveniles.</p>	<p>La propuesta regulatoria establece la obligación para las operadoras a restringir sus señales radioeléctricas hacia los establecimientos penitenciarios y centros juveniles, mediante adecuaciones y ajustes técnicos en sus estaciones radioeléctricas. Asimismo, establece la implementación de monitoreos de red y reportes regulares, así como, análisis de geolocalización ; sin necesidad de interferir con la señal general de telecomunicaciones en las zonas aledañas. Por tanto, estas medidas de ajuste permiten una reducción en las comunicaciones ilegales sin un bloqueo total, ofreciendo un nivel de efectividad moderado en la contención de</p>

	<p>telecomunicaciones en zonas vecinas.</p> <p>Puntaje: +2</p>	<p>Asimismo, teniendo en cuenta que el sistema no requiere emisión de señales de alta potencia y utiliza tecnología de baja interferencia, reduce significativamente el riesgo de afectar la conectividad en las zonas aledañas, ofreciendo un mayor control sin comprometer el acceso de la población de las zonas aledañas a estos establecimientos a servicios de telecomunicaciones.</p> <p>Puntaje: +3</p>	<p>comunicaciones no autorizadas.</p> <p>No obstante, la dependencia de adecuaciones físicas y monitoreos de red continuos, puede limitar la precisión y efectividad de esta alternativa en comparación con tecnologías de detección avanzada, por lo que la efectividad puede variar en función de la ubicación de las estaciones y las características de cada establecimiento penitenciario y centro juvenil; además, existe la posibilidad de que los ajustes afecten la señal en áreas vecinas.</p> <p>Puntaje: +2</p>
<p>Costo para las empresas</p>	<p>La instalación de celdas dummy implica costos moderados para las empresas, dado que requiere la adquisición de equipos especializados y su configuración en cada centro penitenciario. Además, los operadores deben asumir los costos de implementación, mantenimiento y monitoreo de estas celdas, que necesitan ajustes regulares para garantizar su efectividad y minimizar el impacto en áreas vecinas.</p> <p>Aunque esta alternativa tiene un costo moderado en términos de infraestructura y soporte técnico, es menos costosa que alternativas con tecnologías más avanzadas, como el sistema de detección y/o gestión de acceso.</p>	<p>La implementación de un sistema de detección con equipos avanzados, como los IMSI Catchers, representa altos costos de inversión y operación para las empresas operadoras de telecomunicaciones.</p> <p>Estos sistemas requieren equipos especializados capaces de rastrear y captar identificadores específicos de dispositivos, lo que implica una inversión inicial elevada.</p> <p>Además, los operadores deben incurrir en costos adicionales de mantenimiento, actualización y monitoreo continuo, así como en el entrenamiento de personal técnico para gestionar estos sistemas complejos.</p> <p>A diferencia de otras alternativas, este sistema implica costos más altos debido a su alta tecnología y a la necesidad de un mantenimiento riguroso para asegurar su eficacia.</p>	<p>La propuesta regulatoria implica que las empresas realicen ajustes técnicos en sus estaciones radioeléctricas y lleven a cabo monitoreos permanentes y realicen reportes regularmente. Estos ajustes incluyen cambios en el tilt, azimuth, altura y potencia de las estaciones y, de ser necesario el reemplazo de estaciones radioeléctricas, además, de la implementación de un sistema de monitoreo de red para detectar intentos de conexión en las áreas controladas, así como, para coadyuvar a determinar la funcionalidad u operatividad de los equipos de bloqueo de señales instalados en los establecimientos penitenciarios y centros juveniles.</p> <p>Aunque esta alternativa sí conlleva costos, estos se consideran menores en comparación con las alternativas anteriores. Las adecuaciones en las estaciones, la remisión de reportes y el monitoreo de red</p>

			son menos costosos que la implementación y mantenimiento de nuevos sistemas; además de que muchas operadoras pueden integrar las medidas propuestas en sus procesos de operación y mantenimiento que regularmente realizan. Por tanto, el impacto financiero es menor.
	Puntaje: -2	Puntaje: -3	Puntaje: -1
Costos regulatorios	<p>La instalación de celdas dummy implica un incremento moderado de costos regulatorios debido a la necesidad de supervisión y monitoreo por parte de las autoridades. Aunque las celdas dummy se instalan y configuran en ubicaciones específicas, su efectividad y configuración técnica deben ser verificadas periódicamente para asegurarse de que no afecten a las zonas aledañas a los establecimientos penitenciarios y centros juveniles.</p> <p>Este proceso requiere inspecciones de campo por parte del Estado para asegurar que las celdas operen dentro de los parámetros establecidos, sin afectar a la población de zonas aledañas.</p>	<p>El sistema de detección y gestión de acceso requiere un nivel de supervisión significativo debido a su tecnología avanzada y la naturaleza sensible de los datos capturados.</p> <p>Además, se necesita establecer protocolos de supervisión y control de datos para garantizar que la información recopilada se maneje conforme a las normativas de privacidad y seguridad.</p> <p>Por lo tanto, se deben realizar supervisiones regulares para verificar la precisión y eficacia de estos sistemas, asegurando que cumplan su propósito.</p>	<p>La propuesta regulatoria implica menores costos regulatorios en comparación con las otras alternativas, ya que se basa en ajustes técnicos, monitoreo de red y remisión de reportes por parte de las operadoras, lo cual disminuye la necesidad de supervisión directa por parte del Estado.</p> <p>La supervisión en esta alternativa se limita principalmente a la verificación de la restricción de las señales radioeléctricas, reportes y monitoreos puntuales para confirmar que las operadoras están cumpliendo con las adecuaciones técnicas y la configuración de estaciones.</p> <p>Por lo tanto, se reducen los costos operativos para el Estado a diferencia de las otras alternativas.</p>
	Puntaje: -2	Puntaje: -2	Puntaje: -1

Entonces, se realiza el análisis de puntuación otorgada a cada alternativa por cada criterio:

Comparación entre alternativas

Criterios de evaluación	Ponderación	Alternativa 1	Alternativa 2	Alternativa 3
Efectividad	50%	2	3	2
Costos para las empresas	25%	-2	-3	-1
Costos regulatorios	25%	-2	-2	-1
Resultado de la evaluación		0	0.25	0.5

Elaboración: DGPRC-MTC.

Luego de evaluar las tres alternativas bajo los tres criterios (efectividad, costo para las empresas y costo regulatorio), la **Alternativa 3** presenta una combinación balanceada que minimiza los costos para las empresas y el Estado, manteniendo una efectividad adecuada en la restricción de las comunicaciones ilegales desde los establecimientos penitenciarios y centros juveniles. Si bien no presentan la máxima efectividad en comparación con la Alternativa 2 (teniendo en cuenta que ninguna alternativa por sí sola puede brindar el 100% de efectividad o evitar el riesgo de afectar a la población de zonas aledañas), sus costos regulatorios y de implementación para las empresas son significativamente menores, lo que permite una implementación más sostenible y viable.

VIII. Análisis de impacto de la vigencia de la norma en la legislación nacional

El numeral 10.1 del artículo 10 del Reglamento de la Ley N° 26889, Ley Marco para la Producción y Sistematización Legislativa, aprobado por Decreto Supremo N° 007-2022-JUS, señala que el análisis de impacto de la vigencia de la norma en la legislación nacional debe precisar si la propuesta normativa trata de innovar supliendo vacíos en el ordenamiento jurídico o si trata de una propuesta que modifica o deroga normas vigentes.

Sobre el particular, es preciso considerar que la emisión del Reglamento del Decreto Legislativo N° 1688, se realiza en mérito a lo establecido en la Segunda Disposición Complementaria Final del mencionado decreto legislativo, el cual dispone que el MTC, en coordinación con el OSIPTEL, mediante Decreto Supremo aprueba el Reglamento correspondiente.

De este modo, las disposiciones del Reglamento se encuentran alineadas con las disposiciones del Decreto Legislativo N° 1688, en tanto que desarrolla su contenido y precisa sus disposiciones.

En efecto, en el Reglamento se han incorporado obligaciones específicas y concretas para las empresas operadoras de servicios públicos de telecomunicaciones en relación con las comunicaciones ilegales en establecimientos penitenciarios y centros juveniles; así como, se han establecido disposiciones sobre la facultad fiscalizadora y sancionadora del MTC y del OSIPTEL respecto de las obligaciones estipuladas en la mencionada norma.

Cabe resaltar que el articulado del Reglamento se encuentra alineado con lo dispuesto en el artículo 44 de la Constitución Política del Perú, el cual establece que son deberes primordiales del Estado, garantizar la plena vigencia de los derechos humanos, proteger a la población de las amenazas contra su seguridad, y promover el bienestar general que se fundamenta en la justicia y en el desarrollo integral y equilibrado de la Nación.

Asimismo, la emisión del Reglamento guarda coherencia con lo dispuesto en la Única Disposición Preliminar del TUO de la Ley de Telecomunicaciones, el cual declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional.

Del mismo modo, se encuentra acorde con el artículo 2 del TUO de la Ley de Telecomunicaciones, el cual declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y establece que su fomento, administración y control corresponde al Estado de acuerdo a dicha Ley; así como, con lo dispuesto en su artículo 3, el cual establece el derecho que tiene toda persona de usar y prestar servicios de telecomunicaciones en la forma señalada en las disposiciones que regulan la materia.

Por otro lado, en el Reglamento se ha dispuesto la modificación del artículo 2 y 6 de la Resolución Ministerial N° 954-2016-MTC/01.03, con la finalidad de incluir dentro de su ámbito de aplicación a los centros juveniles; así como, actualizar los parámetros de señales radioeléctricas de los equipos de telecomunicaciones de las empresas operadoras y de los equipos bloqueadores, a fin de que se encuentren más acorde con las nuevas tecnologías móviles.

De esta forma, en la siguiente tabla se muestra el comparativo de la mencionada modificación:

Texto vigente de la Resolución Ministerial N° 954-2016-MTC/01.03	Propuesta de modificación de la Resolución Ministerial N° 954-2016-MTC/01.03										
<p align="center">Artículo 2.- Ámbito de aplicación.</p> <p><i>El presente Protocolo se aplica a los responsables del funcionamiento de equipos bloqueadores de señales radioeléctricas en los establecimientos penitenciarios y a las empresas operadoras de servicios de telecomunicaciones.</i></p>	<p align="center">“Artículo 2.- Ámbito de aplicación.</p> <p><i>El presente Protocolo se aplica a los responsables del funcionamiento de equipos bloqueadores de señales radioeléctricas en los establecimientos penitenciarios, centros juveniles y a las empresas operadoras de servicios de telecomunicaciones.</i></p> <p><i>Asimismo, cuando en el presente Protocolo se haga referencia a establecimientos penitenciarios, entiéndase también a los centros juveniles, en lo que resulte aplicable.”</i></p>										
<p>“Artículo 6.- Niveles de recepción de señales radioeléctricas de los equipos bloqueadores.</p> <p>6.1 Los equipos bloqueadores y los equipos de las Operadoras garantizan un nivel de recepción menor o igual a -100 dBm en el límite de la Zona de Intangibilidad.</p> <p>6.2 Se establece una zona de exclusión especial, la misma que inicia desde el borde externo de la Zona de Intangibilidad hasta la distancia donde se verifique niveles de recepción igual a -95 dBm. Esta zona, se considera excluida de los parámetros de cobertura o de calidad del OSIPTEL, así como de la verificación de obligaciones contractuales y/o administrativas aplicables.”</p>	<p>“Artículo 6.- Parámetros de señales radioeléctricas de los equipos de telecomunicaciones de las Operadoras y de los equipos bloqueadores.</p> <p>6.1 La Operadora restringe la emisión de su señal radioeléctrica de los servicios públicos de telecomunicaciones hacia los establecimientos penitenciarios, centros juveniles y zonas restringidas y de alta seguridad, de tal forma que cumpla con los siguientes parámetros:</p> <table border="1" data-bbox="823 1729 1378 2029"> <thead> <tr> <th>Tecnología</th> <th>Nivel de señal</th> </tr> </thead> <tbody> <tr> <td align="center">2G</td> <td>RxLev < -100 dBm</td> </tr> <tr> <td align="center">3G</td> <td>RSRP (Received Signal Code Power) < -100 dBm</td> </tr> <tr> <td align="center">4G</td> <td>RSRP (Reference Signal Received Power) < -115 dBm</td> </tr> <tr> <td align="center">5G</td> <td>SS-RSRP (Synchronization</td> </tr> </tbody> </table>	Tecnología	Nivel de señal	2G	RxLev < -100 dBm	3G	RSRP (Received Signal Code Power) < -100 dBm	4G	RSRP (Reference Signal Received Power) < -115 dBm	5G	SS-RSRP (Synchronization
Tecnología	Nivel de señal										
2G	RxLev < -100 dBm										
3G	RSRP (Received Signal Code Power) < -100 dBm										
4G	RSRP (Reference Signal Received Power) < -115 dBm										
5G	SS-RSRP (Synchronization										

	<table border="1" data-bbox="823 192 1378 309"> <tr> <td data-bbox="823 192 1066 309"></td> <td data-bbox="1066 192 1225 309">Signal- Reference Received < X0 dBm</td> <td data-bbox="1225 192 1378 309">Signal Power)</td> </tr> </table> <p><i>Donde: X0 será definido por el operador, de tal manera que restrinja las comunicaciones ilegales desde establecimientos penitenciarios y centros juveniles.</i></p> <p><i>6.2 Los equipos bloqueadores y los equipos de las Operadoras garantizan un nivel de relación del valor pico de la señal deseada con la señal no deseada no mayor a -7 dB, según corresponda.</i></p> <p><i>En caso durante el proceso de medición no se detecte señal deseada, se toma como referencia de señal deseada -100 dBm.</i></p> <p><i>6.3 Los parámetros establecidos en los numerales 6.1 y 6.2 son exigibles a partir del borde externo de la zona de intangibilidad o zona restringida y de alta seguridad, comprendiendo a toda el área de dicha zona y de los establecimientos penitenciarios y centros juveniles.</i></p> <p><i>6.4 Se establece una zona de exclusión especial para los establecimientos penitenciarios y centros juveniles. En el caso de los establecimientos penitenciarios, dicha zona inicia desde el borde externo de la zona restringida y de alta seguridad y se extiende hasta la distancia de 200 metros a su alrededor. En el caso de los centros juveniles, dicha zona comprende 400 metros alrededor del perímetro de dichos centros. La zona de exclusión especial, se considera excluida de los parámetros de cobertura o de calidad del OSIPTEL, así como de la verificación de obligaciones contractuales y/o administrativas aplicables.”</i></p>		Signal- Reference Received < X0 dBm	Signal Power)
	Signal- Reference Received < X0 dBm	Signal Power)		

IX. Análisis de impacto regulatorio Ex-Ante

El 28 de mayo de 2023 se publicó en el diario oficial El Peruano el Decreto Legislativo N° 1565, que aprueba la Ley General de Mejora de la Calidad Regulatoria, cuya única disposición complementaria regulatoria derogó el artículo 2 del Decreto Legislativo N° 1310, que estableció como instrumento para la mejora de la calidad regulatoria el Análisis de Impacto Regulatorio.

Sin perjuicio de lo señalado, la segunda disposición complementaria final del Decreto Legislativo N° 1565, dispuso que en tanto se apruebe su reglamento, continúa vigente el Reglamento que desarrolla el Marco Institucional que rige el Proceso de Mejora de la Calidad Regulatoria y establece los Lineamientos Generales para la aplicación del Análisis de Impacto Regulatorio Ex Ante, aprobado por Decreto Supremo N° 063-2021-PCM.

Con fecha 25 de febrero de 2025, se publicó el Decreto Supremo N° 023-2025-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1565, Decreto Legislativo que aprueba la Ley General de Mejora de la Calidad Regulatoria (en adelante, el Reglamento de la Ley General de Mejora de la Calidad Regulatoria).

Al respecto, se tiene que, conforme al literal f) del artículo 15 del el Reglamento de la Ley General de Mejora de la Calidad Regulatoria las entidades del Poder Ejecutivo tienen, entre otras obligaciones, la obligación de determinar si un proyecto normativo requiere la presentación de un expediente AIR Ex Ante o ACR Ex Ante ante la Comisión

Multisectorial de Calidad Regulatoria (CMCR), así como el aplicar dichos instrumentos de forma previa a la elaboración de normas de carácter general, cuya responsabilidad es del órgano proponente del proyecto normativo, según corresponda.

Mediante Resolución de Secretaría de Gestión Pública N° 008-2021-PCM-SGP se aprobó el Plan de Implementación del Análisis de Impacto Regulatorio Ex Ante para las entidades públicas del Poder Ejecutivo. Dicho Plan señala el Cronograma de implementación del AIR Ex Ante y la Agenda Temprana en las entidades públicas del Poder Ejecutivo, siendo que resulta de aplicación obligatoria el Análisis de Impacto Regulatorio Ex Ante para el MTC a partir del 02 de enero de 2023.

Ahora bien, el Reglamento de la Ley General de Mejora de la Calidad Regulatoria, señala en el literal g) del artículo 5 que se entiende por “norma de carácter general” a aquella que crea, modifica, regula, declara o extingue derechos u obligaciones de carácter general, de cuyo texto se deriva un mandato genérico, objetivo y obligatorio, vinculando a la Administración Pública y a los administrados, sea para el cumplimiento de una disposición o para la generación de una consecuencia jurídica.

Asimismo, de acuerdo con el numeral 33.2 del artículo 33 del el Reglamento de la Ley General de Mejora de la Calidad Regulatoria estipula que las entidades públicas tienen la obligación de aplicar un AIR Ex Ante como herramienta de análisis previo, cuando el proyecto normativo de carácter general establezca y/o modifique una obligación, condición, requisito, responsabilidad, prohibición, limitación y/o cualquier otra regla que imponga exigencias: a) que genere(n) o modifique(n) costos en su cumplimiento por parte de las personas; y/o, b) que limite(n) el ejercicio, otorgamiento y/o reconocimiento de derechos de las personas, restringiendo el desarrollo de actividades económicas y sociales que contribuyan al desarrollo integral, sostenible, y al bienestar social.

Bajo dicho contexto, se tiene que el Reglamento amerita la realización de un análisis de impacto regulatorio ya que se subsume en lo regulado en numeral 33.2 del artículo 33 del el Reglamento de la Ley General de Mejora de la Calidad Regulatoria, dado que se establecen obligaciones específicas a ser cumplidas por las empresas operadoras respecto a la restricción de señales radioeléctricas, así como, a los mecanismos que impidan las comunicaciones ilegales en los establecimientos penitenciarios y centros juveniles y coadyuven a los sistemas y/o equipos de seguridad tecnológica implementados por las entidades competentes. Además, se tipifican infracciones y sanciones ante el incumplimiento de las mencionadas obligaciones.

En ese sentido, la presente norma cuenta con dictamen favorable de fecha **xxx** de la Comisión Multisectorial de Calidad Regulatoria que valida el expediente AIR Ex Ante correspondiente

X. Análisis de Calidad Regulatoria Ex Ante

Por otro lado, es importante mencionar que el presente proyecto de Decreto Supremo no establece la creación de procedimientos administrativos a iniciativa de parte; por lo que no se encuentra dentro del ámbito de aplicación del Análisis de Calidad Regulatoria, conforme a lo previsto en el Capítulo V del Reglamento de la Ley General de Mejora de la Calidad Regulatoria.