EXPOSICIÓN DE MOTIVOS

I. Objeto

El presente Proyecto de Norma tiene por objeto establecer medidas preventivas y reactivas contra las llamadas y los mensajes de texto con fines ilícitos; así como, establecer disposiciones sobre el uso de la numeración para la identificación del remitente de las llamadas realizadas para promover tanto productos como servicios y prestar el servicio de telemercadeo, toda vez que no se cuenta con una regulación específica orientada a afrontar dicha problemática y que permita garantizar la seguridad de los servicios públicos de las telecomunicaciones, en salvaguarda del bienestar e integridad de la población y la sociedad.

II. Finalidad

El presente Proyecto de Norma tiene por finalidad reducir la problemática vinculada a la realización de llamadas y envío de mensajes de texto con fines ilícitos y los efectos negativos que generan en la sociedad; así como, generar fiabilidad y seguridad en las comunicaciones mediante la identificación del remitente de las llamadas realizadas para promover tanto productos como servicios y prestar el servicio de telemercadeo.

III. Antecedentes

Conforme al numeral 1 y el segundo párrafo del numeral 4 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho, a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar; así como, a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida, y a que el Estado promueva el uso de las tecnologías de la información y la comunicación en todo el país.

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 Nº 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, 2 y 3 del artículo 75 del TUO de la Ley de Telecomunicaciones, establecen que son funciones del Ministerio de Transportes y Comunicaciones (MTC), fijar la política de telecomunicaciones a seguir y

controlar sus resultados; 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; otorgar y revocar concesiones, autorizaciones, permisos, licencias y controlar su correcta utilización; entre otras.

Mediante la Resolución Suprema Nº 022-2002-MTC, se aprobó el Plan Técnico Fundamental de Numeración (en adelante, PTFN), documento que contiene los planes técnicos fundamentales, que establecen las pautas y lineamientos técnicos y básicos que aseguran la integración e implementación de los servicios de telecomunicaciones en el territorio nacional.

De acuerdo con la parte introductoria del PTFN, la numeración en los servicios públicos de telecomunicaciones es un recurso escaso que debe ser usado eficientemente, por lo cual dicho plan establece los criterios para el adecuado uso de los números asignados en la red pública nacional de telecomunicaciones. Asimismo, como la numeración está asociada directamente con los procesos de marcación y encaminamiento, el PTFN proporciona las pautas correspondientes para el desarrollo de estos procesos. Además, la adecuada administración y oportuna supervisión del cumplimiento del PTFN, deben asegurar una regular e imparcial asignación de los recursos numéricos para el beneficio mutuo de los usuarios y operadores de los servicios públicos.

En el numeral 1. Objetivos del PTFN se menciona que uno de sus objetivos, consiste en establecer las bases para una adecuada administración, supervisión y uso de la numeración, a través de una eficiente asignación, así como definir las estructuras de numeración para la prestación de los servicios públicos de telecomunicaciones. Adicionalmente, cabe destacar que constituye uno de los objetivos del PTFN, facilitar al abonado, en lo posible, el reconocimiento de los diferentes servicios y sus proveedores.

Por su parte, el artículo 106 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado mediante Decreto Supremo Nº 020-2007-MTC (en adelante, TUO del Reglamento de la Ley de Telecomunicaciones), establece que los contratos de interconexión deben sujetarse, entre otros, a lo establecido por los planes técnicos fundamentales contenidos en el Plan Nacional de Telecomunicaciones, así como a las disposiciones que dicte el Organismo Supervisor de la Inversión en Telecomunicaciones (OSIPTEL). Asimismo, dicho artículo establece que, los contratos de interconexión deberán contemplar, entre otros aspectos, las características de las señales transmitidas o recibidas incluyendo arreglos de encaminamiento, transmisión, sincronización, señalización, numeración, tarifas y calidad de servicio y seguridad de telecomunicaciones.

De otro lado, los numerales 5 y 6 del artículo 258 del TUO del Reglamento de la Ley de Telecomunicaciones, establecen que constituye infracciones muy graves la utilización de numeración sin la debida asignación por parte del órgano competente del MTC o de una distinta a la asignada, así como, la utilización de señalización o numeración en condiciones distintas a las contempladas en el respectivo plan técnico, respectivamente.

Asimismo, la romanilla (i) del literal a) del artículo 23 del Texto Único Ordenado de las Normas de Interconexión, aprobado mediante Resolución de Consejo Directivo Nº 134-2012-CD-OSIPTEL (en adelante, TUO de Interconexión), al tratar sobre la

interconexión vía transporte conmutado local con liquidación indirecta (liquidación en cascada) establece que, el operador solicitante deberá requerir al operador que brinda el transporte conmutado local la interconexión con el operador de la tercera red, indicando los códigos de numeración asignados por el MTC y los escenarios de llamadas que se cursarán, especificando si se trata de uno o ambos sentidos.

Por su parte, el artículo 43 del TUO de Interconexión establece que los operadores que se interconectan de forma directa o vía el transporte conmutado local no podrán modificar la numeración respecto del tráfico que se cursa, impidiendo el reconocimiento del número de origen y/o número de destino. Sin perjuicio de ello, los operadores podrán acordar la inclusión de prefijos.

Por otro lado, el numeral 9) del artículo 87 del TUO de la Ley de Telecomunicaciones, establece que constituyen infracciones muy graves, el incumplimiento de las normas de la referida Ley, sus reglamentos y disposiciones de la autoridad, que sean tipificadas como muy graves por el reglamento. Asimismo, los numerales 9 y 12 del artículo 88 de dicha Ley establecen que constituyen infracciones graves, la utilización indebida de los servicios de telecomunicaciones, y cualquier otra infracción de la normativa de telecomunicaciones tipificada como falta grave.

Por su parte, el artículo 261 del TUO del Reglamento de la Ley de Telecomunicaciones, establece los supuestos que se consideran como utilización indebida del servicio a efectos del artículo 88 del TUO de la Ley de Telecomunicaciones.

Asimismo, el artículo 262 del TUO del Reglamento de la Ley de Telecomunicaciones, establece que para la aplicación del numeral 2 del artículo 89 de la Ley, entiéndase por utilización indebida de servicios de telecomunicaciones, aquellos casos en que los usuarios de los servicios de telecomunicaciones hacen mal uso de los mismos para efectuar llamadas maliciosas, entre otros.

Aunado a lo anterior, el artículo 129 del TUO del Reglamento de la Ley de Telecomunicaciones establece que son derechos del concesionario, entre otros, verificar que sus abonados o usuarios no hagan mal uso de los servicios que les preste y, si de tal verificación se desprendiese un uso fraudulento o indebido, pondrá tales hechos en conocimiento del OSIPTEL, a fin de que éste adopte las medidas necesarias para que cese la irregularidad.

Además de lo antes mencionado, el Reglamento para la Gestión y Supervisión de la Numeración de los Servicios Públicos de Telecomunicaciones, aprobado mediante Decreto Supremo Nº 021-2004-MTC, regula la gestión y supervisión de los recursos de numeración, así como sus condiciones de uso, estableciendo principios, procedimientos y plazos para la asignación y reversión de números, entre otros aspectos vinculados con la administración eficiente de dicho recurso.

En línea con lo antes mencionado, el artículo 33 de la Norma de las Condiciones de Uso de los Servicios Públicos de Telecomunicaciones, aprobado mediante Resolución de Consejo Directivo Nº 172-2022-CD/OSIPTEL (en adelante, las Condiciones de Uso), establece qué constituye la utilización debida del servicio por parte del abonado. Así, según el mencionado artículo, el abonado y/o usuario tiene la obligación de utilizar debidamente el servicio, conforme al uso residencial o comercial que hubiera declarado a la empresa operadora y cumpliendo con la

normativa vigente y las disposiciones contractuales aplicables, bajo responsabilidad prevista en el ordenamiento legal. En ningún caso el abonado y/o usuario puede hacer uso fraudulento del servicio, ni efectuar directamente o a través de terceros modificación, alteración o cambio en la planta externa de la empresa operadora, ni puede extender el servicio contratado fuera del domicilio de instalación, salvo lo dispuesto en el artículo 34.

Asimismo, las Condiciones de Uso también establecen que la empresa operadora puede suspender cautelarmente y cortar el servicio por uso indebido de este, de conformidad con lo dispuesto en el en el punto 1.2 del Anexo 8 de la misma norma.

De otro lado, el literal e del artículo 58 de la Ley Nº 29571, Código de Protección y Defensa del Consumidor (en adelante, Código de Protección y Defensa del Consumidor), recoge los casos de métodos comerciales agresivos y engañosos, entre otros, mediante centros de llamada (call centers), sistemas de llamado telefónico, envío de mensajes de texto a celular o de mensajes electrónicos masivos para promover productos y servicios, así como prestar el servicio de telemercadeo, a todos aquellos números telefónicos y direcciones electrónicas de consumidores que no hayan brindado a los proveedores de dichos bienes y servicios su consentimiento previo, informado, expreso e inequívoco, para la utilización de esta práctica comercial.

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.

Por otro lado, mediante la Ley N° 32323 se modificó la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, estableciendo que, para garantizar la protección del consumidor contra los métodos comerciales agresivos o engañosos, el Estado establece las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones. Asimismo, la única disposición complementaria final establece que la aplicación del párrafo 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, incorporado por dicha ley, el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información trasmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de la presente ley.

Finalmente, 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 Nº 07-2020-CD-OSIPTEL, se desarrollaron las disposiciones sobre el Registro Nacional de Equipos Terminales Móviles para la Seguridad - RENTESEG.

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

Conforme al numeral 1 y el segundo párrafo del numeral 4 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho, a la vida, a su identidad, a su integridad moral, psíquica y física y a su libre desarrollo y bienestar; así como, a gozar de un ambiente equilibrado y adecuado al desarrollo de su vida, y a que el Estado promueva el uso de las tecnologías de la información y la comunicación en todo el país.

De acuerdo al numeral 22 del artículo 2 de la Constitución Política del Perú, toda persona tiene derecho, a la paz, a la tranquilidad, al disfrute del tiempo libre y al descanso.

Asimismo, el artículo 44 de la Constitución Política del Perú, establece que son deberes primordiales del Estado; entre otros, 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.

Por otra parte, al artículo 4 de la Ley Nº 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.

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, la Disposición Preliminar del TUO de la Ley de Telecomunicaciones se declara de necesidad pública el desarrollo de las Telecomunicaciones como instrumento de pacificación y de afianzamiento de la conciencia nacional, para cuyo fin se requiere captar inversiones privadas, tanto nacionales como extranjeras.

El artículo 1 del TUO de la Ley de Telecomunicaciones dispone que, las Telecomunicaciones, como vehículo de pacificación y desarrollo, en sus distintas formas y modalidades, se rigen por la referida Ley, por los reglamentos que la

complementan y por las disposiciones emanadas de la autoridad competente con sujeción a lo establecido en los tratados y acuerdos internacionales de Telecomunicaciones de los que el Perú es parte.

Asimismo, los artículos 2 y 3 del TUO de la Ley de Telecomunicaciones establecen que, se declara de interés nacional la modernización y desarrollo de las telecomunicaciones, dentro del marco de libre competencia, y su fomento, administración y control corresponde al Estado de acuerdo a la referida Ley; así como, toda persona tiene derecho a usar y prestar servicios de telecomunicaciones en la forma señalada por las disposiciones que regulan la materia.

Por otra parte, los numerales 1, 2 y 3 del 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; 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; así como, otorgar y revocar concesiones, autorizaciones, permisos y licencias y controlar su correcta utilización.

Mediante la Ley N° 32323 que modifica la Ley N° 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM, se establece que para garantizar la protección del consumidor contra los métodos comerciales agresivos o engañosos, el Estado establece las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones.

Asimismo, la única disposición complementaria final de la mencionada ley establece que la aplicación del párrafo 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, incorporado por la mencionada ley, el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como los mecanismos de validación de la información trasmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de dicha ley.

En ese sentido, considerando el marco jurídico habilitante, se sustenta el presente Proyecto de Norma, que tiene el propósito de aprobar el marco normativo para la lucha contra llamadas y mensajes con fines ilícitos que tiene por objeto establecer medidas preventivas y reactivas contra las llamadas y mensaje con fines ilícitos; así como, establecer disposiciones sobre el uso de la numeración para la identificación del remitente de las llamadas realizadas para promover productos y servicios, así como prestar el servicio de telemercadeo.

V. Fundamento Técnico de la Propuesta Normativa

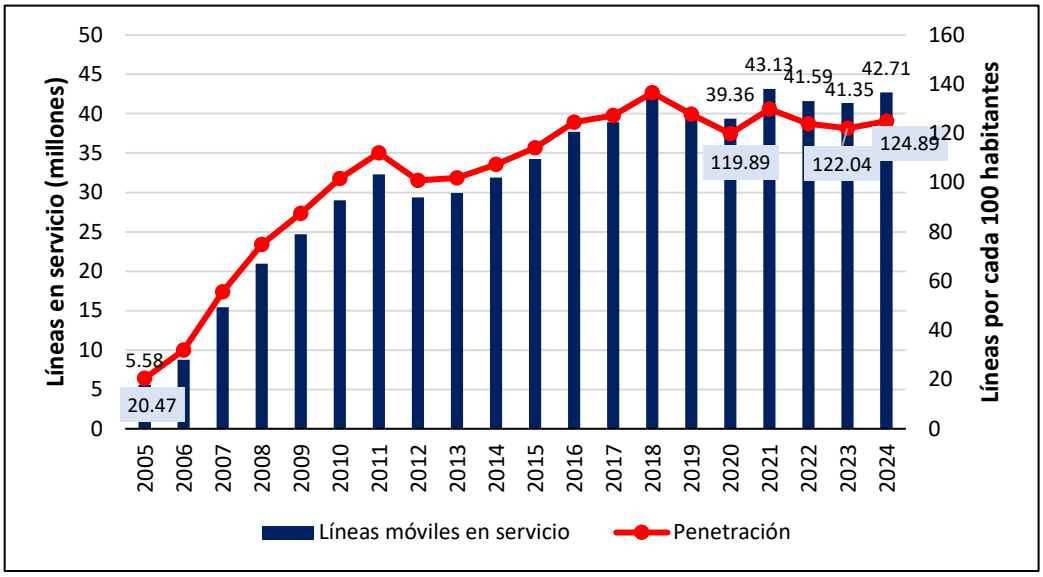
5.1. Problemática Identificada

5.1.1. Contexto general y panorama internacional

En los últimos 20 años, el acceso a telefonía móvil ha presentado un crecimiento sostenido como consecuencia de los avances tecnológicos y mayores necesidades de comunicación por parte de la población, es así que, el número de líneas móviles al 2024,

asciende a 42.71 millones de líneas móviles, de esta manera, la penetración del servicio telefónico móvil se incrementó a 124.89 líneas por cada 100 habitantes.

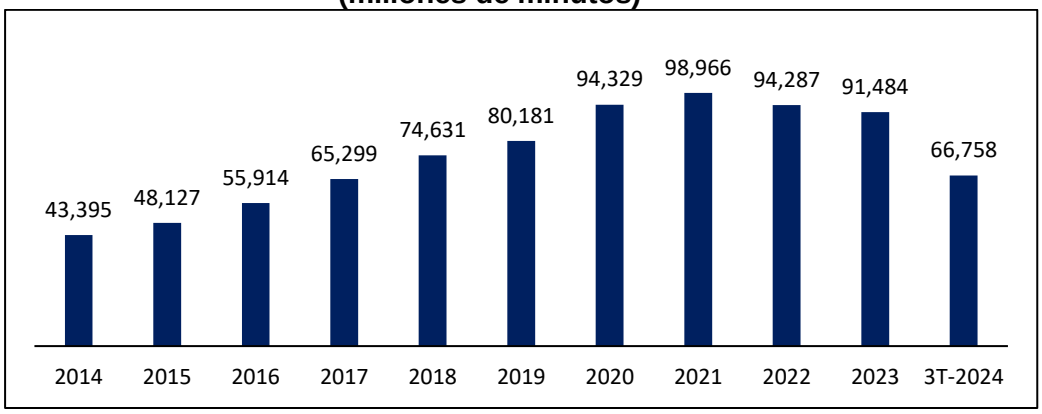
Gráfico 1. Líneas móviles en servicio (en millones) y Penetración a nivel nacional



Fuente: PUNKU-OSIPTEL.
Elaboración: Propia.

En esa línea, en los últimos 10 años (2014-2023) el tráfico de llamadas desde teléfonos móviles se ha incrementado en más de 110%, pasando de un total de 43,395 millones de minutos registrados en el 2013 a 91,484 millones de minutos registrados en el 2023, para comunicarse a teléfonos fijo y celulares del país y del exterior. Como se observa, si bien el tráfico de voz ha presentado una disminución respecto al periodo de pandemia, donde este se incrementó exponencialmente, debido a que los usuarios intensificaron el contacto a través de las llamadas, el tráfico de llamadas aún es superior a los periodos pre pandemia.

Gráfico 2. Tráfico de llamadas desde teléfonos móviles (millones de minutos)

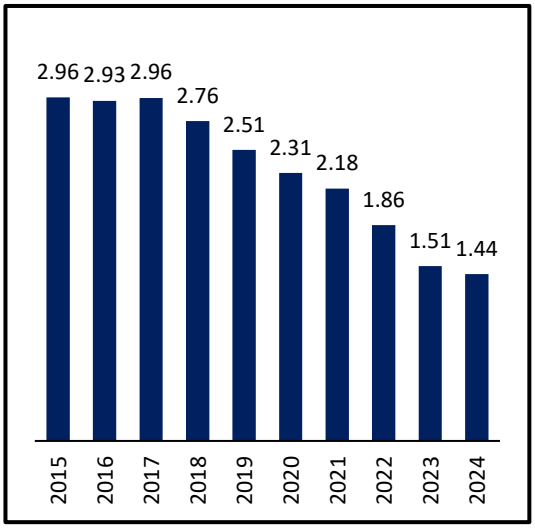


Fuente: PUNKU-OSIPTEL.
Elaboración: Propia.

Respecto de las líneas fijas de abonado, en los últimos 10 años, estas líneas han experimentado una notable reducción, con una caída del 51% en su número, descendiendo de más de 2.96 millones en 2015 a aproximadamente 1.44 millones en 2024. Esta disminución se atribuye al avance tecnológico y al aumento en la

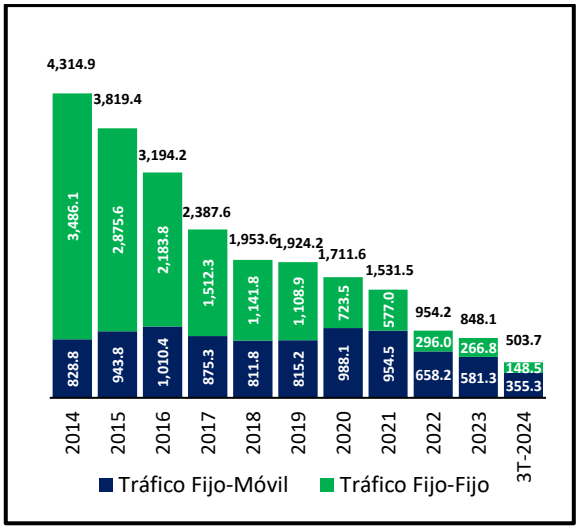
preferencia por los teléfonos móviles. Paralelamente, el tráfico de llamadas desde líneas fijas también ha disminuido significativamente, registrando una caída del 80% en la misma década (2014-2023). Además, el tipo de tráfico de llamadas ha experimentado un cambio, mientras que, en 2014, el 81% de las llamadas desde líneas fijas eran de fijo a fijo y solo el 19% eran de fijo a móvil, para el 3T-2024, estas proporciones se invirtieron, con el 71% de las llamadas dirigidas a móviles y solo el 29% de fijo a fijo. No obstante, las líneas fijas continúan siendo una herramienta de comunicación utilizada, con un total de 503.7 millones de minutos de tráfico registrado al tercer trimestre 2024. A pesar de su uso decreciente, las líneas fijas podrían representar un canal relevante para la realización de prácticas fraudulentas, lo que subraya la necesidad de mantener vigilancia y medidas de protección adecuadas.

Gráfico 3. Líneas fijas de abonados (en millones)



Fuente: PUNKU-OSIPTEL.
Elaboración: Propia.

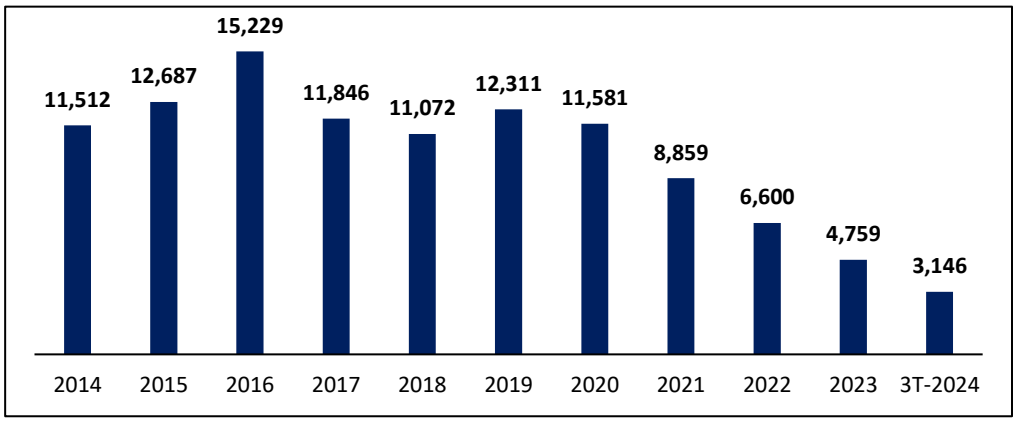
Gráfico 4. Tráfico de llamadas desde teléfonos fijos (millones de minutos)



Fuente: PUNKU-OSIPTEL.
Elaboración: Propia.

De otro lado, como herramienta de comunicación, tenemos a los mensajes de texto que, a pesar de la disminución en su uso, con una caída promedio anual del 9.3% en la última década (2014-2023), esta forma de comunicación sigue siendo activa en el Perú. Incluso, con el avance de las telecomunicaciones y la popularidad creciente de las redes sociales, tanto personas como empresas continúan recurriendo a los mensajes de texto. Esta persistencia se refleja en el hecho de que, al tercer trimestre de 2024, se enviaron aproximadamente 3,146 millones de mensajes de texto. Los mensajes de texto se utilizan no solo para comunicaciones personales entre familiares y amigos, sino también como una herramienta efectiva por parte de las empresas para promocionar productos y servicios o mantener el contacto con sus clientes.

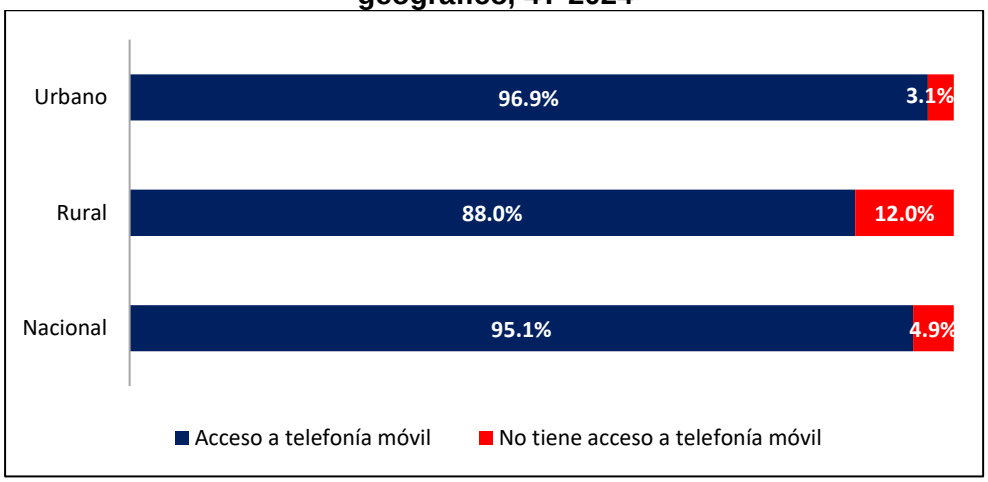
Gráfico 5. Tráfico de mensajes de texto (en millones)



Fuente: PUNKU-OSIPTEL.
Elaboración: Propia.

En ese contexto, como consecuencia del mayor número de líneas móviles debido a las mayores necesidades de comunicación por parte de la población, se tiene que de acuerdo al Instituto Nacional de Estadística e Informáticas (INEI, 2024), para el 4T-2024, el acceso a servicio de telefonía móvil en los hogares peruanos asciende al 95.1% de los hogares que cuentan con al menos un miembro con acceso al servicio de telefonía móvil a nivel nacional.

Gráfico 6. Hogares con acceso a telefonía móvil por ámbito geográfico, 4T-2024



Fuente: Encuesta Nacional de Hogares 4T-2024 – INEI.
Elaboración: Propia.

Bajo ese análisis se evidencia que gran parte de los hogares peruanos cuenta con algún miembro que tiene teléfono celular y, además, conforme a lo reportado a través de la Encuesta Residencial de Servicios de Telecomunicaciones (Erestel, 2023) realizada por OSIPTEL, los teléfonos móviles se han convertido en el dispositivo más presente en los hogares peruanos.

Ante este avance en el desarrollo de las telecomunicaciones y un uso masivo de los teléfonos celulares, se ha producido un uso inadecuado de las llamadas y mensajes de texto para la comisión de hechos ilícitos, así como para publicitar productos y servicios, conllevando al envío de comunicaciones no deseadas o spam y dentro de estas, posibles fraudes o estafas.

De acuerdo con Tu, Doupé y Zhao (2016)[1], varios factores contribuyen a la proliferación de las comunicaciones spam, es decir, la distribución masiva de contenido no deseado que afecta a los consumidores. Entre estos factores se destacan el avance tecnológico y la reducción de los costos asociados con la distribución de estas comunicaciones, así como la alta accesibilidad a los números de teléfono. Las comunicaciones *spam* no solo buscan promover productos y servicios, sino que también pueden estar orientadas a realizar estafas, fraudes, difundir campañas políticas, entre otras actividades.

Asimismo, el mencionado autor destaca que los *spammers* están encontrando maneras de eludir los mecanismos de defensa contra el *spam* telefónico, tales como el bloqueo de llamadas. Entre estas técnicas se incluye: (i) el uso de mensajes de voz automatizados, que permiten dejar mensajes pregrabados directamente en el buzón de voz de los destinatarios sin necesidad de que la llamada sea respondida o rechazada; y (ii) la suplantación o enmascaramiento de numeración, una práctica que implica falsificar deliberadamente la información de identificación del llamante que se muestra al destinatario. Estas estrategias subrayan la creciente vulnerabilidad de los usuarios frente a las molestias y riesgos asociados con las comunicaciones a través de llamadas y mensajes de texto.

Según un estudio realizado por Kimball et al. (2014)[2], revela que el 75% de las personas escucharon más de 19 segundos de una llamada automática, mientras que una abrumadora mayoría, el 97%, escuchan al menos 6 segundos de la misma. Estos hallazgos son indicativos de la considerable interrupción que estas llamadas representan para los usuarios, afectando significativamente su tiempo y atención, por lo que, este alto nivel de atención prestada a las llamadas automáticas subraya la eficacia de esta técnica de comunicación, aunque también plantea preocupaciones sobre su eventual fin ilícito, intrusividad y el impacto negativo en la vida diaria de los usuarios.

De esta manera, el *spam* telefónico tiene el potencial de ser más persuasivo que un *spam* por correo electrónico, especialmente cuando se usan técnicas como suplantación del identificador de llamadas, lo que da lugar a que las comunicaciones parezcan provenir de una fuente legítima cuando en realidad tienen un fin ilícito (fraudes o estafas), aumentando las posibilidades de que la llamada se responda y provoque importantes pérdidas económicas o financieras.

Por otro lado, el informe global del 2022 de Proofpoint[3], una empresa estadounidense de ciberseguridad empresarial, revela una preocupante falta de conciencia sobre las amenazas digitales emergentes, señalando que, solo el 29% y el 30% de los encuestados están familiarizados con los términos *smishing* y *vishing*, respectivamente, cifras que han permanecido relativamente constantes durante los últimos años, lo que indica una continua falta de conocimiento entre los usuarios acerca de estos tipos de amenazas digitales.

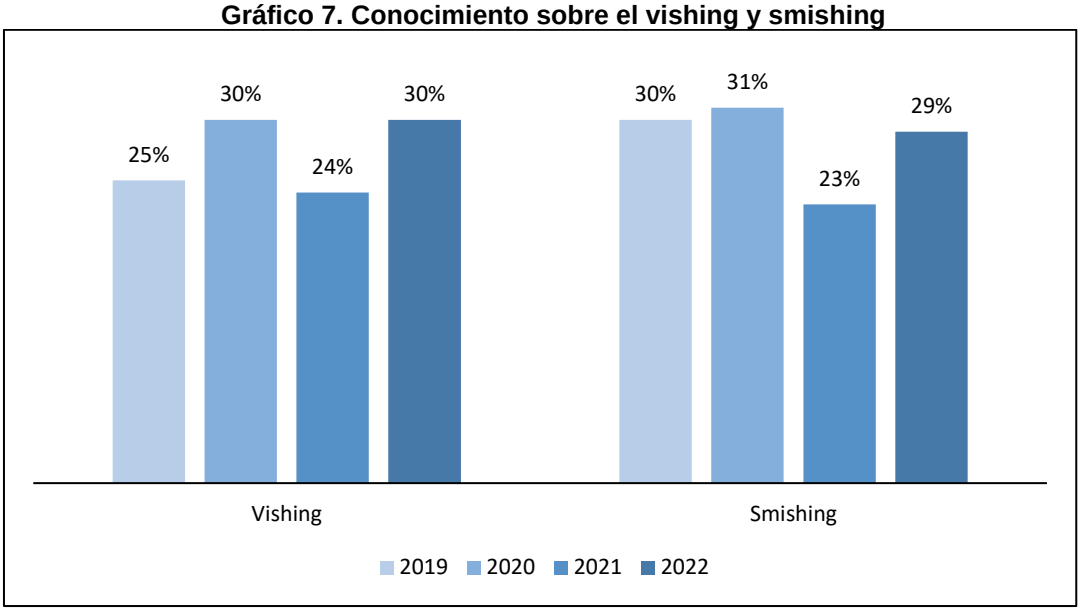
---

[1] Tu, H., Doupé, A., Zhao, Z., & Ahn, G.-J. (2016). Everyone hates robocalls: A survey of techniques against telephone spam. Recuperado de https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7546510

[2] Kimball, S. H., Levy, T., Venturelli, H., & Miller, S. (2014). "Interactive Voice Recognition Communication in Electoral Politics: Exploratory Metadata Analysis" American Behavioral Scientist. En esta investigación se consideró un total de 389,588 llamadas telefónicas respondidas en vivo desde la última semana de las elecciones de 2012 en Estados Unidos.

[3] Proofpoint. (2023). 2023 State of the Phish. Recuperado de https://assets-global.website-files.com/615d3b1833fa9330d4c96b6a/643d7471d2826f4534113baa_State%20of%20the%20Phish%202023%20SkyriverIT.pdf El informe se basa en encuestas realizadas a 7.500 adultos que trabajan y 1.050 profesionales de seguridad de TI en 15 países.

Gráfico 7. Conocimiento sobre el vishing y smishing



Fuente: Proofpoint. (2023). 2023 State of the Phish. El informe se basa en encuestas realizadas a 7.500 adultos que trabajan y 1.050 profesionales de seguridad de TI en 15 países.
Elaboración: Propia.

Además, según Proofpoint (Proofit, 2024)[4], una gran mayoría de los encuestados en su informe global del 2024, reconoce la presencia de este tipo de ataques, donde el 67% y el 75% indicaron que el *vishing* y el *smishing*, respectivamente, son algunas de las formas más comunes de ataques a la ciberseguridad. Estos datos resaltan la importancia de intensificar las acciones sobre ciberseguridad para combatir efectivamente la creciente incidencia de estos tipos de ataques cibernéticos

Según datos de la Federal Trade Commission (FTC)[5] de Estados Unidos, los consumidores reportaron pérdidas superiores a los $10 mil millones debido a fraudes en 2023, de un total de más de 2.5 millones de reportes de fraude. Los métodos de contacto más frecuentes utilizados por los estafadores fueron el correo electrónico, que representaron el 24%, las llamadas telefónicas, que representaron el 20%, y los mensajes de texto, con un 15%. Sin embargo, a lo largo de los últimos tres años, en promedio, las llamadas telefónicas han sido consistentemente el principal medio de contacto para cometer fraude, seguidas por los mensajes de texto y los correos electrónicos.

Asimismo, de acuerdo a los resultados de la "Encuesta sobre comunicaciones sin consentimiento"[6], en referencia a las llamadas, se observa que las personas que tienden a contestar siempre o casi siempre las llamadas reportan experiencias diversas: un 14.5% de estas llamadas son aquellas que llaman y cortan, un 14% son llamadas en las que el llamante no dice nada (silenciosas), y un 4.9% de las llamadas son identificadas por los encuestados como estafa o aparente estafa.

[4] Proofpoint. (2024). 2024 State of the Phish. Recuperado de https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-state-of-the-phish-2024.pdf

[5] Federal Trade Commission. (2024). Consumer Sentinel Network. Data Book 2023. Recuperado de https://www.ftc.gov/system/files/ftc_gov/pdf/CSN-Annual-Data-Book-2023.pdf

[6] Centro Especial de Monitoreo del Indecopi. (2022). Comunicaciones sin consentimiento. Recuperado de https://cdn.www.gob.pe/uploads/document/file/3619072/Comunicaciones%20sin%20consentimiento.pdf.pdf?v=1663019735

En efecto, más allá de ser simplemente una molestia, el spam puede ser un vehículo para actividades fraudulentas y estafas, incluidas llamadas de extorsión. Estas prácticas a menudo emplean técnicas de ingeniería social[7], que es una técnica de manipulación para explotar el error humano y obtener acceso a información privada, financiera, sistemas u objetos de valor. Este tipo de manipulación representa una amenaza seria para la seguridad de las telecomunicaciones y dentro del amplio espectro de amenazas y desafíos a esta seguridad, se encuentran modalidades de apropiación de identidad[8] como el *phishing, vishing* y *smishing*, cada uno adaptado a diferentes medios de comunicación para maximizar su efectividad y eludir las defensas tradicionales.

Por lo tanto, debido al avance tecnológico y al uso cada vez más generalizado de dispositivos electrónicos, como los teléfonos celulares, se ha observado un notable incremento en los fraudes informáticos, tan es así que, modalidades como el *phishing*, *vishing* y *smishing* son técnicas comúnmente utilizadas por ciberdelincuentes para extraer datos privados de los usuarios. Estas prácticas aprovechan la tecnología para engañar a las personas y obtener acceso ilegítimo a información confidencial.

En este contexto, es crucial considerar que, dado el alto porcentaje de hogares peruanos con acceso a teléfonos celulares y la preponderancia de las llamadas telefónicas y mensajes de texto como método de contacto por parte de las empresas, las personas se convierten en blanco de estafas y prácticas fraudulentas. Las estafas telefónicas y los mensajes de texto son los canales más utilizados para estas actividades ilícitas, poniendo en riesgo la seguridad y privacidad de los consumidores.

Panorama internacional

A nivel internacional, de acuerdo al Global Call Threat Report[9] (Hiya, 2024), durante el cuarto trimestre del 2023, se observaron 7.3 mil millones de llamadas spam[10] a nivel global, lo que significa que se generaron más de 81 millones de llamadas no deseadas cada día, ello significa, que este problema es un problema a nivel global.

Asimismo, conforme al reporte de Hiya, el 19% de las llamadas entrantes a nivel mundial fueron etiquetadas como llamadas molestas y el 6% como llamadas fraudulentas, ello significa que aproximadamente un 25% de las llamadas a nivel mundial, son llamadas spam. Las tasas de spam representan la cantidad de llamadas no deseadas de personas que no son contactos, que son llamadas realizadas desde números que no están en la libreta de direcciones local de un individuo.

---

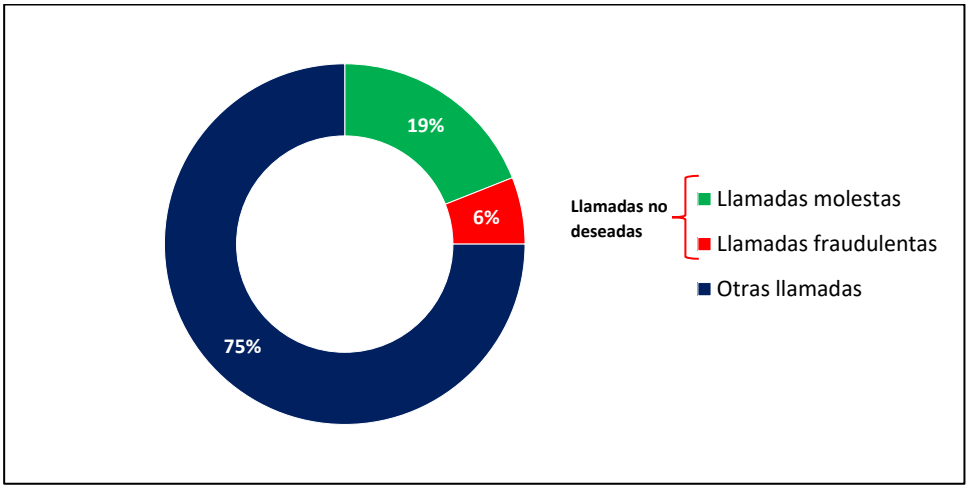
7 Kaspersky. (n.d.). ¿Qué es la ingeniería social? Recuperado de https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering

8 Osiptel. (2022). Amenaza y desafíos de la seguridad en las telecomunicaciones. Recuperado de https://cdn.www.gob.pe/uploads/document/file/3942954/Webinar%20-%20Amenazas%20y%20desaf%C3%ADos%20de%20la%20seguridad%20en%20las%20telecomunicaciones.pdf

9 Hiya. (2024). Global Call Threat Report Q4 2023. Recuperado de https://es.hiya.com/global-call-threat-report

10 De acuerdo a la metodología del reporte, spam se define como llamadas no deseadas e incluye tanto llamadas fraudulentas como llamadas molestas.

Gráfico 8. Participación del volumen de llamadas entrantes no deseadas a nivel mundial



Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

Este asunto de las llamadas spam, entre llamadas molestosas y llamadas por fraude, se ha convertido en un problema global, debido a que a nivel internacional se tiene que, para el cuarto trimestre de 2023, por ejemplo, en países como Estados Unidos, aproximadamente 2 de cada 10 llamadas son spam, donde el 28% son llamadas molestosas y el 1% son llamadas por fraude; mientras que, en Canadá, la situación es algo distinta, pues el 15% de las llamadas son llamadas molestosas y el 7% son llamadas por fraude.

En Estados Unidos, durante el tercer trimestre de 2023[11], las llamadas por fraude principalmente se han dado por estafas de perfiles comerciales de google, estafas haciéndose pasar por un familiar, esquemas dirigidos a varias plataformas de aplicaciones de pago donde el estafador llama diciendo que hay un problema con la cuenta y que necesita verificar la información de la cuenta y la contraseña del usuario para aclarar las cosas y la estafa del “sí” donde si el destinatario responde "sí" y la llamada se graba, se puede editar para que suene como si la persona hubiera autorizado la compra de un producto o servicio. Mientras que, durante el cuarto trimestre de 2023[12], las llamadas fraudulentas más comúnmente reportadas estaban relacionadas con temas como Medicare, seguros, impuestos, Amazon, tarjetas de crédito, alivios de deuda y fiscal, así como aplicaciones de plataformas de pago como Venmo y PayPal. Además, numerosos usuarios indicaron que estas llamadas fraudulentas apuntaban frecuentemente a personas mayores, explotando su vulnerabilidad. Durante el mismo período, también emergieron noticias sobre víctimas que fueron engañadas por cloness de la voz de sus seres queridos, una táctica cada vez más sofisticada y preocupante en el ámbito del fraude telefónico

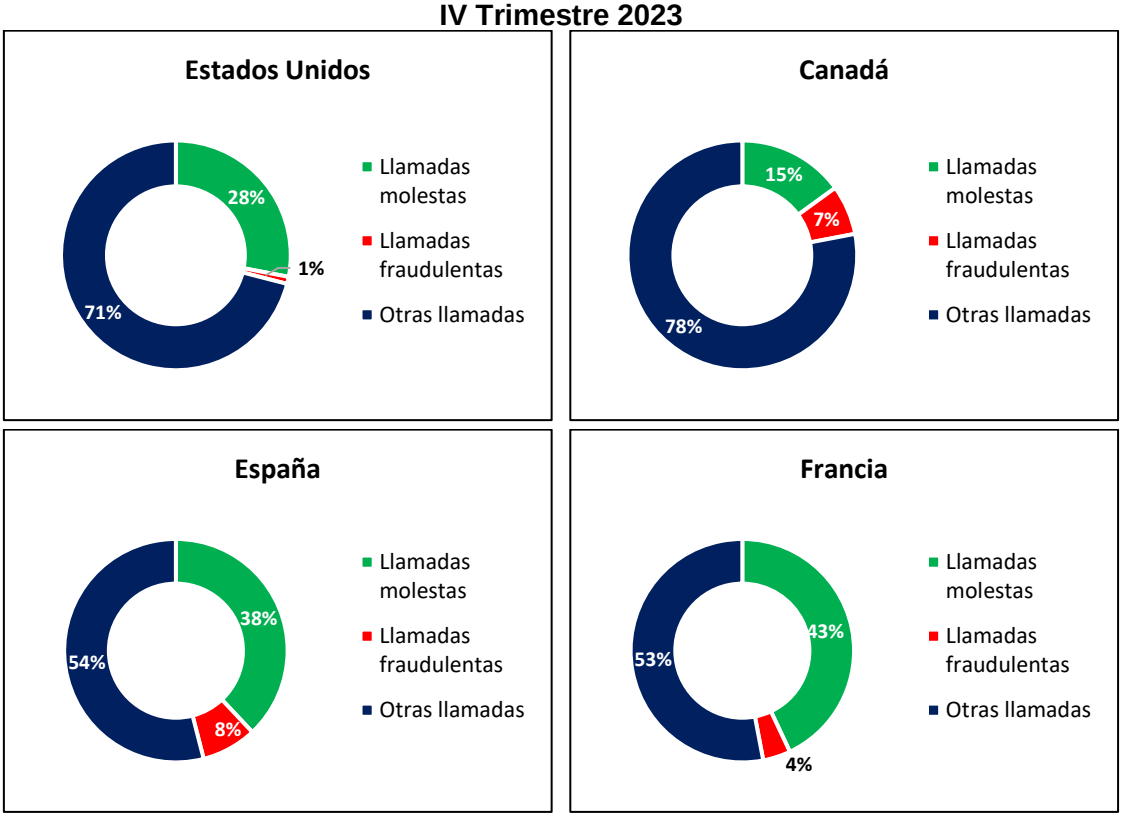
De otro lado, durante el tercer y cuarto trimestre de 2023 en Canadá (Hiya, 2023), se tiene que las principales llamadas por fraude se dieron por llamadas fraude de Amazon, por suplantación de identidad donde se hacían pasar por empleados del gobierno o algún familiar o llamadas por fraude para apoderarse de los datos de las tarjetas de crédito, así como, fraude por vacaciones.

[11] Hiya. (2023). Global Call Threat Report Q3 2023.
[12] Hiya. (2024). Global Call Threat Report Q4 2023.

De acuerdo a Hiya, para el cuarto trimestre 2023, las tasas más altas de llamadas spam en Europa las lideran Francia y España, con tasas de spam del 47% (43% de llamadas molestosas y 4% de llamadas por fraude) y 46% (38% de llamadas molestosas y 8% de llamadas por fraude), respectivamente.

En España, casi la mitad de las llamadas recibidas de números que no están en la libreta de contactos, son llamadas spam, donde las estafas por llamadas más comunes son las estafas bancarias, donde el estafador se hace pasar por un trabajador del banco para obtener sus datos e información personal como cuentas y contraseñas, las estafas de seguro, así también, las estafas por llamadas y/o mensajes sms haciéndose pasar por un familiar para obtener dinero, además, las estafas wangiri (donde la persona que llama, llama una vez y cuelga con la esperanza de que el destinatario vuelva a marcar a un número de tarifa premium). De otro lado, en Francia, se han identificado estafas en la entrega de paquetes donde los estafadores llaman o envían un mensaje sms indicando que el paquete se encuentra en espera y deberán pagar una tarifa de envío, así también, llamadas para estafar sobre programas de ayudas del gobierno y las estafas por llamadas bancarias. Asimismo, ha aparecido en Francia una estafa llamada “Hello mom”, en la que el estafador se hace pasar por un hijo y envía un mensaje SMS diciendo que su teléfono está roto y solicita conectarse por WhatsApp y pronto sigue una solicitud urgente de dinero (Hiya, 2023).

Gráfico 9. Porcentaje del volumen de llamadas entrantes no deseadas respecto del total de llamadas de no contactos
IV Trimestre 2023

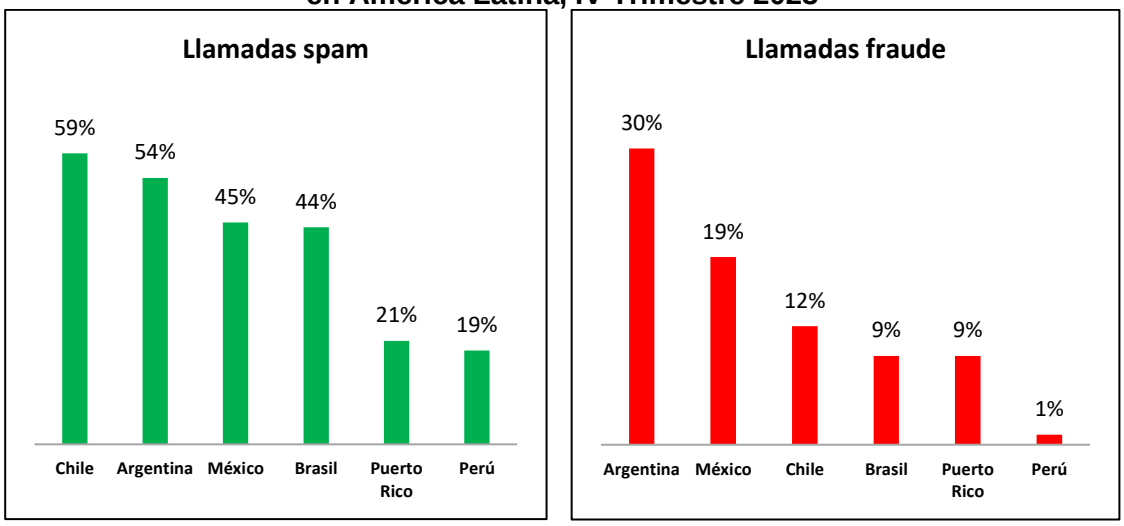


Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

Para el caso latinoamericano, de acuerdo a Hiya, durante el cuarto trimestre de 2023, Chile se ubicó como el país con la mayor tasa de spam no solo en

Latinoamérica, sino en todo América[13], mientras que, Argentina se ubicó como el país con la mayor participación de llamadas fraudulentas.

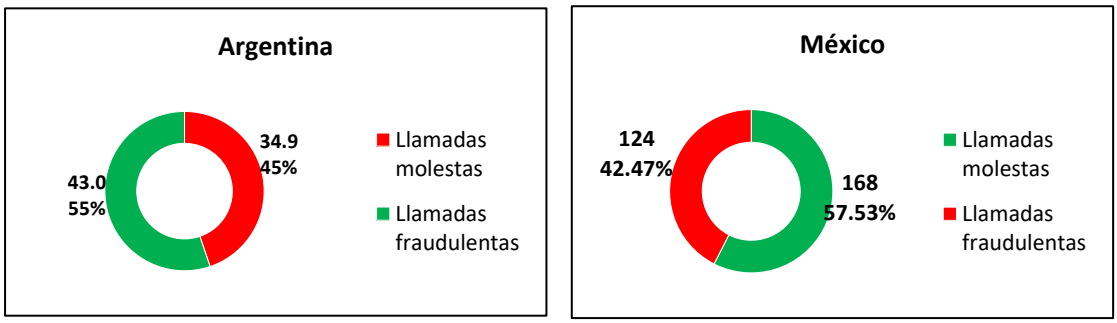
Gráfico 10. Porcentaje del volumen de llamadas spam y llamadas fraudulentas en América Latina, IV Trimestre 2023



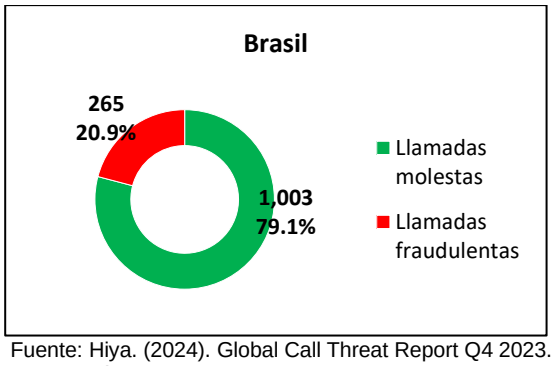
Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

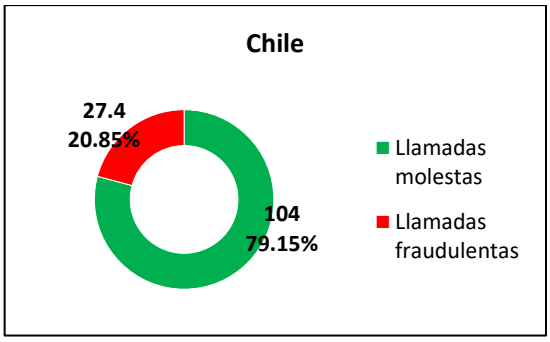
En esa línea, se observa que, de acuerdo al reporte de Hiya, que si bien Chile es el país con la mayor tasa de llamadas spam de Latinoamérica, Argentina presenta la mayor tasa de llamadas para acciones fraudulentas respecto de las llamadas no deseadas de "no contactos", que son llamadas realizadas desde números que no están en el teléfono de un individuo, donde alrededor del 55% de todas las llamadas spam, representaban llamadas para acciones de fraude, de otro lado, para México, del total de llamadas calificadas como spam, el 42.47% representaban llamadas fraudulentas, mientras que para Brasil y Chile, el 20.9% y 20.85% de todas las llamadas calificadas como spam, representaban llamadas fraudulentas, respectivamente.

Gráfico 11. Total de llamadas spam en países de América Latina, III Trimestre 2023 (en millones)



[13] En el tercer trimestre de 2023, Chile se ubicó como el país con la mayor tasa de llamadas spam (Hiya, 2023).



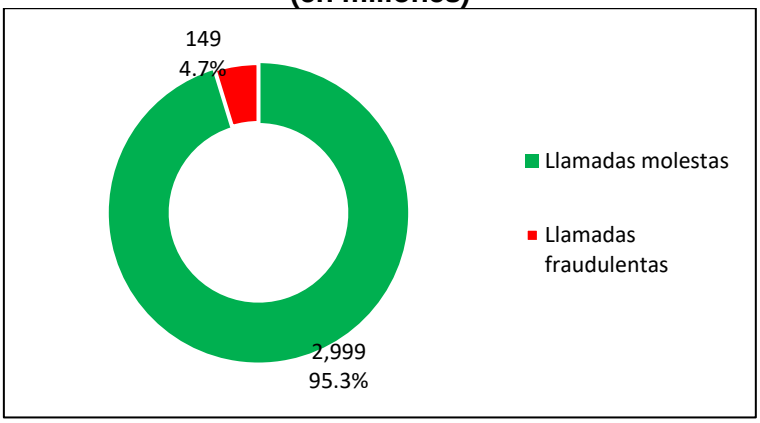


Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

Estados Unidos

Como se indicó previamente, de acuerdo al Global Call Threat Report, elaborado por Hiya para el cuarto trimestre de 2023, Estados Unidos presentó una tasa del 28% del total de llamadas entrantes que no están en los contactos, como llamadas molestosas y un 1% como llamadas por fraude; mientras que, si solo consideramos a las llamadas spam, el 4.75% de estas son llamadas fraudulentas.

Gráfico 12. Volumen de llamadas entrantes no deseadas
IV Trimestre 2023
(en millones)



Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

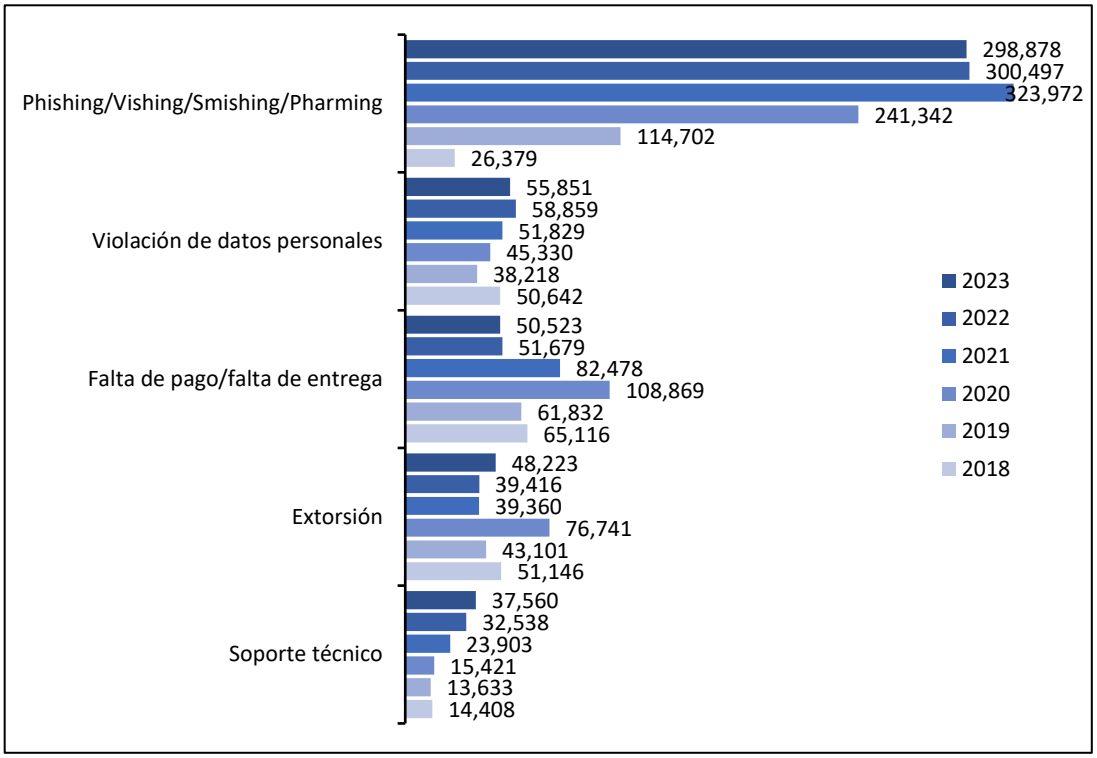
Esta fuerte presencia de llamadas y mensajes fraudulentos se puede evidenciar a su vez en las denuncias existentes por este tipo de delito.

De acuerdo al documento Internet Crime Report 2023 del Federal Bureau of Investigation (FBI)[14], el principal crimen digital está relacionado a actividades de ingeniería social, tales como el *phishing, vishing y smishing*, las cuales han presentado un mayor crecimiento en los últimos cinco años, donde se registró para el 2023, un incremento en las denuncias por *phishing/vishing/smishing/pharming* de más de 1,000% respecto del 2018[15].

[14] Federal Bureau of Investigation. (2024). Internet Crime Report 2023. Recuperado de https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

[15] Federal Bureau of Investigation. (2022). Internet Crime Report 2021. Recuperado de https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

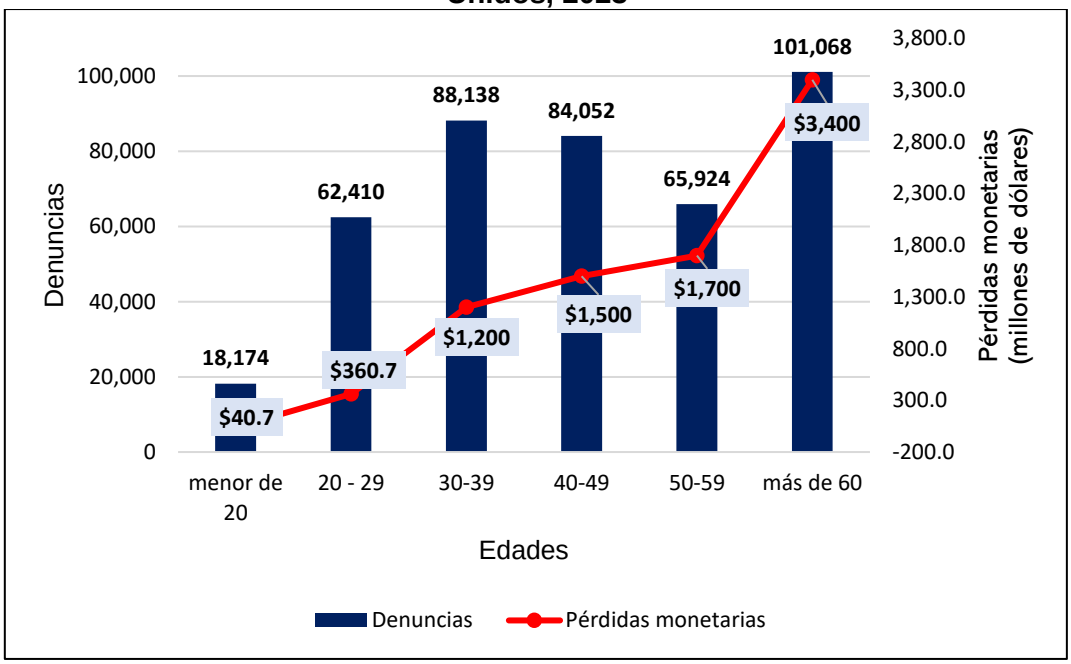
Gráfico 13. Crecimiento de los cinco principales delitos digitales en Estados Unidos



Fuente: Internet Crime Report 2023. Internet Crime Report 2021.
Elaboración: Propia.

Asimismo, el documento indica que el grupo de personas que presentó la mayor cantidad de víctimas de delitos digitales fueron las personas mayores de 60 años, quienes a su vez tuvieron las mayores pérdidas por estos delitos.

Gráfico 14. Víctimas de delitos digitales según grupos de edad en Estados Unidos, 2023



Fuente: Internet Crime Report 2023.
Elaboración: Propia.

Además, indican que los *call centers* ilegales defraudan miles de personas cada año, suplantando la identidad a través de servicios de apoyo técnico al cliente, así como, de trabajadores del gobierno. Estos se dirigen principalmente a las personas mayores, con efectos devastadores. Casi la mitad de las víctimas dicen tener más de 60 años (40%) y experimentan el 58% de las pérdidas (más de 770 millones de dólares).

Respecto a las pérdidas monetarias de las víctimas por *phishing / vishing / smishing / pharming/spoofing* durante el 2023, estas ascendieron a más de 18.7 millones de dólares.

Siguiendo esa línea de análisis, conforme al reporte de Robokiller[16] para Estados Unidos, se tiene registrado que para el 2022, los estafadores enviaron 225,700 millones de mensajes de texto no deseados, presentando un incremento del 157% respecto a la cantidad de mensajes de texto no deseados enviados en el 2021. Ello a su vez generó pérdidas estimadas de 20,600 millones de dólares, presentando un incremento del 105% respecto de las pérdidas estimadas en el 2021. De otro lado, durante el primer semestre de 2023, se estiman pérdidas monetarias por mensajes de texto de aproximadamente 13 mil millones de dólares[17].

Por lo tanto, se evidencia que, incluso en un país desarrollado como Estados Unidos, este tipo de fraude tecnológico ha comprometido significativamente la seguridad de la información de los ciudadanos, generando grandes pérdidas económicas. Este contexto resalta la urgencia y necesidad de implementar acciones robustas para proteger a la población y restablecer la confianza en los sistemas de comunicación, un desafío que no es exclusivo de un solo país, sino que es una preocupación global que requiere atención inmediata.

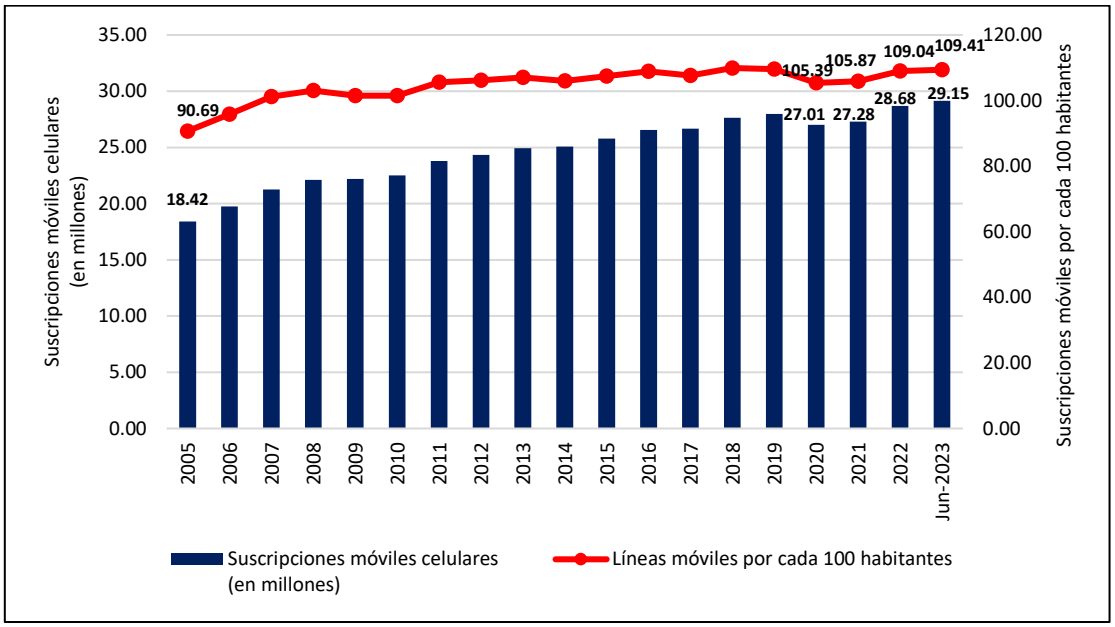
Australia

Por su parte, Australia que ha presentado un crecimiento constante en el número de líneas móviles celulares en los últimos 18 años, durante el periodo del 2020 al 2022 ha presentado un crecimiento aproximado del 6% en el número de líneas móviles, similar al crecimiento presentado por el Perú en dicho periodo. Al primer semestre de 2023, la cantidad de líneas móviles celulares asciende a 29.15 millones, indicando un nivel de penetración de 109.41 líneas móviles por cada 100 habitantes. Al igual que Perú, Australia evidencia la existencia de más líneas móviles por habitantes.

[16] Robokiller. (2022). The Robokiller phone scam report | 2022 insights & analysis. Recuperado de https://www.robokiller.com/robokiller-2022-phone-scam-report

[17] Robokiller (2023). The Robokiller Phone Scam Report | 2023 mid-year Insights & Analysis. Recuperado de https://www.robokiller.com/robokiller-2023-mid-year-phone-scam-report

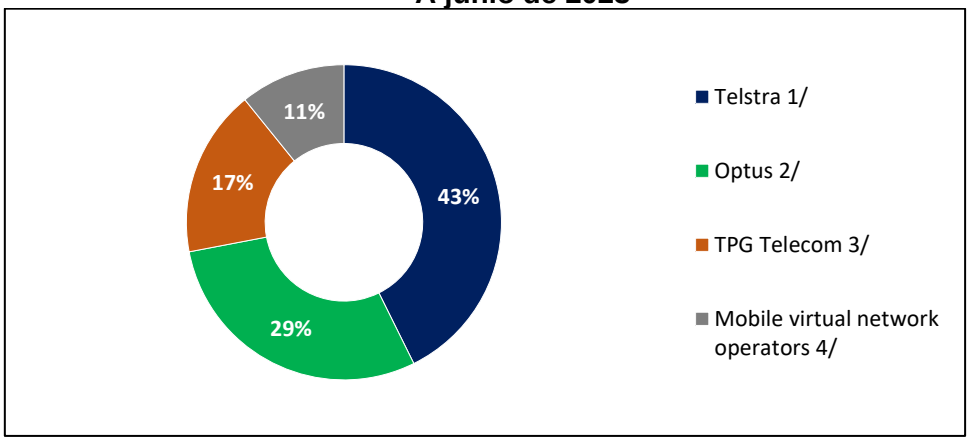
Gráfico 15. Suscripciones móviles celulares (en millones) y Penetración a nivel nacional



Fuente:
Mobile-cellular subscriptions. DataHub. ITU.
Internet activity report For the period ending 30 June 2023. ACCC.
National, state and territory population. June 2023. Australian Bureau of Statistics.
Elaboración: Propia.

En ese contexto, también se tiene que el mercado móvil australiano presenta características similares al peruano, puesto que además, son tres los operadores que comprenden una participación de más del 80% del mercado móvil. Para el caso australiano, los tres principales operadores concentran el 89% del total de líneas móviles en servicio, siendo el operador Telstra quien tiene una participación del 43% de líneas móviles en operación.

Gráfico 16. Participación del mercado móvil australiano (% líneas móviles en operación)
A junio de 2023

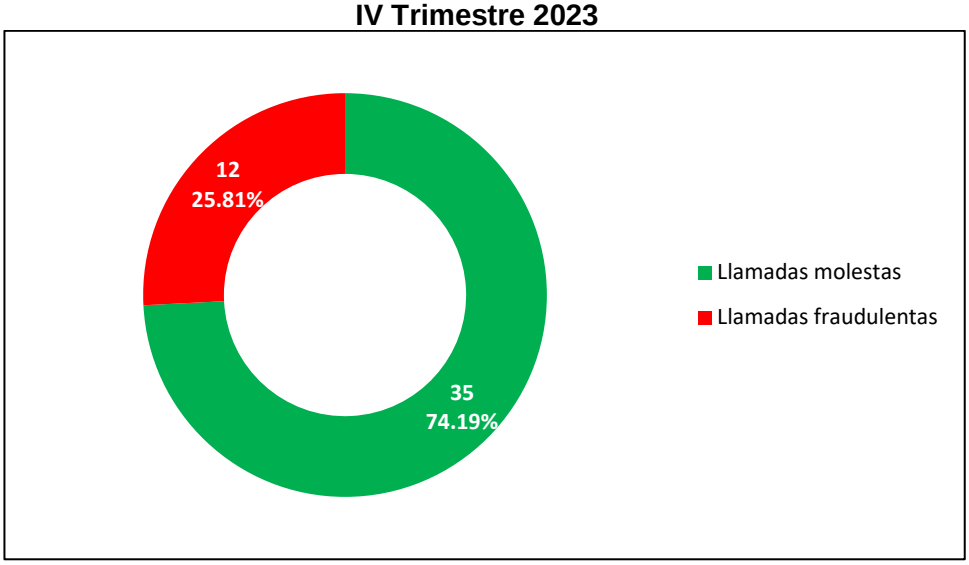


Notas:
1/ Incluye marcas propias y secundarias de Telstra.
2/ Incluye marcas propias y secundarias de Optus.
3/ Incluye marcas propias y submarcas de TPG Telecom.
4/ Es la suma de los servicios mayoristas prepago y pospago.
Fuente: Internet activity report For the period ending 30 June 2023. ACCC. Disponible en: https://www.accc.gov.au/by-industry/telecommunications-and-internet/telecommunications-industry-record-keeping-and-reporting-rules/internet-activity-record-keeping-rule/june-2023-report
Elaboración: Propia.

Conforme se extiende el uso de los teléfonos móviles y la tecnología, Australia ha presentado problemas por fraude informático, ya sea a través de las llamadas o mensajes de texto fraudulentos.

De acuerdo al Global Call Threat Report, elaborado por Hiya, para el cuarto trimestre de 2023, alrededor de 3 de cada 10 llamadas no identificadas son spam, donde el 21% son llamadas molestosas y el 7% son llamadas por fraude. No obstante, si solo consideramos a las llamada spam, la tasa de llamadas por fraude es del 25.81%.

Gráfico 17. Porcentaje del volumen de llamadas por fraude del total de llamadas entrantes no deseadas
IV Trimestre 2023



Fuente: Hiya. (2024). Global Call Threat Report Q4 2023.
Elaboración: Propia.

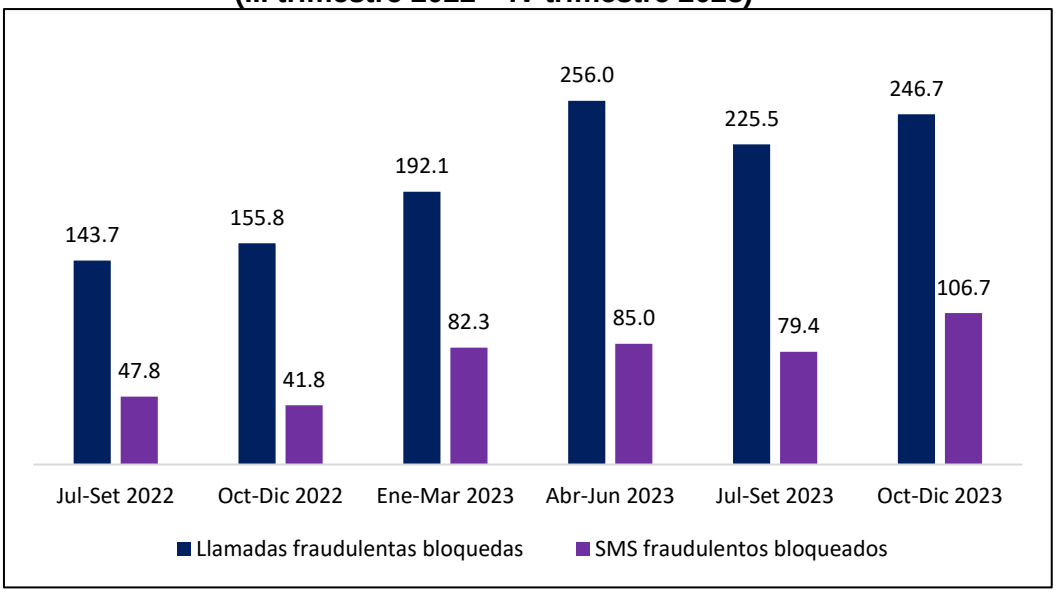
Asimismo, conforme al Intelligence Report Q4 2022-23[18] elaborado por the Australian Communications and Media Authority (the ACMA), tan solo durante el segundo trimestre de 2023, se han bloqueado más de 250 millones de llamadas por fraude y más de 85 millones de mensajes de texto fraudulentos. Respecto del total de bloqueo de llamadas fraudulentas, el reporte indica que el 82% del bloqueo de llamadas corresponde a bloqueos por “Números australianos no válidos o no asignados” o “Números internacionales no válidos (código de país o longitud de dígitos no asignados)”; mientras que en el caso de los sms bloqueados, el 42% de los bloqueos en dicho trimestre corresponden a bloqueos por “SMS bloqueados que se originan en los propios clientes de los operadores” o a “SMS bloqueados recibidos de operadores de tránsito o de origen”.

En esa línea, desde diciembre de 2020, se han bloqueado más de 1,800 millones de llamadas fraudulentas, y desde julio de 2022, se han bloqueado otros 443 millones de mensajes SMS fraudulentos[19][20]. De esta manera, estas cifras impresionantes no solo confirman la existencia, sino también el creciente problema de este tipo de actividades fraudulentas. Por lo que, el volumen

[18] Australian Communications and Media Authority. (2023). Phone scams: Intelligence report Q4 2022-23.
[19] Australian Communications and Media Authority. (2023). Action on scams, spam, and telemarketing: April to June 2023. Recuperado de https://www.acma.gov.au/publications/2023-08/report/action-scams-spam-and-telemarketing-april-june-2023
[20] Australian Communications and Media Authority. (2024). Action on scams, spam, and telemarketing: October to December 2023. Recuperado de https://www.acma.gov.au/publications/2024-02/report/action-scams-spam-and-telemarketing-october-december-2023

significativo de comunicaciones bloqueadas refleja la eficacia de las medidas implementadas en Australia para proteger a los consumidores de estas amenazas persistentes y disruptivas.

Gráfico 18. Cantidad de llamadas y sms fraudulentos bloqueados (III trimestre 2022 – IV trimestre 2023)



Fuente: Australian Communications and Media Authority. (2024). Action on scams, spam, and telemarketing: October to December 2023.
Elaboración: Propia.

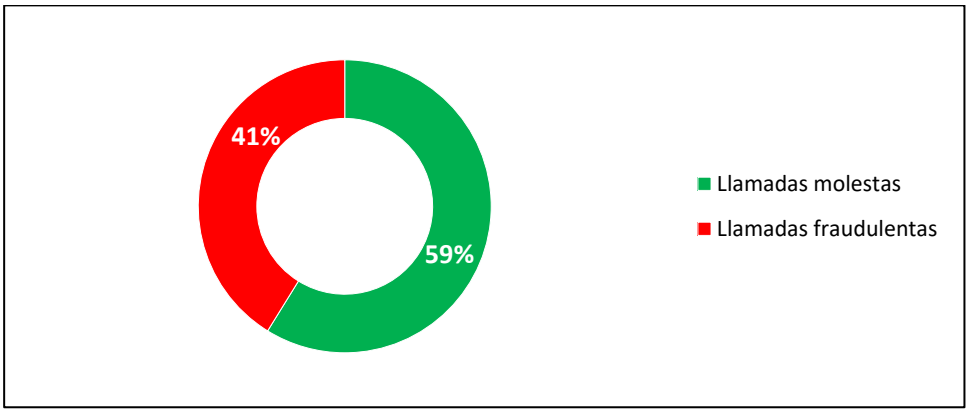
Panorama Nacional

Siguiendo este análisis y conforme al panorama internacional, queda claro que las amenazas asociadas con las prácticas ilícitas en las comunicaciones, ya sea mediante llamadas o mensajes de texto, no son exclusivas de países desarrollados como Estados Unidos o aquellos con mercados móviles similares como Australia; sino que estas también afectan significativamente al escenario local.

En el Perú, durante el cuarto trimestre de 2023, el panorama de las comunicaciones no deseadas reveló un dato alarmante: el 41% de todas las llamadas catalogadas como spam fueron identificadas como fraudulentas, mientras que el 59% restante correspondió a llamadas molestosas[21]. En efecto, este elevado porcentaje de fraudes telefónicos no solo subraya la magnitud del problema, sino que también resalta el considerable riesgo que estas prácticas representan para la seguridad y la privacidad de la población. Es así que, la significativa presencia de llamadas fraudulentas es un claro indicativo de que los estafadores están utilizando activamente este medio para engañar y obtener beneficios ilícitos, lo que requiere una respuesta urgente y medidas robustas para proteger a la población.

[21] Hiya. (2024). Global Call Threat Report Q4 2023.

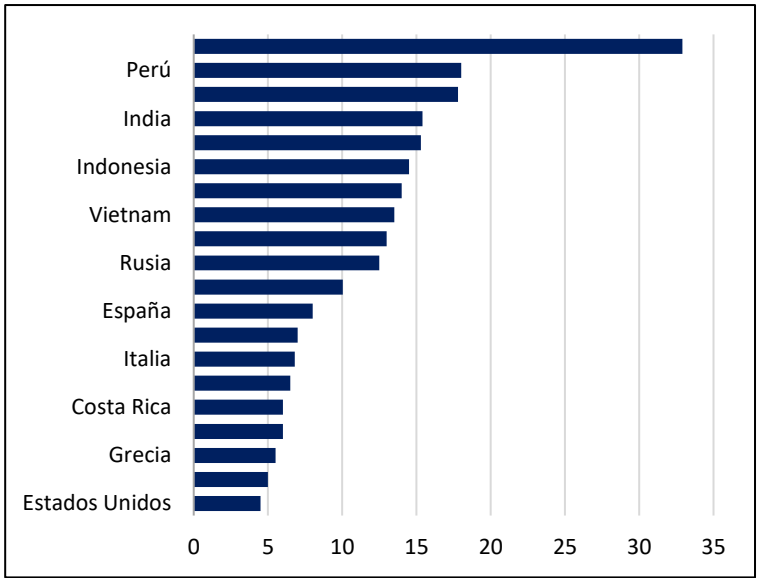
Gráfico 19. Porcentaje de llamadas fraudulentas respecto del total de llamadas spam
IV Trimestre 2023



Fuente: Global Call Threat Report. Insights into today's worldwide spam problem. Q3 2023. Hiya.
Elaboración: Propia.

Asimismo, de acuerdo al informe anual llamado Truecaller Insigths 2021[22], Perú fue el país más afectado por las llamadas no deseadas durante el 2021, con un promedio de 18.02 llamadas al mes por usuario. De igual manera, durante el 2019[23], Perú se volvió a ubicar como el segundo país más afectado por llamadas spam, con una cifra que asciende a 30.9 llamadas al mes por usuario, sin embargo, en el 2020, se ubicó en el puesto 14 con un total de 12.8 llamadas al mes por usuario, evidenciando de igual forma, la gran presencia de este tipo de llamadas.

Gráfico 20. Top 20 de los países afectados por llamadas spam en 2021



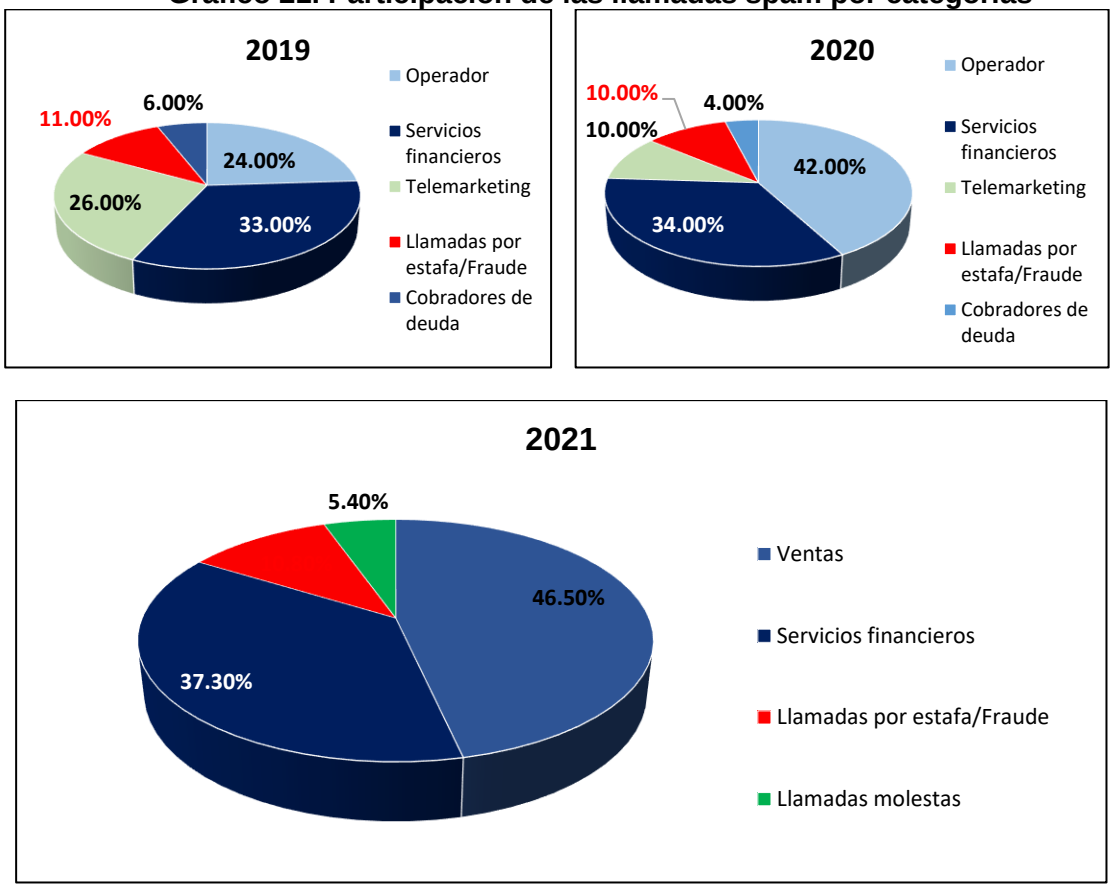
Fuente: 2021 Global Spam & Scam Report. Truecaller Insights: Top 20 Countries Affected By Spam Calls In 2021.

[22] Truecaller. (2022). Truecaller insights: Top 20 Countries Affected By Spam Calls in 2021. 2021 Global Spam & Scam Report. Recuperado de https://www.truecaller.com/blog/insights/top-20-countries-affected-by-spam-calls-in-2021

[23] Truecaller. (2019). Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019. The top 20 Countries Affected by Spam Calls & SMS in 2019. Recuperado de https://www.truecaller.com/blog/insights/truecaller-insights-top-20-countries-affected-by-spam-calls-sms-in-2019
Truecaller. (2020). Truecaller Insights: Top 20 Countries Affected by Spam Calls in 2020. 2020 Global Spam & Scam Report. Extraído de https://www.truecaller.com/blog/insights/truecaller-insights-top-20-countries-affected-by-spam-calls-in-2020-2

En esa línea, de acuerdo a los informes Truecaller Insigths para los años 2019, 2020 y 2021, se observa que para el Perú, la participación de las llamadas categorizadas como fraude o estafa ha representado entre el 10% y 11% del total de llamadas marcadas como spam, lo que indica que este tipo de llamadas ha presentado un comportamiento constante y presente durante esos tres años.

Gráfico 21. Participación de las llamadas spam por categorías



Fuente:
Truecaller. (2022). Truecaller insights: Top 20 Countries Affected By Spam Calls in 2021. 2021 Global Spam & Scam Report.
Truecaller. (2020). Truecaller Insights: Top 20 Countries Affected by Spam Calls in 2020. 2020 Global Spam & Scam Report.
Truecaller. (2019). Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019.The top 20 Countries Affected by Spam Calls & SMS in 2019.
Elaboración: Propia.

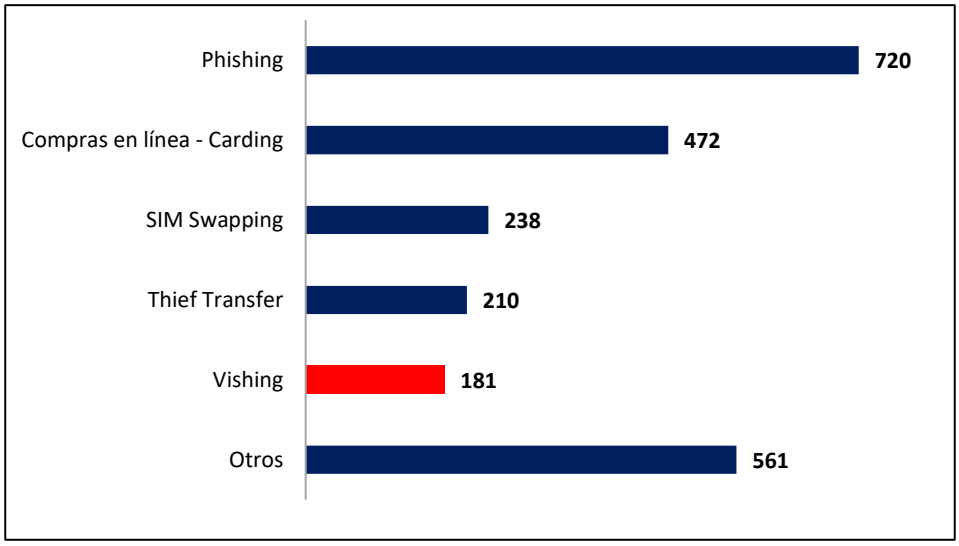
Bajo este contexto, existe una fuerte presencia de llamadas fraudulentas no solo a nivel internacional, sino también a nivel nacional como se ha expuesto en las líneas precedentes, lo cual a su vez se evidencia en las denuncias por este tipo de delito.

En el Perú, la ola de fraudes informáticos se ha vuelto muy recurrente, tan es así que, durante el 2022, según datos de la División de Alta Tecnología (Divindat), se registraron 2,382 denuncias por causas de fraude informático[24], lo cual lo convierte en el delito informático más denunciado en ese año.

Si bien el *phishing* es la modalidad de fraude más frecuente, otras modalidades de fraude están tomando relevancia como el *vishing*, donde el 8% de las denuncias presentadas por fraude, correspondían a esta modalidad.

[24] https://www.elperuano.pe/noticia/216043-cuidado-con-los-fraudes-informaticos-estas-son-las-modalidades-mas-denunciadas-en-peru

Gráfico 22. Denuncias por modalidad de fraude 2022



Fuente: DIVINDAT
Elaboración: Propia.

Asimismo, conforme a lo indicado por el Ministerio Público, hasta el 31 de octubre de 2022, se han atendido 9,403 casos de delitos informáticos solo en Lima Centro y 16 distritos de la capital[25], donde las modalidades de delitos más frecuentes fueron los fraudes informáticos y las estafas agravadas, que se aplican por la modalidad de *vishing, phishing y smishing.*

Además, de acuerdo a la División de Estafas y Otras Defraudaciones (Divieod) de la Policía Nacional del Perú (PNP), durante los meses de enero y mayo del 2023, se recibieron 3,410 denuncias por estafa en Lima Metropolitana[26], donde las llamadas suplantando la identidad de un familiar fue el método más común de estafa, representando el 16% de las denuncias presentadas en dicho periodo y, de otro lado, las denuncias por suplantación de identidad representaron el 10%.

En esa línea, estas denuncias por estafa generan perjuicios económicos a los ciudadanos, tan es así que, las estafas por llamada familiar representaron pérdidas económicas de S/ 391,576.60 y, por otro lado, las pérdidas económicas por suplantación de identidad ascendieron a S/ 1,067,886.94.

En este contexto, una de las principales empresas operadoras de telecomunicaciones en Perú ha emitido una alerta sobre una creciente campaña de smishing que afecta a sus usuarios[27]. Esta estrategia maliciosa se manifiesta a través de mensajes de texto que informan sobre el supuesto vencimiento de una popular promoción de la operadora. Estos mensajes de texto engañosos invitan a los usuarios a ingresar a un enlace que simula ser la tienda virtual de la operadora, con el objetivo de sustraer información personal sensible, principalmente los datos de las tarjetas de crédito o débito de los usuarios, por lo que, aquellos que puedan ser víctimas de esta trampa están en riesgo de sufrir significativas pérdidas económicas debido al fraude.

[25] https://www.linkedin.com/pulse/en-el-2022-ministerio-p%C3%BAblico-recibi%C3%B3-casi-10-mil-denuncias-/?originalSubdomain=es

[26] https://elcomercio.pe/lima/la-llamada-telefonica-o-mensaje-de-un-supuesto-familiar-es-la-estafa-mas-utilizada-en-lima-metropolitana-de-que-formas-operan-los-delincuentes-informe-ecdata-delincuencia-delitos-crimen-seguridad-pnp-policia-nacional-del-peru-noticia/?ref=ecr#google_vignette

[27] Cornejo, D. (2024). Esta es la nueva modalidad de estafa a clientes de Claro: ¿cómo operan para robar datos personales? La República. Recuperado de https://larepublica.pe/sociedad/2024/05/01/nueva-modalidad-de-estafa-a-usuarios-de-claro-asi-obtienen-datos-personales-para-robar-informacion-claro-puntos-claro-club-76386

Gráfico 23. Campaña de smishing a usuarios de América Móvil

Fuente: Cornejo, D. (2024). La República. Recuperado de https://larepublica.pe/sociedad/2024/05/01/nueva-modalidad-de-estafa-a-usuarios-de-claro-asi-obtienen-datos-personales-para-robar-informacion-claro-puntos-claro-club-76386

En resumen, las modalidades por fraude a través de las llamadas telefónicas y mensajes de texto han tomado relevancia en el contexto nacional, tan es así que el porcentaje de llamadas por fraude ha presentado una tasa de entre el 10% y 11% del total de llamadas spam, tasa que ha sido superior a la de muchos países de Sudamérica, siendo superado solo por Brasil, incluso Perú ha presentado una mayor tasa de llamadas por fraude que países desarrollados como Estados Unidos.

5.1.1. Identificación del problema público

El creciente avance tecnológico y el aumento en el uso de los servicios públicos de telecomunicaciones han contribuido significativamente al desarrollo social, educativo y económico. No obstante, este crecimiento también ha expuesto a la sociedad a nuevas vulnerabilidades, siendo aprovechadas por actores malintencionados para cometer delitos como el robo de identidad y la realización de estafas o fraudes. Estos criminales utilizan técnicas de ingeniería social para obtener información confidencial, personal y financiera, manipulando los servicios de telecomunicaciones para sus fines ilícitos.

Dentro de las actividades delictivas más comunes en este ámbito se encuentran el *smishing* y el *vishing*, perpetrados a través de los servicios de telefonía y mensajes de texto. Estas prácticas no solo violan la privacidad individual, sino que también erosionan la confianza en los servicios de telecomunicaciones, impactando negativamente en la percepción de seguridad de dichos servicios.

Cabe mencionar que, frecuentemente, los delincuentes emplean tácticas como el enmascaramiento del número de origen, tanto en llamadas como en mensajes de texto. Estos, utilizan centrales virtuales, que pueden operar tanto dentro como fuera del país, para interconectarse indirectamente con las redes de telecomunicaciones peruanas. Ello, les permite presentarse falsamente como entidades legítimas y de esta manera, se facilita la gestión de fraudes. De forma similar, existen aplicaciones móviles que permiten configurar un número llamante (identificador de llamada) y son usadas para este tipo de engaños, complicando aún más la detección y prevención de estas actividades fraudulentas.

En este contexto, la problemática actual no solo pone en riesgo la seguridad de la información personal y financiera de los individuos, sino que también erosiona la confianza en los sistemas de telecomunicaciones en su conjunto. Este problema público es complejo y multifacético, lo que subraya la urgencia de implementar una respuesta regulatoria efectiva, siendo esencial desarrollar y aplicar regulaciones que protejan a la población, garanticen la seguridad de las comunicaciones y preserven la integridad de los sistemas de telecomunicaciones; solo así se podrá garantizar un entorno de telecomunicaciones seguro y confiable para todos los usuarios.

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

El desarrollo tecnológico y la masificación de las redes de telecomunicaciones han transformado radicalmente la forma en que las personas se comunican, acceden a la información y participan en la vida económica, social y cultural. Sin embargo, este avance también ha traído desafíos importantes, especialmente en cuanto al mal uso de estas redes.

Uno de estos desafíos tiene que ver con las comunicaciones no deseadas que tienen por objeto la realización de actividades ilícitas como el robo de identidad, fraudes bancarios, estafas, phishing, extorsión, etc., siendo que los delincuentes aprovechan el anonimato y el alcance global de las redes de telecomunicaciones para causar afectación a la población.

Así también, otro de los grandes desafíos que se presentan respecto a las comunicaciones no deseadas, está vinculado al marketing digital, puesto que muchas de las empresas que realizan este tipo de actividades han adoptado nuevas tecnologías para masificar sus actividades de promoción comercial. Así, el uso masivo de tecnologías automatizadas ha generado que a nivel global las comunicaciones no deseadas sean un problema público.

Estas prácticas, además de afectar la tranquilidad y privacidad de los usuarios, generan saturación de redes, pérdidas de productividad y desconfianza en los servicios de telecomunicaciones. En esa línea, algunos países han optado por implementar medidas regulatorias, tecnológicas y/o de cooperación público privada para combatir este fenómeno. Entre las principales experiencias internacionales se tienen las siguientes:

- **Canadá**

En Canadá, las llamadas y mensajes no solicitados están regulados por la Ley de Telecomunicaciones[28], la Legislación Antispam de Canadá (CASL)[29] y el Reglamento sobre Telecomunicaciones No Solicitadas (UTR)[30].

El UTR se aplica a las llamadas no solicitadas, incluyendo las llamadas de voz en vivo y las llamadas de telemercadeo automatizadas a números de teléfono. En su artículo 2 se exige que quienes realizan llamadas de telemercadeo obtengan el consentimiento expreso de los consumidores antes de realizar cualquier tipo de telemercadeo o solicitud a través de llamadas.

[28] Ley de Telecomunicaciones Canadá: https://laws-lois.justice.gc.ca/eng/acts/t-3.4/
[29] Ley antispam Canadá: https://ised-isde.canada.ca/site/canada-anti-spam-legislation/en
[30] Reglamento sobre comunicaciones no solicitadas: https://crtc.gc.ca/eng/ce/utrpro.htm

Los mensajes automatizados están regulados por la CASL, definiendo a los mensajes electrónicos comerciales (MEC) como aquellos mensajes enviados a correos electrónicos, mensajes SMS, mensajería instantánea y otros mensajes remitidos a teléfonos y dispositivos móviles. Para el envió de mensajes se deben cumplir tres requisitos principales: (1) obtener el consentimiento, (2) proporcionar información de identificación y (3) proporcionar un mecanismo de cancelación de la suscripción. Los telemercadeos que realizan llamadas a canadienses deben identificarse con precisión a sí mismos y a sus clientes.

Respecto a medidas para combatir comunicaciones con fines ilícitos, de acuerdo a lo establecido por la Comisión Canadiense de Radio, Televisión y Telecomunicaciones (CRTC), los teleoperadores que realizan llamadas están obligados a identificarse, así como a identificar a sus clientes. En noviembre de 2018, la CRTC también exigió a los operadores y proveedores de servicios de telecomunicaciones que implementaran el bloqueo universal de llamadas a nivel de red, de la siguiente manera:

Los proveedores de servicios telefónicos que aún no ofrezcan un sistema de filtrado de llamadas opcional deben bloquear todas las llamadas con identificadores de llamadas que:

- Superen los 15 dígitos, o
- No sean marcables según el Plan de Numeración de América del Norte (por ejemplo, las llamadas del número "999-999-9999" se bloquearían antes de llegar al suscriptor).
- La opción de filtrado de llamadas que utilicen, debe ser capaz de detectar llamadas sospechosas e interceptarlas (ya sea enviándolas directamente al buzón de voz o solicitando a la persona que llama que introduzca una entrada en el teclado de su teléfono para comunicarse con el cliente).[31]

En abril de 2021, la CRTC ordenó a los proveedores de servicios de telecomunicaciones implementar la tecnología STIR/SHAKEN para combatir las llamadas falsas.

Con esta solución tecnológica los proveedores podrán autenticar y verificar la información de identificación de llamadas (ID) para llamadas de voz basadas en el Protocolo de Internet (IP) certificando si la identidad de la persona que llama es confiable, ello como condición para la oferta y prestación de servicios de telecomunicaciones.[32] En noviembre de 2021, el CRTC anunció la implementación de las referidas medidas[33].

- **Ecuador**

La Agencia de Regulación y Control de las Telecomunicaciones (Arcotel), publicó en febrero de 2020 la Resolución No. ARCOTEL-2020-074[34] a través del cual se implementó la política para la identificación de llamadas que se realicen en las plataformas de las empresas operadoras del Servicio Móvil Avanzado con la

[31] Ver norma: https://crtc.gc.ca/eng/phone/telemarketing/identit.htm
[32] Ver decisión Stir/shaken: https://crtc.gc.ca/eng/archive/2021/2021-123.htm
[33] Ver comunicado de prensa: https://www.canada.ca/en/radio-television-telecommunications/news/2021/11/canadians-to-benefit-from-new-caller-id-technology-to-combat-spoofed-calls.html
[34] Ver norma: https://www.arcotel.gob.ec/wp-content/uploads/downloads/2020/02/Resolucion-ARCOTEL-2020-0074.pdf

finalidad de que la población pueda decidir si recibe o no las llamadas con fines informativos, de venta directa, comercial, publicitaria o proselitista.

Las llamadas solo podrán efectuarse a quienes hayan dado su autorización previa y expresa.

Cabe mencionar que el procedimiento se aplica a todos los proveedores de servicios de telecomunicaciones y a personas físicas y jurídicas de todos los sectores y cubre llamadas provenientes de números de teléfono móviles y fijos.

La norma para la identificación de llamadas exige a las empresas operadoras del servicio móvil avanzado realizar los cambios tecnológicos necesarios para que las llamadas asociadas a los cuatro sectores priorizados (VENTA, FINANZAS, TURISMO y PROSELITISMO), puedan ser previamente identificados. Para tal efecto, se genera un número único que agrupa todos los números telefónicos de un determinado sector, según el siguiente listado:

- Bancos, Cooperativas, Tarjetas de Crédito y Seguros: Identificador "FINANZAS"
- Actividad Turística, oferta de paquetes, viajes, aerolíneas y otros similares: Identificador: "TURISMO".
- Venta de productos varios (de uso personal, comida, libros, muebles, inmuebles y otros afines): Identificador: "VENTA"
- Proselitismo: Identificador "PROSELITISMO".
- Prestadores del Servicio Móvil Avanzado: identificador por cada prestador del servicio.

- **Brasil**

La Agencia Nacional de Telecomunicaciones (Anatel), organismo regulador de telecomunicaciones en el país, ha venido adoptando acciones para combatir las comunicaciones no deseadas, al emitir cuatro medidas cautelares sucesivas (Orden de Decisión Nº 160/2022/COGE/SCO, de junio de 2022, Orden de Decisión Nº 250/2022/COGE/SCO, de octubre de 2022, Orden de Decisión Nº 103/2023/COGE/SCO, de abril de 2023 y Orden de Decisión nº 22/2024/RCTS/SRC, de abril de 2024), Anatel determinó que los proveedores de servicios de telecomunicaciones fijos (STFC) y proveedores de servicios móviles (SMP) bloquean las llamadas originadas por usuarios que configuran un uso inadecuado del servicio telefónico caracterizado por un volumen excesivo de llamadas diarias cortas.

Entre las principales medidas adoptadas para mitigar las comunicaciones no deseadas se tienen:

- Proveedores bloquean a los usuarios que realicen más de 100 mil llamadas diarias de hasta tres segundos. (Decisión Nº 160/2022/COGE/SCO)
- Proveedores bloquean temporalmente las llamadas de usuarios que generen al menos 100.000 (cien mil) llamadas en un día, considerando el número total de accesos asignados a la persona jurídica, y en las que el número total de llamadas cortas represente una proporción igual o superior al 85% del total de llamadas. (Orden de Decisión nº 250/2022/COGE/SCO)
- Mediante la Decisión No. 103/2023/COGE/SCO se prorrogó la vigencia de las medidas establecidas en la Decisión No. 250/2022/COGE/SCO.

- Otra medida introducida fue ordenar a las empresas prestadoras de servicios de telecomunicaciones la creación de la plataforma de consulta[35] , a través de la cual los ciudadanos interesados podrán consultar la identificación del titular de determinados códigos de acceso de telefonía fija (STFC) y telefonía celular (SMP), cuando este sea una persona jurídica.
- Posteriormente, la Orden de Decisión Nº 22/2024/RCTS/SRC ajustó el concepto de llamadas cortas, considerando ahora todas aquellas completadas con una duración de hasta 6 segundos (con desconexión en el origen o destino). En las tres Decisiones anteriores, el concepto se limitaba a llamadas de hasta 3 segundos, con desconexión únicamente por parte del originador.

Medidas para la identificación de llamadas:

Para evitar llamadas no deseadas a los consumidores y mejorar la relación entre estos y el sector del telemarketing, el 24 de noviembre de 2021, ANATEL publicó la Ley Nº 10.413 (Procedimiento Operativo para el Uso de Recursos de Numeración), que estableció el prefijo 0303 para el servicio de telemarketing activo. Esta medida se aplica a las llamadas de telemarketing que ofrecen productos y servicios, como líneas telefónicas fijas o teléfonos celulares. Tanto los proveedores de servicios de telecomunicaciones como los proveedores de servicios de telemarketing activos (usuarios de la red de telecomunicaciones) están sujetos a las sanciones del artículo 173 de la Ley n.º 9.472, de 16 de julio de 1997 (advertencia, multa, suspensión temporal, caducidad y declaración de incompetencia).

El 27 de septiembre de 2022, la Ley N.° 13.672[36] derogó y sustituyó a la Ley N.° 10.413, manteniendo la obligatoriedad del uso del prefijo 0303 para el ejercicio de actividades activas de telemarketing e incorporando además el uso del prefijo 0500 para identificar a las entidades sin fines de lucro. El nuevo procedimiento prohíbe el reenvío de tráfico de llamadas originadas por recursos no asignados, vacantes o en cuarentena, así como el cambio del número del usuario que origina la llamada, asimismo determinan el establecimiento, por parte de los proveedores de telecomunicaciones, de procesos de control y administración de los recursos de numeración, a fin de garantizar su uso adecuado y eficiente.

- **Inglaterra**

En Inglaterra, el Reglamento de Comunicaciones Electrónicas y Privacidad (PECR) regula las comunicaciones electrónicas y restringe el marketing no solicitado por teléfono, fax, correo electrónico, SMS u otros mensajes electrónicos.

Asimismo, existen diferentes normas para los distintos tipos de comunicación. Estas normas suelen ser más estrictas para el marketing dirigido a particulares que para el dirigido a empresas. A menudo, se requiere el consentimiento expreso para enviar marketing directo no solicitado. La mejor manera de obtener un consentimiento válido es solicitar a los clientes que marquen las casillas de aceptación. Las casillas premarcadas no otorgan una autorización válida.

[35] Ver web de consulta brasileña sobre llamadas: https://qualempresameligou.com.br/
[36] Ver norma https://informacoes.anatel.gov.br/legislacao/atos-de-numeracao/1741-ato-13672

El regulador de comunicaciones inglés Ofcom actualizó la normativa relacionada a los datos de identidad de la línea llamante (CLI)[37] y que los operadores deben cumplir, como identificar y bloquear llamadas con datos CLI que no sean válidos, que no identifiquen de forma única a la persona que llama o que no contengan un número que se pueda marcar.

- El formato de una CLI debe ser un número de 10 u 11 dígitos;
- Identificación de números que no deben usarse como CLI, la información de asignación de numeración de Ofcom y la lista de no originarios (DNO).
- Identificación y bloqueo de las llamadas con origen en el extranjero que no tengan CLI válido.
- Identificación y bloqueo de llamadas desde el extranjero falsificando la CLI del Reino Unido.
- Prohibición del uso de 09 números no geográficos como CLI.

Si una red de tránsito realiza el progreso de una llamada con una CLI no válida, faltante o sospechosa, debe reemplazar el número con uno dentro del rango 0879 asignado por Ofcom. Esto ayudará a otros en la ruta de la llamada a identificar que la llamada se originó desde orígenes potencialmente desconocidos (por ejemplo, internacional) y se utilizará para ayudar a las redes de destino a tomar decisiones de enrutamiento.

El número 0879 también ayuda a las redes a rastrear la llamada a lo largo de la ruta de la llamada hasta el origen de la llamada dentro del Reino Unido.

La red de destino debe tomar medidas razonables para evitar que las llamadas con una CLI sospechosa o mal formada lleguen a la parte llamada; esto puede incluir bloquear llamadas o enviar llamadas directamente al correo de voz.

Se espera que las redes de destino lleven a cabo comprobaciones razonables de cualquier número de presentación recibido, incluida la longitud del número insertado y el estado en comparación con el Plan Nacional de Numeración mantenido por Ofcom.

La guía actual de Ofcom reconoce que no es técnicamente factible verificar la propiedad o asignación de números individuales en esta etapa, pero verificaciones como el número de dígitos o el formato pueden ser apropiadas para que muchos proveedores satisfagan este requisito.

Bloquear o detener llamadas

Todos los proveedores de servicios y redes de tránsito que puedan bloquear, desviar o impedir el progreso de llamadas debido a CLI mal formado o sospechoso deben contar con un proceso para revisar sus decisiones y manejar disputas. Así, el proceso de disputa debe publicarse en el sitio web de los proveedores de servicios y anunciarse internamente para garantizar una acción rápida en caso de que se bloqueen inadvertidamente llamadas legítimas.

---

[37] Ver norma https://www-ofcom-org-uk.translate.goog/consultations-and-statements/category-2/improving-cli-data-accuracy?utm_medium=email&utm_campaign=New+Ofcom+rules+to+fight+fake+number+fraud&utm_content=New+Ofcom+rules+to+fight+fake+number+fraud+CID_ec84e0f22524edc394783b305f7a1255&utm_source=updates&utm_term=new+rules&_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp

- **Colombia**

La Comisión de Regulación de Comunicaciones (CRC) publicó en febrero de 2022, la Resolución 6522 de la CRC[38] por el cual se establecen nuevas obligaciones para el envió invasivo de SMS con contenido comercial y publicitario y se refuerzan las acciones para contrarrestar el fraude a través de este tipo de mensajes. Con esta resolución se obliga a incluir en todos los mensajes publicitarios el nombre, marca o razón social del PCA responsable de la provisión de contenidos y aplicaciones.

El envío de mensajes SMS o USSD, con fines comerciales o publicitarios, están autorizados siempre que el usuario haya autorizado expresamente su envío. Asimismo, solo podrán ser enviados a los usuarios entre las 8 am y 9 pm. Finalmente, cuando el usuario lo soliciten se deberá restringir el envío de mensajes no solicitados.

- **Irlanda**

En Irlanda las llamadas y los mensajes de texto automatizados están regulados por el Reglamento General de Protección de Datos de la Unión Europea y la Directiva sobre Privacidad y Comunicaciones Electrónicas[39]. Estas normas exigen que el destinatario haya dado su consentimiento expreso para recibir llamadas o mensajes de texto automatizados de marketing directo.

Los proveedores de servicios de comunicaciones electrónicas están sujetos a las condiciones establecidas por el organismo regulador de comunicaciones de Irlanda, la Comisión para la Regulación de las Comunicaciones (ComReg). Estas condiciones incluyen requisitos relacionados con la identificación de llamadas y exigen a los proveedores que tomen medidas para garantizar que el número mostrado sea el asignado a quien realiza la llamada y que pueda recibir una devolución de llamada.

Irlanda cuenta con un registro de prohibición de llamadas. Su Base de Datos del Directorio Nacional, que es una lista de números de teléfonos móviles y fijos asignados en Irlanda, permite a los clientes seleccionar si desean aparecer en la lista y si desean ser contactados por empresas de marketing directo.[40]

Irlanda además publicó un documento de consulta que propone medidas para reducir los daños y restablecer la confianza en las comunicaciones de voz[41]:

- Una lista de No Originar (“DNO”) se refiere a números de teléfono que nunca se utilizan para llamadas salientes. Por ejemplo, ciertos bancos proporcionan números para que los consumidores se comuniquen con ellos, pero nunca se comunican con un consumidor utilizando el mismo número. En consecuencia, cualquier llamada que parezca provenir de estos números es falsa y, por lo tanto, debe bloquearse automáticamente.
- Una lista de Números Protegidos (“PN”) se refiere a números de teléfono que ComReg no ha asignado a ningún operador o empresa y, por lo tanto,

[38] Ver norma https://www.crcom.gov.co/sites/default/files/normatividad/00006522.pdf
[39] Ver regulación: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058-20091219
[40] Ver registro: https://www.comreg.ie/advice-information/unsolicited-contacts-national-directory-database/
[41] Ver documento de consulta: https://www.comreg.ie/media/2023/06/ComReg-2352e.pdf

cualquier llamada que los presente es falsa y, por lo tanto, debe bloquearse.

- El bloqueo de llamadas CLI móvil identificaría y bloquearía llamadas molestas provenientes de redes internacionales que se presentan con identificadores de llamadas móviles irlandeses, a menos que la persona que llama sea genuina y se sepa que está en el extranjero. Estas llamadas intentan engañar a los clientes haciéndoles creer que la llamada proviene de alguien en Irlanda desde su teléfono móvil.
- El bloqueo de llamadas CLI fijas funciona de la misma manera que el bloqueo de llamadas CLI móviles, pero bloquea las llamadas molestas que falsifican números geográficos (p. ej., 01, 061) y/o los números no geográficos que utilizan las empresas (p. ej., 0818).

➢ **Estados Unidos**

En Estados Unidos el Congreso estadounidense aprobó la Ley para el Control del Ataque de Pornografía y Marketing No Solicitado (CAN-SPAM) y su reglamento[42] en 2003, estableciendo límites para la adopción del spam en todo el país. La ley que establece las reglas para el correo electrónico comercial, define los requisitos para mensajes comerciales, da a los destinatarios el derecho a pedir que se les deje de enviar este tipo de información y detalla fuertes sanciones por su violación.

Tanto los mensajes transaccionales como los relativos a mercadotecnia están bajo la jurisdicción de la Ley CAN-SPAM. Los correos electrónicos transaccionales sólo están obligados a transmitir información veraz, pero los correos electrónicos de carácter comercial están sujetos además a los siguientes requerimientos:

- Evitar engañar al destinatario
- Incluir una dirección postal en el cuerpo del correo electrónico
- Proveer un enlace para anular la suscripción
- Honrar las solicitudes de exclusión voluntaria en un plazo de 10 días
- Responsabilidad de los emisores y sus agencias

Por otro lado, la Communications Commission (FCC), regulador de telecomunicaciones norteamericano y la Federal Trade Commission (FTC) han implementado varias políticas para combatir las llamadas y los mensajes de texto ilícitos:

- STIR/SHAKEN[43]: Es un sistema que autentica las llamadas para combatir la suplantación de identidad (caller ID spoofing). El sistema permite verificar que las llamadas provienen realmente del número que dicen tener, ayudando a reducir las estafas telefónicas.

[42] Ver norma https://www.ftc.gov/legal-library/browse/rules/can-spam-rule
[43] Ver https://www.fcc.gov/call-authentication

- Regulaciones contra el Robo de Identidad y Estafas por SMS: A través de la Truth in Caller ID Act[44], se prohíbe la suplantación de identidad y el uso de información falsa en las llamadas. También, se ha trabajado en la promoción de aplicaciones y tecnologías que bloquean o etiquetan los mensajes sospechosos de ser estafas.

- Regulación de los SMS comerciales: A través de la Telephone Consumer Protection Act (TCPA)[45], las llamadas automáticas y los mensajes no solicitados están regulados, y las empresas deben obtener el consentimiento explícito del consumidor para enviarlos.

Desde la Ley Traced del 2019, la FCC inició un conjunto de disposiciones para disuadir y combatir las llamadas automáticas (robocallers) entre las que incluía sanciones y el desarrollo de tecnologías de autenticación de llamadas por parte de los proveedores de servicios de voz. En octubre de 2020, se ordenó a los proveedores de voz intermedios y de terminación de EE.UU. que no aceptaran llamadas utilizando números de EE.UU. directamente de proveedores de origen extranjero que no figuran en la base de datos de Mitigación de Robocalls (RMD).

Para combatir las robocallers originadas en el extranjero, la FCC colocó a los proveedores de puerta de enlace bajo el régimen anti-robocall con un nuevo conjunto de reglas en el 2022.

Las nuevas reglas exigen que:

- Los proveedores de puerta de enlace apliquen el protocolo de verificación de identificación de llamadas anti-robocall existente, conocido como STIR/SHAKEN a todas las llamadas originadas en el extranjero no autenticadas (solo tráfico IP de voz) que muestran números de identificación de llamadas (CLI) utilizando el plan de numeración de EE. UU.
- El desarrollo y envío de planes de mitigación de tráfico a la Base de Datos de Mitigación de Robocalls.
- Se responda a los esfuerzos para rastrear las llamadas automáticas ilegales hasta su origen dentro de las 24 horas.
- El bloqueo de cualquier llamada que el proveedor de puerta de enlace pueda identificar claramente como conductos para el tráfico ilegal.
- Se tomen medidas razonables y efectivas para garantizar que el proveedor de servicios de voz extranjero inmediato ascendente no esté utilizando la puerta de enlace para traer un alto volumen de tráfico ilegal a una red de EE. UU.

➢ **Chile**

Entre las principales iniciativas regulatorias adoptadas por Chile en su búsqueda de combatir las comunicaciones no deseas se tiene la Ley N° 19.496 sobre Protección de los Derechos de los Consumidores[46], que establece que los consumidores tienen el derecho de no recibir comunicaciones publicitarias no solicitadas, ya sea por llamadas telefónicas, correos electrónicos u otros medios.

[44] Ver https://www.fcc.gov/document/rules-and-regulation-implementing-truth-caller-id-act-2009
[45] Ver norma https://www.fcc.gov/sites/default/files/tcpa-rules.pdf
[46] Ver https://www.bcn.cl/leychile/navegar?idNorma=1160403&idVersion=2025-01-14&idParte=

Además, el Decreto N° 62 de 2019[47], aprobado por el Ministerio de Economía, Fomento y Turismo, establece el sistema "No Molestar" o Antispam, que permite a los consumidores inscribirse para evitar recibir comunicaciones publicitarias no deseadas.

En cuanto a las comunicaciones con fines ilícitos, Chile ha implementado la Ley N° 21.459, que tipifica delitos informáticos y establece sanciones para quienes utilicen las redes de telecomunicaciones con fines delictivos.

En febrero de 2025, la Subsecretaría de Telecomunicaciones (SUBTEL) publicó la Resolución Exenta Nº286, que modifica la Resolución Exenta N°1.319/2004, mediante el cual introduce nuevas medidas para regular las comunicaciones masivas y/o automatizadas.

El principal objetivo de esta normativa es brindar a los usuarios la capacidad de identificar de forma clara y precisa las llamadas comerciales, distinguiendo entre aquellas comunicaciones que han sido solicitadas y las que no.

Entre las principales características de esta nueva normativa se encuentra el de diferenciar entre llamadas comerciales solicitadas y no solicitadas, así como definir bloques de numeración específicos para cada servicio, introduciendo dos nuevos servicios complementarios, cada uno con un prefijo de numeración especial.

- **Australia**

En Australia, los usuarios pueden registrar sus números en el Registro de No Llamar, y las llamadas comerciales no solicitadas a números registrados están prohibidas, ello con la implementación del registro nacional de no llamar a través de la Ley del Registro de No Llamar del 2006 y su reglamentación [48].

Las normas federales australianas generales sobre telemarketing y spam se aplican a los usuarios de las redes de telecomunicaciones y abarcan las llamadas robóticas y los mensajes de texto robotizados. Esto incluye la Ley de Spam de 2003[49] y su reglamento de 2021[50] y el Estándar de la Industria de las Telecomunicaciones (Telemarketing e Investigación) de 2017[51].

Estas normas para las llamadas de telemarketing y de investigación se encuentran en un estándar industrial de obligado cumplimiento e incluyen requisitos relacionados con la identificación de la línea de llamada, la duración de las llamadas, la finalización de la llamada y el suministro de información durante la misma. Cuando las llamadas incluyen un mensaje automatizado, el receptor debe poder obtener cierta información sobre la persona que llama.

En cuanto a los mensajes de texto, la legislación antispam prohíbe el envío de mensajes electrónicos comerciales no solicitados con un enlace australiano. El consentimiento para recibir mensajes puede ser expreso o implícito. En caso de consentimiento, los mensajes deben incluir información clara y precisa sobre el remitente e incluir una función funcional para cancelar la suscripción.

[47] Ver https://www.bcn.cl/leychile/navegar?idNorma=1142343
[48] Ley Registro no llamar: https://www.legislation.gov.au/F2017L00237/asmade/2017-03-16/text/original/pdf
[49] Ver norma: https://www.legislation.gov.au/C2004A01214/2016-03-10/2016-03-10/text/original/pdf
[50] Ver reglamentación: https://www.legislation.gov.au/F2021L00285/asmade/2021-03-22/text/original/pdf
[51] Ver: https://www.legislation.gov.au/F2017L00323/asmade/2017-03-28/text/original/pdf

Asimismo, se aprobó un código de la industria de las telecomunicaciones para la reducción de llamadas y mensajes de texto fraudulentos[52], desarrollado por la industria de las telecomunicaciones, aborda el problema de las estafas mediante llamadas telefónicas y mensajes de texto cortos (SMS). El código "establece procesos para identificar, rastrear, bloquear e interrumpir llamadas y SMS fraudulentos", su cumplimiento es voluntario, a menos que la Autoridad Australiana de Medios y Comunicaciones (ACMA) lo exija.

Según el código, los operadores y proveedores de servicios de transporte deben hacer todo lo posible para identificar, rastrear, bloquear e interrumpir dichas llamadas y mensajes. Abarca las llamadas y los mensajes de texto originados tanto en Australia como a nivel internacional, e incluye normas y procesos para combatir la suplantación de identidad y el uso indebido de identificadores alfanuméricos de remitente.

El gobierno australiano realizó recientemente una consulta sobre un Marco de Código contra Estafas[53] que propone nuevos códigos obligatorios para el sector privado, incluidas las empresas de telecomunicaciones. El gobierno también está implementando un proyecto piloto de un Registro de Identificadores de Remitentes de SMS destinado a proteger los encabezados alfanuméricos de los mensajes de marcas y agencias de la suplantación de identidad por parte de estafadores y evitar que los consumidores sean víctimas de estas estafas.[54]

- **España**

España es uno de los principales países de Europa en implementar medidas regulatorias para combatir comunicaciones no deseadas, especialmente las llamadas comerciales invasivas, mensajes de spam, correos electrónicos publicitarios sin consentimiento y suplantaciones de identidad (phishing y smishing). Entre las principales medidas legislativas se tienen:

Ley General de Telecomunicaciones (Ley 11/2022)55, por el cual se prohíbe expresamente las llamadas comerciales no deseadas (spam telefónico), a menos que el usuario haya dado su consentimiento previo y expreso; y cuyas principales medidas son:

- Reforzar los derechos de los usuarios frente a las comunicaciones intrusivas.
- Exigir que los operadores garanticen la identificación clara de las llamadas comerciales.
- Las personas tienen derecho a oponerse al tratamiento de sus datos con fines de marketing en cualquier momento.

Ley de protección de datos o LOPDGDD (Ley Orgánica 3/2018)[56]

- Exige el consentimiento explícito para enviar comunicaciones publicitarias electrónicas (correo, SMS, llamadas).
- El usuario tiene derecho a acceder, rectificar y borrar sus datos, así como a oponerse al uso de sus datos para fines comerciales.

[52] Ver código: https://www.commsalliance.com.au/__data/assets/pdf_file/0015/72150/C661_2022.pdf
[53] Ver https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf
[54] Ver https://www.infrastructure.gov.au/have-your-say/sms-sender-id-registry-fighting-sms-impersonation-scams
[55] Ver norma: https://www.boe.es/buscar/doc.php?id=BOE-A-2022-10757
[56] Ver norma: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673

- Sanciona a empresas que no respeten estas normas (la AEPD impone multas que pueden superar los 100.000 €).

Ley de Servicios de la Sociedad de la Información (LSSI - Ley 34/2002)[57], cuyas principales medidas son:

- Regular el envío de comunicaciones comerciales electrónicas (emails, SMS, etc.).
- Establecer que este tipo de comunicaciones solo pueden enviarse si el usuario las ha solicitado o existe una relación contractual previa.
- Las empresas deben incluir un método sencillo para darse de baja en cada mensaje.

En febrero de 2025, Ministerio para la Transformación Digital y de la Función Pública publicó la Orden TDF/149/2025[58] por el cual se establecen medidas para combatir las estafas de suplantación de identidad a través de llamadas telefónicas y mensajes de texto fraudulentos y para garantizar la identificación de la numeración utilizada para la prestación de servicios de atención al cliente y realización de llamadas comerciales no solicitadas. Entre los principales objetivos de la Orden, se tiene:

- Combatir la manipulación del identificador de línea llamante (CLI): La orden introduce mecanismos para evitar fraudes relacionados con la manipulación del CLI en llamadas y mensajes.
- Garantizar la identificación de la numeración utilizada en servicios de atención al cliente y llamadas comerciales no solicitadas: Establece medidas para asegurar que la numeración utilizada en estos servicios sea claramente identificable y esté debidamente registrada
- Bloqueo de llamadas y mensajes fraudulentos: Los operadores deben bloquear llamadas y mensajes que presenten numeración no atribuida, asignada o adjudicada, incluyendo numeración vacía, así como aquellos con origen internacional que utilicen numeración del plan nacional de numeración, salvo en casos de itinerancia internacional
- Registro de alias comerciales: Se establece la obligación de registrar los alias utilizados en servicios de mensajería (SMS/MMS/RCS) en un registro gestionado por la Comisión Nacional de los Mercados y la Competencia (CNMC).

Con estas medidas el gobierno español busca reforzar la protección de los usuarios frente a fraudes y mejorar la transparencia en las comunicaciones comerciales.

5.3. Medidas consideradas para la solución del problema público

Al respecto, en el Proyecto de Norma se han considerado medidas para enfrentar la problemática de las llamadas y mensajes de texto con fines ilícitos, las cuales serán aplicables para los operadores, comprendiendo a las personas naturales o jurídicas que poseen un título habilitante o registro para prestar el servicio público de telefonía fija o móvil; así como, el registro de valor añadido para prestar el servicio de almacenamiento y retransmisión de datos, lo que también alcanza a los operadores móviles virtuales (OMV).

[57] Ver norma: https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
[58] Ver norma: https://www.boe.es/buscar/doc.php?id=BOE-A-2025-2870

a) Información a abonados y usuarios sobre llamadas y mensajes de texto ilícitos

Sobre el particular, en el Proyecto de Norma se ha contemplado la obligación de los operadores que cuentan con una página web de internet, incorporar en su página principal información relevante sobre los canales de atención para que los usuarios y abonados reporten ante el operador los casos de llamadas o mensaje de texto ilícitos o sospechosos de serlo, los tipos de riesgos relacionados a llamadas y mensaje de texto a los que los usuarios y abonados pueden estar expuestos, información sobre productos o servicios para ayudar a los usuarios y abonados a bloquear llamadas y mensaje de texto ilícitos o sospechosos de serlo; así como, las acciones que los usuarios y abonados pueden realizar para evitar los referidos riesgos.

Lo antes mencionado se debe a la importancia y necesidad de que los usuarios cuenten con información orientativa relevante que los ayude a reconocer situaciones vinculadas a llamadas y mensajes de texto que podrían representar un riesgo para su seguridad, las acciones que podrían adoptar frente a dicha situación; así como, los canales de atención que la empresa operadora pone a su disposición para que el usuario pueda reportar dichas situaciones.

Nótese que la falta de información antes referida, genera que el usuario se encuentre más vulnerable ante los posibles riesgos de llamadas y mensajes de texto con fines ilícitos, lo cual contribuye a que estos hechos queden impunes y continúen produciéndose, ocasionando cada vez mayor perjuicio a la población.

Por otro lado, la medida prevé que la operadora incorpore en su página principal un enlace visiblemente notorio que direccione a la información antes mencionada, dado que se requiere que pueda ser fácilmente advertible por los usuarios, de tal forma que se cumpla con la finalidad de mantenerlos informados y prevenidos ante tales situaciones.

b) Medidas sobre llamadas ilícitas

- **Características que podrían presentar las llamadas ilícitas**

Diversas organizaciones, tales como, UIT, ETSI, FCC, GSMA y otras, han desarrollado distintas recomendaciones relacionadas a la gestión de tráfico fraudulento, prevención de suplantación de llamadas, el formato que debe seguir un número telefónico internacional, entre otros. Todas estas recomendaciones están orientadas a prevenir llamadas ilícitas, las mismas que podrían contar con ciertas características que se han incorporado al Proyecto de Norma de forma referencial, a efectos de que las empresas operadoras las tomen en cuenta para sus labores de monitoreo e investigación.

En relación al alto volumen de tráfico proveniente de un Identificador de número A particular o un rango particular y llamadas de corta duración o que se cortan a los pocos segundos sin que se haya iniciado la comunicación verbal, se tiene que, patrones anómalos de tráfico pueden

indicar intentos de fraude (como "Wangiri fraud[59]" o llamadas masivas para generar ingresos ilícitos). El tráfico masivo desde un mismo origen es característico de sistemas automáticos (robocalls[60]) o campañas de fraude telefónico, como también las llamadas de muy corta duración o llamada perdida para que el usuario devuelva la llamada a un número de tarificación especial ("Wangiri fraud").

Asimismo, las buenas prácticas de señalización (como, por ejemplo, protocolos empleados en SS7 o SIP) requieren que el número A esté correctamente configurado. Es decir, ocultar o enviar en blanco este número, así como que el número A sea idéntico al número B, puede indicar enmascaramiento malicioso, el cual es una práctica asociada a fraudes.

Además, la recomendación UIT-T E.164 define el formato internacional estándar de los números telefónicos. Un número que no cumple con este formato podría ser falso o inválido, y se considera sospechoso. Esta recomendación establece el plan internacional de numeración para las telecomunicaciones públicas, definiendo la estructura y funcionalidad de los números utilizados en las telecomunicaciones internacionales. El incumplimiento de este estándar puede indicar números falsificados o inválidos, utilizados comúnmente en actividades fraudulentas.

La Recomendación UIT-T E.164 también aborda la asignación de códigos de país y la estructura de los números de teléfono, permitiendo identificar rangos de numeración no asignados o reservados. El uso de números provenientes de estos rangos puede ser una señal de manipulación del identificador de llamadas con fines fraudulentos.

En el Perú, el uso de rangos no asignados, reservados o de emergencia (como el 911, 909, entre otros) indica manipulación del identificador de llamada, puesto que estos números no deben ser usados, como número A, para comunicación alguna. La validación de estos números con la base de datos de numeración del MTC[61] permite verificar su legitimidad.

Por otro lado, la retroalimentación de usuarios es clave para alimentar listas negras o sistemas de reputación de números. Este criterio se considera una forma de detección colaborativa de amenazas. Los usuarios pueden "coadyudar" en la detección de, por ejemplo, números que intenten obtener información o que presenten enmascaramiento, ambas acciones suele involucrar técnicas de *spoofing* para ocultar la verdadera identidad del originador. El reporte del usuario complementa los sistemas de detección, sean manuales o automáticos, u otros que el operador considere.

En ese sentido, en el Proyecto de Norma se han considerado las siguientes características que podrían indicar que una llamada es fraudulenta:

a) Alto volumen de tráfico proveniente de un Identificador de número A particular o un rango particular.

[59] https://www.europol.europa.eu/sites/default/files/documents/wangiri_final_2.pdf
[60] https://www.fcc.gov/consumers/guides/stop-unwanted-robocalls-and-texts
[61] https://www.gob.pe/institucion/mtc/colecciones/227-directorio-de-numeracion-dgppc

b) Llamadas de corta duración o que se cortan a los pocos segundos sin que se haya iniciado la comunicación verbal.
c) Identificador de número A en blanco o que se muestra como oculto.
d) Identificador de número A es igual al identificador del número B.
e) Identificador de número A no cumple con las recomendaciones de la UIT-T E.164.
f) El identificador de número A pertenece a rangos de numeración no asignados por el MTC o reservados para otros usos como los rangos 911 y 909, 90820, 90821, 99820, 99821, entre otros, que establezca el MTC.
g) Reporte de un abonado indicando que las llamadas de un determinado Identificador de número A buscan obtener información para realizar fraude, o este ya ha sido ejecutado.
h) Reporte de un abonado o usuario hacia su operador indicando que ha detectado que el Identificador de número A se encuentra enmascarado.
i) Otras que el operador considere relevante.

Las características indicadas no son taxativas y/o definitivas para considerar que una llamada es ilícita, por lo que el operador, en base a su experiencia y análisis, puede contemplar otras que resulten pertinentes.

- **Medidas de investigación sobre llamadas ilícitas**

La Recomendación UIT-T M.3362 describe los requisitos para la gestión antifraude en redes de telecomunicaciones, incluyendo la detección, monitoreo y mitigación del fraude, así como la gestión de información relacionada con fraude. Además, aborda escenarios de fraude como llamadas molestosas y llamadas con suplantación de identidad (*spoofing*). Esta recomendación enfatiza la importancia de compartir información sobre fraudes detectados, lo que respalda la relevancia de los reportes de abonados para identificar y prevenir actividades fraudulentas.

El enmascaramiento del identificador de llamadas (spoofing), es una técnica común en fraudes telefónicos. La GSMA, a través de iniciativas como Call Check, ofrece servicios para que los operadores verifiquen la probabilidad de que una llamada sea fraudulenta o que el identificador de llamadas haya sido falsificado. Estas herramientas permiten a los operadores detectar y mitigar llamadas con identificadores enmascarados, basándose en información reportada por los usuarios y análisis técnicos.

Si bien la especificación ETSI TS 102 232-5 se centra en la interceptación legal en servicios de voz sobre IP, proporciona ciertas directrices sobre cómo los operadores o autoridades competentes pueden monitorear y analizar el tráfico de VoIP para detectar actividades sospechosas o fraudulentas.

Ambas especificaciones ofrecen un marco técnico para que los operadores y proveedores de servicios implementen medidas efectivas contra el fraude en redes de telecomunicaciones, incluyendo la identificación de patrones de tráfico inusuales u otras cuando sea necesario.

En esa línea, se busca que los operadores, a fin de realizar un apropiado tratamiento e investigación sobre la posible existencia de llamadas ilícitas o llamadas sospechosas en sus redes, realicen las acciones de investigación detalladas en el artículo 7 del Proyecto de Norma.

Así, las acciones de investigación que realizan los operadores se gatillan a partir de situaciones que la propia empresa haya advertido a partir del monitoreo de sus redes o a partir de los reportes generados por sus usuarios. Producto de ello, la empresa debe realizar las investigaciones correspondientes, considerando si el número A se encuentra enmascarado o no, así como si la llamada fue origina en su propia red o si proviene de la interconexión con otro operador. Así para cada caso se plantean las acciones de investigación que deben realizar los operadores.

Lo antes mencionado, permitirá conocer la fuente de la llamada y, dependiendo de las casuísticas, adoptar las medidas para lograr el cese de tales comunicaciones.

En esa línea, una de las medidas consideradas es la recepción de reportes de los abonados o usuarios, considerando que los usuarios representan una fuente crítica para detectar amenazas que podrían no ser detectadas automáticamente por los operadores. De este modo, tener canales de reporte permite activar investigaciones para identificar el origen de las comunicaciones ilícitas.

Por parte de la operadora, el monitoreo constante de su red permite detectar patrones anómalos, tal como alto volumen de tráfico proveniente de un Identificador de número A particular o un rango particular, llamadas de corta duración o que se cortan a los pocos segundos sin que se haya iniciado la comunicación verbal, identificador de número A en blanco o que se muestra como oculto. Como se ha indicado anteriormente, esta actividad está alineada con normas como UIT-T X.805 y buenas prácticas GSMA. Además, para realizar una correcta investigación se considera la solicitud de evidencias adicionales de soporte.

En caso el operador detecte alguna conducta ilícita o sospechosa realizada por un usuario suyo, debe iniciar el procedimiento de uso indebido del servicio, normado por el OSIPTEL[62,] siendo que este procedimiento permite a los operadores actuar frente a conductas irregulares de sus abonados y constituye una herramienta para prevenir el uso fraudulento de la red.

Sin perjuicio de ello, dado el continuo avance tecnológico, se considera necesario que el OSIPTEL actualice el procedimiento de uso indebido del servicio, a efectos de que se aborde con mayor eficacia las nuevas casuísticas de llamadas y mensajes de texto con fines ilícitos que se han incrementado en los últimos años.

Se ha considerado, además, la participación de la Policía Nacional del Perú (PNP) para comunicar casos que podrían constituir delitos, a fin de investigar posibles estafas u otros ilícitos.

[62] Resolución N° 172-2022-CD/OSIPTEL.

En escenarios de interconexión, también es necesario alertar al operador desde cuya red se originó la llamada para que tome acciones correctivas. Se requiere trazabilidad (fecha, hora, PDI, identificador del número A, cantidad de llamadas ilícitas en un periodo determinado, entre otras evidencias) para respaldar la investigación.

En esa misma línea, se considera que en caso el circuito se origine en un operador LDI, el operador que se interconecta con este debe usar todos los mecanismos legales y contractuales para el cese de las llamadas ilícitas.

Finalmente, se debe brindar respuesta al usuario, lo cual refuerza la confianza en el sistema y cierra el ciclo del incidente reportado.

- **Acciones para cautelar la veracidad del identificador de número A**

En este punto se toma como referencia las características que podrían presentar las llamadas ilícitas, descritas en el artículo 6 del Proyecto de Norma, para establecer las acciones respectivas, que deben adoptar los operadores, a fin de cautelar la veracidad del identificador de número A.

En todos los casos se pone énfasis en prevenir el enmascaramiento ilícito del número A, ya que se entiende que un esquema de fraude muy común parte de este tipo de prácticas, sobre todo en el ámbito de llamadas internacionales.

En ese sentido, la finalidad es detectar este tipo de tráfico y evitar que la llamada se establezca o concrete.

- **Medidas tecnológicas para permitir a los abonados y usuarios advertir sobre posibles llamadas ilícitas**

Sobre el particular, se plantea que el operador añada el prefijo 00 al Identificador de número A de todas las llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes que no cuenten con este prefijo.

Una técnica común en fraudes telefónicos consiste en manipular el número A para que una llamada internacional aparezca como local, generando confianza en el usuario. Esta práctica se utiliza en fraudes como:

- Suplantación de bancos o instituciones públicas.
- Estafas de ingeniería social.
- Llamadas tipo “Wangiri”.

En ese sentido, el uso del prefijo "00" en llamadas internacionales para la presentación del número A busca advertir al usuario sobre el verdadero origen de la llamada y le permite detectar de manera más clara que la llamada proviene del extranjero, aun si el número fue manipulado y aparenta ser uno nacional, mitigando prácticas de fraude como las mencionadas anteriormente.

Asimismo, esta medida técnica concuerda con distintas recomendaciones internacionales[63] que promueven la transparencia del identificador de llamadas (Número A).

Por lo tanto, agregar el prefijo "00" a todas las llamadas internacionales tiene un valor preventivo y orientativo, puesto que ayuda al usuario a identificar llamadas potencialmente sospechosas, protege contra suplantación de identidad y fortalece la confianza en el servicio de telecomunicaciones.

Otra medida tecnológica considerada es que el operador con más de 500 000 líneas debe contar con plataformas tecnológicas que garanticen el bloqueo de las llamadas que presenten las características contenidas en los literales a, b, c, d, e y f del numeral 6.1 del Proyecto de Norma.

Cabe resaltar que las medidas contempladas en el Proyecto de Norma, se han definido como aplicables a los operadores que gestionan más de 500 000 líneas, sean estas fijas o móviles. Esta delimitación no solo responde a criterios de escala operativa y capacidad económica para asumir los costos asociados a la implementación de las medidas, sino también a que dichos operadores concentran el mayor volumen de tráfico de comunicaciones, tanto en llamadas como en mensajes de texto, lo que los posiciona como actores clave en la prevención y mitigación de las comunicaciones con fines ilícitos. Es en ese sentido que, focalizar las obligaciones en este segmento permite maximizar el impacto de la normativa sin generar cargas desproporcionadas para operadores de menor tamaño.

Estas plataformas tecnológicas deben monitorear activamente el tráfico de red y, dependiendo de las reglas configuradas en ella, bloquear llamadas ilícitas. Dichas reglas o técnicas de filtrado analizan varias características de las llamadas tales como: el número A o patrones inusuales de datos de señalización o volumen de llamada para determinar si esta es legítima o no.

La implementación, por parte de las empresas operadoras, de este tipo de plataformas tecnológicas para llamadas ha sido abordada y recomendada por algunos estándares internacionales[64]. Estos mecanismos son esenciales para prevenir fraudes y proteger a los usuarios de amenazas como llamadas y mensajes falsificados, phishing, smishing y suplantación de identidad.

Las plataformas tecnológicas de voz monitorean y filtran el tráfico de llamadas en tiempo real. Detectan patrones asociados a:

- Spoofing (suplantación del número A).
- Wangiri (llamadas de corta duración).
- Manipulación del número A.

[63] UIT-T E.164 y E.156: establecen que las llamadas internacionales deben ser claramente identificables mediante un prefijo estándar.
UIT-T Q.731.3: destaca la importancia de la presentación correcta del número llamante y la necesidad de evitar su manipulación.

[64] GSMA FS.11: recomienda el uso de plataformas tecnológicas para prevenir fraude por SMS y llamadas.
UIT-T M.3362: establece un marco para la gestión antifraude que incluye monitoreo de voz y mensajes en tiempo real.
UIT-T X.805: define la necesidad de implementar puntos de control y medidas de seguridad a lo largo de las capas de red, incluyendo plataformas tecnológicas de filtrado para comunicaciones de extremo a extremo.

- Tráfico desde rangos no asignados o mal formateados.

De este modo, las medidas antes mencionadas permiten aplicar reglas automáticas de bloqueo según origen, duración, volumen o comportamiento sospechoso.

5.3.1. Medidas sobre mensajes de texto ilícitos

- **Características que podrían presentar los mensajes de texto ilícitos**

Las características que podrían presentar los mensajes de texto ilícitos están alineadas con las buenas prácticas internacionales y recomendaciones de organizaciones como la GSMA, ETSI y la UIT-T.

Así, una gran cantidad de mensajes de texto dirigidos a múltiples Números B se identifica como un comportamiento típico de spam desde dispositivos personales (P2P) no autorizados para servicios A2P. Este comportamiento viola prácticas estándar de uso de canales P2P, lo cual es indicativo de actividad automatizada no autorizada. Cabe mencionar que esta característica no se considera aplicable a los mensajes de texto A2P puesto que estos normalmente son mensajes masivos.

Por su parte, la ausencia del identificador del remitente (número A) impide la trazabilidad del mensaje, lo cual representa una vulnerabilidad de seguridad. Esta condición puede ser utilizada maliciosamente para ocultar la identidad del emisor y evadir mecanismos de filtrado. Las buenas prácticas de la industria, incluyendo recomendaciones de la UIT[65], establecen que debe existir siempre un número de origen válido y verificable.

Asimismo, cuando un mensaje de texto presenta la característica de que el número A es igual al número B se da una condición técnicamente anómala, ya que no corresponde a un patrón de comunicación habitual entre usuarios. Su uso es común en escenarios de spoofing, donde se intenta simular que el mensaje proviene del propio dispositivo del usuario. Este tipo de tráfico suele utilizarse para evadir sistemas de detección automática de spam o fraude.

Además, se tiene los casos en que el mensaje de texto ingresa a través de un Punto de Interconexión (PDI) con otro operador, pero el número A pertenece a la red propia del operador que recibe el mensaje. Este comportamiento indica una posible suplantación del origen del mensaje, ya que un número perteneciente a una red no debería originar tráfico legítimo a través de infraestructuras ajenas. Este patrón puede revelar el uso de plataformas externas no autorizadas para enviar mensajes con identidad falsificada.

Otro supuesto se presenta cuando se identifican mensajes de texto salientes con un identificador de origen que coincide con numeración reservada para servicios especiales. En estos casos, se debe tener en consideración que los prefijos mencionados están reservados por el MTC para servicios públicos esenciales, de emergencia o suplementarios. En

[65] UIT-T Q.731.3.

ese sentido, el uso de estos prefijos como identificadores de origen está prohibido para tráfico de mensajería regular, y constituye una vulneración a la normativa de numeración nacional. Así, suplantar estos números puede inducir a error al usuario y facilitar fraudes como el phishing o estafas de soporte técnico.

De otro lado, si el contenido del mensaje de texto alienta al destinatario a ingresar a URL maliciosos, se puede estar ante una técnica de smishing en la que el mensaje incluye enlaces a sitios de phishing o malware[66].

De igual modo, si el contenido del mensaje de texto alienta a realizar una llamada al remitente, puede tratarse de un intento de fraude combinado que emplea mensajes de texto para inducir llamadas con fines fraudulentos, como ingeniería social o llamadas a números premium.

Otro ejemplo de phishing o smishing, se da cuando el contenido del mensaje de texto solicita información personal o bancaria del abonado. En este caso, el objetivo es engañar al usuario para revelar datos sensibles.

También se tienen casos de suplantación de identidad, a través del uso no autorizado de remitentes alfanuméricos (enmascaramiento del identificador de número A)[67] tomando la identidad de entidades legítimas, como bancos o instituciones públicas[68].

Las características descritas corresponden a patrones anómalos y potencialmente maliciosos, frecuentemente asociados a mensajes de texto de origen fraudulento, siendo que estas consideraciones tienen amplio respaldo técnico en recomendaciones de la GSMA, ETSI y UIT. La detección temprana de estos patrones, combinada con el uso de plataformas tecnológicas para el análisis y filtrado de este tipo de tráfico, así como la educación del usuario es fundamental para la protección de los usuarios e integridad de la red, constituyendo una estrategia robusta de mitigación del fraude en redes móviles.

- **Medidas de investigación sobre mensajes de texto ilícitos o sospechosos**

En el Proyecto de Norma se han considerado distintas medidas, las cuales se basan en principios de seguridad, trazabilidad, responsabilidad operativa y cooperación institucional.

Una de las medidas consideradas es la recepción de reportes de los abonados o usuarios, considerando que los usuarios representan una fuente crítica para detectar amenazas que podrían no ser detectadas automáticamente por los operadores. De este modo, tener canales de reporte permite activar investigaciones para identificar el origen de las comunicaciones ilícitas.

---

66 UIT-T X.1205 aborda amenazas como el phishing como parte del entorno de ciberseguridad.

67 Prácticas abordadas en UIT-T X.1252 (framework de identidad confiable).

68 En ciertos países se han implementado los “SMS Sender ID protection registries” que permiten a las organizaciones registrar y proteger las cabeceras de los mensajes empleadas en las comunicaciones con sus clientes o usuarios, limitando el impacto del SMS phishing y spoofing

Por parte de la operadora, el monitoreo constante de su red permite detectar patrones anómalos, como altos volúmenes de mensajes de texto o uso de remitentes irregulares. Como se ha indicado anteriormente, esta actividad está alineada con normas como UIT-T X.805 y buenas prácticas GSMA. Además, para realizar una correcta investigación se considera la solicitud de evidencias adicionales de soporte.

En caso el operador detecte alguna conducta ilícita o sospechosa realizada por un usuario suyo, debe iniciar el procedimiento de uso indebido del servicio, normado por el OSIPTEL, siendo que este procedimiento permite a los operadores actuar frente a conductas irregulares de sus abonados y constituye una herramienta para prevenir el uso fraudulento de la red.

Se ha considerado, además, la participación de la PNP para comunicar casos que podrían constituir delitos, a fin de investigar posibles estafas u otros ilícitos.

En escenarios de interconexión, también es necesario alertar al operador desde cuya red se originó el mensaje para que tome acciones correctivas. Se requiere trazabilidad (fecha, hora, PDI, tipo de mensaje, entre otras evidencias) para respaldar la investigación.

En esa misma línea, se considera que los operadores deben exigir, por contrato, a sus agregadores, como intermediarios técnicos, que estos identifiquen y controlen el uso fraudulento de su plataforma. A nivel internacional se promueve este tipo de acuerdos para prevenir abusos del servicio.

Finalmente, se debe brindar respuesta al usuario, lo cual refuerza la confianza en el sistema y cierra el ciclo del incidente reportado.

- **Acciones para cautelar la veracidad del remitente alfanumérico**

Para el envío de un mensaje de texto con remitente alfanumérico, el operador o agregador nivel 1 que envía el mensaje de texto solicita y obtiene la autorización del operador receptor inmediato para que este le permita cursar y reconocer el remitente alfanumérico del mensaje de texto dentro de su red.

Para tal efecto, el operador o agregador nivel 1 remite al operador receptor inmediato los documentos que acrediten fehacientemente el acuerdo que tiene con su cliente para el uso del remitente alfanumérico. Dicho acuerdo debe evidenciar de forma indubitable que el cliente se encuentra facultado a usar el remitente alfanumérico, no pudiendo usar como remitente alfanumérico nombres, razón o denominación social, nombres comerciales, siglas, acrónimos, entre otros, que no correspondan al cliente.

El receptor de la solicitud indicada en el numeral precedente, emite respuesta en un plazo máximo de cinco (05) días hábiles.

El operador receptor de un mensaje de texto valida y autoriza el remitente alfanumérico del mensaje de texto previamente al progreso de este en su red.

- **Acciones para cautelar la veracidad del identificador de número A en mensajes de texto**

En línea con lo expuesto en el presente documento relacionado a las características que presentan los posibles mensajes de texto fraudulentos, los operadores cumplen con realizar las acciones que se señalan en las siguientes líneas.

El operador en cuya red se originan los mensajes de texto, evita el progreso de estos cuando no haya verificado la autenticidad del Identificador de número A, evitando el enmascaramiento.

El operador no envía mensajes de texto con Identificador de número A en blanco, vacío u oculto.

El operador receptor del mensaje de texto no permite el progreso de estos cuando el número A es igual al número B.

Cuando un mensaje de texto proviene de un PDI con otro operador, el operador receptor evita el progreso del mensaje de texto cuando identifique que el número A pertenece a su red.

- **Medidas tecnológicas para el bloqueo de mensajes de texto ilícitos**

Las plataformas tecnológicas de mensajes de texto monitorean activamente el tráfico de red y, dependiendo de las reglas configuradas en ella, bloquean los mensajes de texto identificados como ilícitos. Dichas reglas o técnicas de filtrado analizan diversas características de los mensajes para determinar si este es legítimo o no.

La implementación, por parte de las empresas operadoras, de este tipo de plataformas tecnológicas para mensajes de texto ha sido abordada y recomendada por algunos estándares internacionales[69]. Estos mecanismos son esenciales para prevenir fraudes, la defensa de las redes móviles y protección del usuario de amenazas como mensajes falsificados, phishing, smishing y suplantación de identidad.

Tanto los fraudes por voz y mensajes de texto afectan la seguridad del usuario, la confianza en el servicio y la integridad de las telecomunicaciones. La implementación de estas plataformas tecnológicas permite a los operadores cumplir con obligaciones de protección al consumidor y ciberseguridad, siendo una práctica estándar en mercados regulados y recomendada como requisito por organismos técnicos y autoridades regulatorias.

- **Obligaciones sobre reporte de información**

Otra medida que se plantea en el Proyecto de Norma es la obligación por parte de los operadores de remitir información, a fin de tener estadísticas

[69] GSMA FS.11: recomienda el uso de plataformas tecnológicas para prevenir fraude por SMS y llamadas.
UIT-T M.3362: establece un marco para la gestión antifraude que incluye monitoreo de voz y mensajes en tiempo real.
UIT-T X.805: define la necesidad de implementar puntos de control y medidas de seguridad a lo largo de las capas de red, incluyendo plataformas tecnológicas de filtrado para comunicaciones de extremo a extremo.

de las llamadas y mensajes analizados y bloqueados, así como de su respectiva categorización y/o motivo de bloqueo; además de realizar un correcto seguimiento y fiscalización de las medidas planteadas en el proyecto de norma, Así, se plantea que los operadores envíen los reportes correspondientes, el último día hábil de cada mes, a la DGFSC, con copia a la DGPRC, respecto al mes inmediato anterior al envío de la misma.

c) Identificación del remitente de las llamadas originadas por proveedores de bienes y servicios

Al respecto, en el Proyecto de Norma se ha considerado conveniente establecer disposiciones para la identificación del remitente de las llamadas realizadas para promover productos y servicios, así como prestar el servicio de telemercadeo, con el fin de tener trazabilidad, garantizar la transparencia y confianza de los usuarios frente a las llamadas comerciales.

A propósito de lo anterior, se debe tener en cuenta que con fecha 9 de mayo de 2025, se publicó en el diario oficial El Peruano, la Ley N° 32323, Ley que modifica la Ley 29571, Código de Protección y Defensa del Consumidor, a fin de ampliar la prohibición de las comunicaciones SPAM.

Así, en el artículo único de la Ley N° 32323, se modifica el párrafo 58.1 - literal e)- y se incorpora el párrafo 58.3 al artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor. En el párrafo 58.3 se estipula que para garantizar la protección del consumidor contra los métodos comerciales agresivos o engañosos, el Estado establece las reglas para el adecuado uso de envío de mensajes y llamadas en las redes de telecomunicaciones.

Asimismo, en la única disposición complementaria final se establece que para la aplicación del párrafo 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, el Poder Ejecutivo establecerá la normativa adicional que otorgue la numeración telefónica especial a los proveedores, los métodos de seguridad y las técnicas de validación para que los usuarios puedan identificar las llamadas (spam) que reciben, así como, los mecanismos de validación de la información trasmitida, en un plazo de sesenta días calendario contados a partir de la entrada en vigor de dicha ley.

En ese sentido, se ha considerado que la asignación de un identificador único (número o conjunto de números) permite una identificación inequívoca de las llamadas comerciales. Esta medida facilita el reconocimiento inmediato del remitente por parte del usuario, lo cual está alineado con prácticas internacionales de gestión de llamadas comerciales y combate el spoofing o suplantación de identidad. Adicionalmente, agrupar las llamadas comerciales bajo un número único permite simplificar la gestión del tráfico generado por *call centers* y terceros autorizados, haciéndolo de manera centralizada, y mejora la trazabilidad de las llamadas.

En esa misma línea, la coordinación entre operadores garantiza que todos los sistemas de red reconozcan e interpreten de forma homogénea los números únicos designados. Esto es fundamental para evitar errores

de enrutamiento y garantizar la consistencia/diferenciación de llamadas comerciales en toda la red nacional.

El conjunto de medidas evita el uso de números no autorizados, minimizando riesgos de fraude, extorsión, suplantación o malas prácticas comerciales, lo cual es clave para la protección del usuario y para mantener un entorno confiable en la recepción de llamadas de promoción o telemercadeo, puesto que, si bien con el avance o desarrollo de la industria de las telecomunicaciones, se ha producido un incremento en el uso de los servicios de públicos de telecomunicaciones, también se ha venido generando vulnerabilidades que afectan la seguridad y bienestar de los usuarios de los mismos

En ese sentido, en el Proyecto de Norma se plantea las medidas de identificación del remitente de las llamadas realizadas para promover productos y servicios, así como prestar el servicio de telemercadeo, respecto de los sectores definidos en dicho proyecto normativo y otros que posteriormente sean definidos.

Así, se ha estimado conveniente iniciar las medidas con el sector financiero y de seguros, puesto que es uno de los principales sectores que está expuesto a la comisión de fraudes y estafas, dada las ventajas económicas que los delincuentes pueden obtener del mismo; así como, se ha considerado al sector de servicios públicos de telecomunicaciones, toda vez que es un sector vulnerable ante la información sensible que manejan de los abonados.

Asimismo, se ha considerado necesario o pertinente que los lineamientos técnicos, operativos, de coordinación u otras condiciones necesarias para la aplicación de las disposiciones antes mencionadas sean definidos por el MTC mediante resolución ministerial y de acuerdo a las disposiciones del Plan Técnico Fundamental de Numeración, aprobado mediante Resolución Suprema Nº 022-2002-MTC o norma que la modifique o sustituya.

Por otro lado, en la segunda disposición complementaria final se faculta al MTC para que, mediante resolución ministerial, determine otros sectores o actividades económicas para la aplicación de las medidas antes mencionadas, lo cual dependerá de las necesidades específicas y la factibilidad operativa de la implementación de las medidas en cada sector en particular.

Para tal efecto, el MTC realizará las coordinaciones con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI u otra entidade pública, según corresponda.

d) Acciones de fiscalización y tipificación de infracciones

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 numeral 2 del artículo 8 de la LOF del MTC establece que, en el marco de sus competencias el MTC cumple la función específica de, cumplir y hacer cumplir el marco normativo relacionado con su ámbito de competencia, ejerciendo la potestad sancionadora correspondiente.

De acuerdo al artículo 86 del TUO de la Ley de Telecomunicaciones es responsable de la comisión de infracciones administrativas tipificadas en la referida Ley: (1) quien realiza actividades normadas por la presente Ley careciendo de la respectiva autorización o concesión; (2) quien realiza actividades en contra de lo dispuesto en la presente Ley, aun contando en la respectiva autorización o concesión; y, (3) el usuario de los servicios de telecomunicaciones por la mala utilización de los servicios, así como por el empleo de los mismos en perjuicio de terceros.

Asimismo, el numeral 9) del artículo 87 del TUO de la Ley de Telecomunicaciones establecen que, constituyen infracciones muy graves, el incumplimiento de las normas de la referida Ley, sus reglamentos y disposiciones de la autoridad, que sean tipificadas como muy graves por el reglamento.

Por su parte, los numerales 9) y 12) del artículo 88 del TUO de la Ley de Telecomunicaciones establecen que, constituyen infracciones graves, la utilización indebida de los servicios de telecomunicaciones; y, cualquier otra infracción de la normativa de telecomunicaciones tipificada como falta grave.

Los numerales 5) y 6) del artículo 258 del TUO del Reglamento de la Ley de Telecomunicaciones establecen que constituyen infracciones muy graves, la utilización de numeración sin la debida asignación por parte del órgano competente del MTC o de una distinta a la asignada; así como, la utilización de señalización o numeración en condiciones distintas a las contempladas en el respectivo plan técnico, respectivamente.

Por otro lado, de acuerdo con el artículo 88 del TUO de la Ley de Telecomunicaciones, constituye infracción grave no presentar la información solicitada y negarse a facilitar información relacionada con el servicio.

Asimismo, el artículo 116 del TUO del Reglamento de la Ley de Telecomunicaciones, establece la obligación de brindar facilidades para las inspecciones y verificaciones, entre ellas, la de proporcionar la información que el Ministerio les solicite, respecto de materias de su competencia, en la forma y plazo que este indique. Ello sin perjuicio de la obligación de presentar la información adicional que requieran para el análisis de casos específicos.

Aunado a lo anterior, el artículo 130 del TUO del Reglamento de la Ley de Telecomunicaciones, establece las diferentes obligaciones de los concesionarios de servicios públicos de telecomunicaciones, entre ellas, la de presentar al MTC la información que este le solicite.

Sumado a lo anterior, el artículo 261 del TUO del Reglamento de la Ley de Telecomunicaciones contiene los alcances de la infracción grave referida a la negativa de presentar información relacionada al servicio y la no presentación de información solicitada, tipificada en el numeral 10 del artículo 88 del TUO de la Ley de Telecomunicaciones.

Conforme a la Segunda Disposición Complementaria Final de la Ley N° 27336, Ley de Desarrollo de las Funciones y Facultades del Organismo Supervisor de Inversión Privada en Telecomunicaciones - OSIPTEL, el MTC aplicará la escala de multas contenida en el Artículo 25 de la referida Ley.

De acuerdo al artículo 25 de la Ley N° 27336, en caso de infracciones leves puede sancionarse con amonestación escrita, de acuerdo a las particularidades del caso. Asimismo, dispone que los límites máximos de las multas correspondientes serán los siguientes: la infracción leve hasta una multa de 100 UIT, la infracción grave hasta una multa de 500 UIT, y la infracción muy grave hasta una multa de 1000 UIT.

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 Dirección General de Fiscalizaciones y Sanciones en Comunicaciones (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.

En ese ámbito, se tiene el Reglamento de Fiscalización y Sanción en la prestación de servicios y actividades de comunicaciones de competencia del MTC aprobado por Decreto Supremo N° 028-2019-MTC que tiene por objeto, regular el ejercicio de las funciones de fiscalización y de sanción atribuidas al MTC de acuerdo a las normas que rigen la prestación de los servicios de comunicaciones y actividades conexas de su competencia, así como el dictado de medidas correctivas y cautelares, con el propósito

de que los administrados bajo su ámbito cumplan con el marco normativo y contractual en materia de comunicaciones a nivel nacional, acorde a su artículo 1.

Atendiendo a dicha potestad, facultades y funciones, en el Capítulo VII del presente proyecto normativo se dispone las acciones de fiscalización y tipificación de infracciones siendo que, en el artículo 16 se establece que la DGFSC tiene a su cargo la supervisión y fiscalización del cumplimiento de lo establecido en la referida norma, en el marco de sus competencias.

Asimismo, el artículo 17 de este proyecto normativo contempla que las infracciones en las que incurra el operador son sancionadas de acuerdo a lo dispuesto por la Ley y el Reglamento.

Dado el marco legal glosado, se ha determinado plantear una Primera Disposición Complementaria Modificatoria que modifique el TUO del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo Nº 020-2007-MTC, incorporando el numeral 27 al artículo 258, para adicionar las conductas sancionables.

Así pues, el artículo 258 incorpora como infracciones muy graves, el incumplimiento de las obligaciones contenidas en (i) el artículo 5 referidas a la información a abonados y usuarios sobre llamadas y mensajes de texto ilícitos; (ii) el artículo 7 referido a la investigación sobre llamadas ilícitas; (iii) los numerales 8.1 y 8.2 del artículo 8, correspondientes a las acciones para cautelar la veracidad del identificador de número A; (iv) los numerales 9.1 y 9.2 del artículo 9, concernientes a las medidas tecnológicas para permitir a los abonados y usuarios advertir sobre posibles llamadas ilícitas; (v) el artículo 11, referido a la investigación sobre mensajes de texto ilícitos; (vi) los numerales 12.1, 12.2 y 12.3 del artículo 12, referidos a las acciones para cautelar la veracidad del remitente alfanumérico; (vii) el artículo 13 que atañe a las acciones para cautelar la veracidad del identificador de número A en mensajes de texto; y, (viii) el artículo 14, referido a las medidas tecnológicas para el bloqueo de mensajes de texto ilícitos, (ix) el numeral 16.1 del artículo 16 concerniente a la identificación del remitente de las llamadas originadas por proveedores de bienes y servicios. Dichas conductas han sido calificadas como infracciones muy graves debido a la relevancia de las obligaciones cuyo cumplimiento se busca asegurar puesto que tienen incidencia directa en la prevención y la lucha contra las llamadas y mensajes de texto con fines ilícitos para contrarrestar o mitigar la inseguridad ciudadana garantizando el buen uso de los servicios públicos de telecomunicaciones, en salvaguarda de la integridad y bienestar de la población.

De otro lado, el incumplimiento por parte de la empresa operadora de la obligación de remisión de alguno o de todos los reportes establecidos en el artículo 15 del Proyecto de Norma constituye una infracción grave, dado que se subsume en el literal a) del numeral 4 del artículo 261 del TUO del Reglamento de la Ley de Telecomunicaciones, según el cual se considera como negativa a facilitar información relacionada con el servicio, a que se refiere el numeral 10 del TUO de la Ley de Telecomunicaciones, no presentar al Ministerio la información prevista en la normativa dentro del plazo fijado.

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

a) Análisis de necesidad de la norma

La necesidad del Proyecto de Norma se sustenta en que mediante su aprobación se contribuirá con la seguridad nacional en el ámbito del orden interno, orden público y seguridad ciudadana, evitando que se establezcan comunicaciones ilegales a través de llamadas y mensajes de texto, 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.

Asimismo, las medidas que se plantean están orientadas a que, a través de configuraciones y habilitaciones técnicas en las redes de telecomunicaciones, de mecanismos de investigación, de coordinación, verificación y de implementación de plataformas tecnológicas, se logre evitar que los usuarios reciban llamadas y mensajes de texto con fines ilícitos; así como, que cuenten con herramientas para reconocer las llamadas comerciales de proveedores que efectivamente son quienes dicen ser, diferenciándolos de aquellos que toman el nombre de proveedores, a efectos de cometer actos ilícitos.

Adicionalmente, la necesidad del Proyecto de Norma, en lo referido a la numeración para identificación del remitente de las llamadas originadas por proveedores de bienes y servicios, se sustenta en que es preciso emitir la normativa adicional para la aplicación del párrafo 58.3 del artículo 58 de la Ley 29571, Código de Protección y Defensa del Consumidor, según lo dispuesto en la única disposición complementaria final de la Ley N° 32323.

b) Análisis de viabilidad de la norma

El Proyecto de Norma resulta viable, toda vez que 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, el PTFN, 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 por las empresas operadoras, además de ser las más eficientes dada la situación actual de la problemática relacionada a las comunicaciones ilegales mediante llamadas y mensajes de texto, los costos que les corresponde asumir a los actores involucrados y los diferentes factores que influyen en dicha problemática.

De otro lado, el Proyecto de Norma, en lo referido a la numeración para identificación del remitente de las llamadas originadas por proveedores de bienes y servicios, es viable toda vez que su elaboración se realiza en el marco de dispuesto en la única disposición complementaria final de la Ley N° 32323, en el ámbito de las competencias y funciones del MTC, toda vez que implica la identificación de las llamadas (spam).

En ese sentido, resulta viable que se emita el Proyecto de Norma.

c) Análisis de oportunidad de la norma

La emisión del Proyecto de Norma se considera oportuna puesto que, debido a que la problemática de las comunicaciones ilegales mediante llamadas y mensajes de texto 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 Proyecto de Norma que precisamente contiene disposiciones dirigidas a enfrentar la mencionada problemática.

Asimismo, se estima oportuno la emisión del Proyecto de Norma en consideración a lo establecido en la única disposición complementaria final de la Ley N° 32323, respecto a la emisión de la normativa adicional, toda vez que se ha otorgado un plazo de sesenta (60) días calendario contados a partir de la entrada en vigor de la referida ley, tomando en cuenta lo señalado en la viabilidad de la norma.

VI. Propuesta normativa

Del Capítulo I: Disposiciones Generales

El **artículo 1** del Proyecto de Norma, contiene el objeto que es establecer las medidas preventivas y reactivas contra las llamadas y mensajes de texto con fines ilícitos, y las disposiciones sobre el uso de la numeración para la identificación del remitente de las llamadas realizadas para promover productos y servicios, así como prestar el servicio de telemercadeo.

El **artículo 2** del Proyecto de Norma, dispone la finalidad reducir la problemática vinculada a la realización de llamadas y envío de mensajes de texto ilícitos y los efectos negativos que generan en la sociedad; así como, generar fiabilidad y seguridad en las comunicaciones mediante la identificación del remitente de las llamadas realizadas para promover tanto productos como servicios y prestar el servicio de telemercadeo.

El **artículo 3** del Proyecto de Norma, establece el ámbito de aplicación, el cual se circunscribe a los operadores, a los operadores LDI peruanos, a los agregadores nivel 1, a las empresas del sistema financiero, sistema de seguros, empresas de telecomunicaciones u otras de los sectores o actividades económicas determinadas por el MTC.

El **artículo 4** del Proyecto de Norma, comprende los términos y definiciones para efectos de la aplicación de la norma.

Del Capítulo II: Información a abonados y usuarios

El **artículo 5** del Proyecto de Norma, contempla la información a abonados y usuarios sobre las llamadas y mensajes de texto con fines ilícitos, disponiendo que, el operador que cuente con una página web de internet debe incorporar en su página principal o portal web principal un enlace visiblemente notorio que direccione hacia la siguiente información: (1) Los canales de atención para que los usuarios y abonados reporten ante el operador los casos de llamadas o mensajes de texto ilícitos o sospechosos de serlo; (2) Los tipos de riesgos relacionados a llamadas y mensajes de texto a los que los usuarios y abonados pueden estar expuestos; (3) Información sobre productos o servicios para ayudar

a los usuarios y abonados a bloquear llamadas ilícitas y mensajes de texto ilícitos o sospechosos de serlo; y, (4) Las acciones que los usuarios y abonados pueden realizar para evitar los mencionados riesgos, tales como: (a) Proteger información personal y datos sensibles, tales como, nombre, DNI, dirección, fecha de nacimiento, números o códigos de tarjetas de débito o crédito, así como, evitar compartirlos con desconocidos, a través de llamadas, mensajes de texto y/o correo electrónico; (b) Contactar a su institución financiera de inmediato si el usuario o abonado considera o presume que ha sufrido algún perjuicio a causa de una llamada o mensaje de texto ilícito; (c) Cambiar con regularidad las contraseñas o PIN de sus SIM card y teléfono móvil; así como, colocar valores distintos a los utilizados usualmente o por defecto; (d) Ser cuidadoso con llamadas o mensajes de texto de origen internacional, con identificador de número A extraño o distinto al usado en el ámbito nacional; (e) No ingresar a URL contenidos en mensajes de texto recibidos de números A desconocidos; (f) No devolver llamadas a números desconocidos o sospechosos; y, (g) Otros que consideren relevantes.

Del Capítulo III: Llamadas ilícitas

En este capítulo se establecen las disposiciones y los mecanismos técnicos para evitar las llamadas que, pueden ser consideradas o catalogadas como ilícitas, lo que comprende lo siguiente:

Características que pueden presentar las llamadas ilícitas:

El **artículo 6** del proyecto normativo, establece que el operador debe considerar las siguientes características que pueden presentar las llamadas ilícitas o sospechosas: (a) Alto volumen de tráfico proveniente de un Identificador de número A particular o un rango particular; (b) Llamadas de corta duración o que se cortan a los pocos segundos sin que se haya iniciado la comunicación verbal; (c) Identificador de número A en blanco o que se muestra como oculto; (d) Identificador de número A es igual al identificador del número B; (e) Identificador de número A no cumple con las recomendaciones de la UIT-T E.164; (f) El identificador de número A pertenece a rangos de numeración no asignados por el MTC o reservados para otros usos como los rangos 911 y 909, 90820, 90821, 99820, 99821, entre otros, que establezca el MTC; (g) Reporte de un abonado indicando que las llamadas de un determinado Identificador de número A buscan obtener información para realizar actividades ilícitas, o estas ya han sido ejecutadas; (h) Reporte de un abonado o usuario hacia su operador indicando que ha detectado que el Identificador de número A se encuentra enmascarado e (i) Otras que el operador considere relevante.

Asimismo, se dispone que las características indicadas anteriormente, no son taxativas y/o definitivas para considerar que una llamada es ilícita, por lo que el operador, en base a su experiencia y análisis, puede contemplar otras que resulten pertinentes.

Medidas de investigación sobre llamadas ilícitas:

El **artículo 7** del proyecto normativo, dispone medidas de indagación; así como, medidas reactivas, contemplando que el operador para realizar un apropiado tratamiento e investigación sobre la posible existencia de llamadas ilícitas o llamadas sospechosas en sus redes, debe realizar las siguientes acciones:

(1) Monitorear constantemente sus redes con la finalidad de detectar llamadas ilícitas o sospechosas terminadas, en tránsito y/u originadas en sus redes.

(2) Recibir reportes de sus abonados y usuarios respecto a llamadas sospechosas o llamadas ilícitas. Para ello, el operador debe disponer de canales de atención que permitan a los abonados y usuarios realizar dichos reportes. Asimismo, el operador debe brindar respuesta a los reportes presentados por sus abonados y usuarios, en base a los resultados de sus investigaciones.

(3) Una vez recibido el(los) reporte(s) antes mencionado(s) o advertida alguna situación anormal o irregular a partir del monitoreo de sus redes, realiza una investigación del origen de las llamadas sospechosas o llamadas ilícitas dentro del plazo de quince (15) días hábiles, a fin de adoptar las acciones correctivas, en la casuística siguiente: (a) Si se detecta que hubo enmascaramiento ilícito; (b) Si se detecta que no hubo enmascaramiento (se contempla el procedimiento de uso indebido); (c) Si un operador determina que una llamada ilícita o sospechosa (enmascarada o no) fue originada desde otro operador, el operador receptor comunica mediante un reporte (con la debida información) tal hecho al operador de origen para que este realice la investigación y rastreo correspondiente; (d) El operador que recibe el reporte referido anteriormente, brinda respuesta al operador que remitió dicho reporte; (e) Las acciones estipuladas en el literal (c) se ejecutan por todos los operadores involucrados en el circuito de las llamadas ilícitas o sospechosas hasta llegar al operador LDI, en lo correspondiente; y, (f) En el caso que el circuito se origine en un operador LDI, el operador que se interconecta con este debe usar todos los mecanismos legales y contractuales para el cese de las llamadas ilícitas.

    En cada casuística se han estimado los plazos correspondientes, para que se adopten las acciones correctivas.

(4) El operador que recibió el reporte indicado en el numeral (1) brinda respuesta al abonado o usuario dentro del plazo de cinco (05) días hábiles desde que haya culminado las acciones indicadas en el numeral (3), en cada caso en particular.

Medidas preventivas para evitar el progreso o bloquear llamadas con fines ilícitos:

El **artículo 8** del Proyecto de Norma, dispone acciones para cautelar la veracidad del identificador de número A, según lo siguiente:

(1) Para llamadas originadas en el ámbito nacional: (a) El operador en cuya red se originan llamadas evita el progreso de estas cuando no haya verificado la autenticidad del Identificador de número A, es decir, evita el enmascaramiento ilícito; (b) El operador no envía llamadas con Identificador de número A en blanco a operadores LDI; (c) El operador receptor de la llamada no permite el progreso de estas cuando el número A es igual al número B; (d) Cuando una llamada proviene de un PDI con otro operador, el operador receptor evita el progreso de la llamada cuando identifique que el número A pertenece a su red; (e) El operador no envía llamadas con Identificador de número A que no cumplan con lo establecido en la recomendación UIT-T E.164; (f) El operador no permite el progreso de llamadas originadas en su red, en las que el Identificador del número A coincida con prefijos reservados para servicios especiales o suplementarios, tales como el 911, 909, 90820, 90821, 99820, 99821, entre otros que establezca el MTC; (g) El operador receptor de la llamada no permite el progreso de estas cuando el identificador de número A pertenece a rangos de numeración no

asignados por el MTC; y, (h) El operador LDI peruano no modifica el Identificador de número A para llamadas dirigidas al extranjero.

(2) Para llamadas originadas internacionalmente: (a) El operador LDI peruano no modifica el identificador de número A para llamadas dirigidas a destinatarios peruanos; (b) El operador no permite el progreso de llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes y que tengan un Identificador de número A vacío u oculto; (c) El operador no permite el progreso de llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes y que tengan un Identificador de número A que sea igual al identificador de número B; (d) Si el operador recibe una llamada proveniente del PDI con su interfaz de llamadas internacionales entrantes que tengan un Identificador de número A con formato de número nacional, verifica si el número A corresponde a un roamer activo. En caso corresponda a uno de sus roamer activo, permite el progreso de la llamada. En caso no corresponda a un roamer activo, el operador bloquea el progreso de la llamada; (e) El operador no permite el progreso de llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes y que tengan un Identificador de número A con formato de número fijo nacional; (f) El operador no permite el progreso de llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes y que tengan un Identificador de número A incorrecto según recomendación UIT-T E.164; y, (g) El operador no permite el progreso de llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes y que tengan un Identificador de número A con prefijos reservados tales como 911, 909, 90820, 99820, 99821.

El **artículo 9** del Proyecto de Norma, establece **las medidas tecnológicas** para permitir a los abonados y usuarios advertir sobre posibles llamadas ilícitas, según lo siguiente: (1) El operador añade el prefijo 00 al Identificador de número A de todas las llamadas provenientes del PDI con su interfaz de llamadas internacionales entrantes que no cuenten con este prefijo; y, (2) El operador con más de 500 000 líneas debe contar con plataformas tecnológicas que garanticen el bloqueo de las llamadas que presenten las características contenidas en los literales (a) al (f) dispuestos en el artículo 6.

Estas plataformas tecnológicas deben monitorear activamente el tráfico de red y, dependiendo de las reglas configuradas en ella, bloquear llamadas ilícitas. Dichas reglas o técnicas de filtrado analizan varias características de las llamadas tales como: el número A o patrones inusuales de datos de señalización o volumen de llamada para determinar si esta es legítima o no.

Del Capítulo IV: Mensajes de texto Ilícitos

En este capítulo se establecen las disposiciones y los mecanismos técnicos para evitar los mensajes de texto que, podrían ser consideradas o catalogadas como ilícitas, lo que comprende lo siguiente:

Características que pueden presentar los mensajes de texto ilícitos:

El **artículo 10** del Proyecto de Norma, establece que el operador y agregador nivel 1 consideran las siguientes características que podrían presentar los mensajes de textos ilícitos o sospechosos: (a) Una gran cantidad de mensajes de texto (no mensajes de texto A2P) dirigidos a una gran cantidad de Números B; (b) Mensajes de texto con Identificador de número A en blanco; (c) Mensajes de texto con identificador de número A igual al número B; (d) Mensajes de texto proviene de un PDI con otro operador cuando el número A pertenece a su red; (e) Mensajes de

texto originadas en su red en las que el Identificador del número A coincida con prefijos reservados para servicios especiales o suplementarios, tales como el 911, 909, 90820, 90821, 99820, 99821, entre otros que establezca el MTC; (f) Mensaje de texto conteniendo URL; (g) Contenido del mensaje de texto alentando al destinatario que realice una llamada al remitente para continuar la comunicación; (h) Contenido del mensaje de texto que busca obtener información personal y/o bancaria del Abonado; (i) Enmascaramiento ilícito del Identificador de número A por un remitente alfanumérico a nombre de entidades conocidas como bancos, instituciones de gobierno o tiendas por departamento; y, (j) Entre otras que el operador considere relevantes.

Asimismo, se dispone que las características indicadas anteriormente, no son taxativas y/o definitivas para determinar a los mensajes de texto ilícitos, por lo que el operador, en base a su experiencia y análisis, puede contemplar otras que resulten pertinentes.

Medidas de investigación sobre los mensajes de texto ilícitos o sospechosos:

El **artículo 11** del proyecto normativo, dispone medidas de indagación; así como, medidas reactivas, contemplando que el operador para realizar un apropiado tratamiento e investigación sobre la posible existencia de un mensaje de texto ilícito o sospechoso en sus redes, debe realizar las siguientes acciones:

(1) El operador monitorea constantemente sus redes con la finalidad de detectar mensajes de texto ilícitos o sospechosos terminados, en tránsito y/u originados en sus redes.
(2) Recibir reportes de sus abonados y usuarios respecto a mensajes de textos ilícitos o sospechosos. Para ello, el operador debe disponer de canales de atención que permitan a los abonados y usuarios realizar dichos reportes. Asimismo, el operador debe brindar respuesta a los reportes presentados por los abonados y usuarios, en base a los resultados de sus investigaciones.
(3) Una vez recibido el(los) reporte(s) antes mencionado(s) o advertida alguna situación anormal o irregular a partir del monitoreo de sus redes, el operador, en el primer supuesto, solicita al abonado o usuario que presentó dicho reporte, y en el segundo supuesto recaba por sí mismo, las evidencias del mensaje de texto ilícito o sospechoso, tal como capturas de pantalla del referido mensaje de texto, a fin de investigar dentro del plazo de quince (15) días hábiles, entre otros, los links que se encuentran dentro de su contenido, conforme con lo siguiente: (a) El operador sigue el procedimiento de uso indebido del servicio, asimismo, pone en copia al MTC en las comunicaciones que curse en el marco de dicho procedimiento; (b) Culminada su investigación, el operador pone en conocimiento de la PNP, con copia al MTC, sobre los números A, o abonados A detectados como trasgresores producto de la investigación realizada; (c) Si el operador determina que un mensaje de texto ilícito o sospechoso (enmascarado o no) fue originada desde otro operador, el operador receptor comunica mediante un reporte (con la debida información) tal hecho al operador de origen para que este realice la investigación correspondiente; (d) El operador que recibe el reporte referido anteriormente, brinda respuesta al operador que remitió dicho reporte; (e) Las acciones estipuladas en el literal (c) se ejecutan por todos los operadores involucrados en el circuito de los mensajes de texto ilícitas o sospechosas hasta llegar al operador de origen del mensaje de texto ilícito o sospechoso, el cual realiza la investigación del remitente que

lo originó y adopta las medidas necesarias para garantizar que estos mensajes no se vuelvan a cursar; y, (f) Si el mensaje de texto ilícito o sospechoso, enmascarado o no, provino de un agregador de nivel 1, el operador que se conecta con este debe usar todos los mecanismos legales y contractuales para el cese de los mensajes ilícitos. Asimismo, el agregador de nivel 1 realiza la investigación sobre el origen del mensaje de texto ilícito y adopta las medidas necesarias para garantizar que dicho tipo mensajes no se vuelvan a cursar.

(4) El operador que recibió el reporte indicado en el numeral (1) brinda respuesta al abonado o usuario dentro del plazo de cinco (05) días hábiles desde que haya culminado las acciones indicadas en el numeral (3), en cada caso en particular.

Medidas preventivas para evitar el progreso o bloquear mensajes de texto con fines ilícitos:

El **artículo 12** del Proyecto de Norma, dispone acciones para cautelar la veracidad del remitente alfanumérico, según lo siguiente:

(1) Para el envío de un mensaje de texto con remitente alfanumérico, el operador o agregador nivel 1 que envía el mensaje de texto solicita y obtiene la autorización del operador receptor inmediato para que este le permita cursar y reconocer el remitente alfanumérico del mensaje de texto dentro de su red.

Para tal efecto, el operador o agregador nivel 1 remite al operador receptor inmediato los documentos que acrediten fehacientemente el acuerdo que tiene con su cliente para el uso del remitente alfanumérico. Dicho acuerdo debe evidenciar de forma indubitable que el cliente se encuentra facultado a usar el remitente alfanumérico, no pudiendo usar como remitente alfanumérico nombres, razón o denominación social, nombres comerciales, siglas, acrónimos, entre otros, que no correspondan al cliente.

(2) El receptor de la solicitud indicada en el numeral precedente, emite respuesta en un plazo máximo de cinco (05) días hábiles.

(3) El operador receptor de un mensaje de texto valida y autoriza el remitente alfanumérico del mensaje de texto previamente al progreso de este en su red.

El **artículo 13** del Proyecto de Norma, establece las **acciones para cautelar la veracidad del identificador de número A en mensajes de texto**, disponiendo lo siguiente: (1) El operador en cuya red se originan los mensajes de texto, evita el progreso de estos cuando no haya verificado la autenticidad del Identificador de número A, evitando el enmascaramiento ilícito; (2) El operador no envía mensajes de texto con Identificador de número A en blanco, vacío u oculto; (3) El operador receptor del mensaje de texto no permite el progreso de estos cuando el número A es igual al número B; (4) Cuando un mensaje de texto proviene de un PDI con otro operador, el operador receptor evita el progreso del mensaje de texto cuando identifique que el número A pertenece a su red; y, (5) El operador no permite el progreso de mensajes de texto en los que el Identificador del número A coincide con numeración o prefijos reservados para servicios especiales o suplementarios, tales como el 911, 909, 90820, 90821, 99820, 99821, entre otros que establezca el MTC.

El **artículo 14** del proyecto normativo, establece las **medidas tecnológicas** para el bloqueo de mensajes de texto ilícitos, pues el operador con más de 500 000 líneas debe contar con plataformas tecnológicas que garanticen el bloqueo de los siguientes mensajes de texto, debiendo salvaguardar la inviolabilidad y el secreto de las telecomunicaciones, así como la protección de datos personales, para lo cual el operador implementa las medidas que fueran necesarias: (a) Mensaje de texto que contengan URL; (b) Mensaje de texto con contenido identificado como ilícito; (3) Mensaje de texto provenientes de SIM boxes usando para ello plataformas tecnológicas; (4) Mensaje de texto con remitente alfanumérico no autorizado; y, (5) Mensaje de texto con las características establecidas en los literales b), c), d), e), f) y g) del numeral 10.1 del artículo 10.

Del Capítulo V: Reporte de información

El **artículo 15** del proyecto normativo, para reforzar las medidas de fiscalización, dispone las obligaciones sobre reporte de información siguientes:

(1) El operador remite a la DGFSC con copia a la DGPRC, el último día hábil de cada mes, la siguiente información correspondiente al mes inmediato anterior:

   (a) Reporte según el Anexo I, en formato CSV de llamadas investigadas y confirmadas como ilícitas, incluyendo la siguiente información: Número A, Número B, fecha y hora de llamada, duración de llamadas, identificador de PDI de entrada y salida, código(s) de Puntos de Señalización Nacional (NSPC) y/o Internacional (ISPC) de entrada y salida, etiqueta de enmascaramiento ilícito, circuito de la llamada, indicativo de red para el servicio móvil (MNC), tipo de industria a donde la llamada ilícita está orientada, descripción de la metodología usada para la ingeniería social y tipo de acto ilícito.

   (b) Reporte según el Anexo II, en formato CSV, correspondiente a llamadas que coinciden con las características indicadas en los literales b), c), d), f) y g) del numeral 8.2, del artículo 8 de la presente norma, incluyendo la siguiente información: Número A, Número B, duración de llamada, fecha y hora de llamada, Identificador de PDI de entrada, código(s) de Puntos de Señalización Nacional (NSPC) y/o Internacional (ISPC) de entrada y salida y casuística sospechosa.

(2) El operador remite a la DGFSC con copia a la DGPRC, el último día hábil de cada mes, la siguiente información, correspondiente al mes inmediato anterior:

   (a) Reporte según el Anexo III, en formato CSV de mensajes de texto investigados y confirmados como ilícitos, incluyendo la siguiente información: Número A, Número B, Fecha y hora de mensaje, enlace, indicativo de red para el servicio móvil (MNC), identificador de PDI de entrada, código(s) de Puntos de Señalización Nacional (NSPC) y/o Internacional (ISPC) de entrada y salida, agregador (concentrador): ID Nombre, etiqueta de enmascaramiento ilícito, circuito del mensaje, tipo de industria, detalles de ingeniería social y tipo de acto ilícito.

   (b) Reporte según el Anexo IV, en formato CSV de mensaje de texto bloqueados que coinciden con las características indicadas en los numerales 14.1, 14.2, 14.3, 14.4 y 14.5 del artículo 14, incluyendo la

siguiente información: Número A, Número B, origen, identificador de PDI de entrada, código(s) de Puntos de Señalización Nacional (NSPC) y/o Internacional (ISPC) de entrada y salida, agregador (concentrador): ID y Nombre y casuística sospechosa.

Del Capítulo VI: Numeración para identificación del remitente de las llamadas originadas por proveedores de bienes y servicios

El **artículo 16** del proyecto normativo, establece la identificación del remitente de las llamadas originadas por proveedores de bienes y servicios, lo que comprende la identificación del remitente de las llamadas realizadas para promover productos y servicios, así como prestar el servicio de telemercadeo, el Operador y las empresas de los sectores definidos por el MTC, cumplen las siguientes disposiciones:

(1) En esta oportunidad, se considera de suma importancia y relevancia determinar para el sistema financiero, el sistema de seguros y las empresas de telecomunicaciones, lo siguiente:

(a) El operador en coordinación con las empresas del sistema financiero, sistema de seguros y empresas de telecomunicaciones, designan un identificador único por empresa o grupo de empresas, de modo tal que solo a través del mismo, las mencionadas empresas puedan realizar llamadas para promover productos y/o servicios, así como prestar el servicio de telemercadeo, a fin de que los consumidores o usuarios puedan identificar plenamente dichas llamadas.
(b) Para el cumplimiento de la obligación antes mencionada, las empresas del sistema financiero, sistema de seguros y empresas de telecomunicaciones, definen un número único que agrupe a todos los números provenientes de sus centros de llamada (*call center*) o de personas naturales o jurídicas que comercialicen sus bienes o servicios.
(c) Las empresas del sistema financiero, sistema de seguros y empresas de telecomunicaciones comunican al(los) operador(es) que le(s) brinda(n) los servicios de telefonía fija y/o móvil, con copia al MTC, el número único designado según el literal precedente.
(d) El operador que reciba la comunicación antes mencionada de sus abonados, remite a los demás operadores el listado de los números designados por las empresas del sistema financiero, sistema de seguros y empresas de telecomunicaciones, a fin de que realicen la configuración y habilitación correspondiente en sus redes.
(e) Las empresas del sistema financiero, sistema de seguros y empresas de telecomunicaciones no pueden realizar llamadas para promover productos y/o servicios, así como tampoco prestar el servicio de telemercadeo, desde números que no hayan sido previamente identificados según lo dispuesto en los literales precedentes.

(2) Los lineamientos técnicos, operativos, de coordinación u otras condiciones necesarias para la aplicación de las disposiciones establecidas en el numeral (1) son definidos por el MTC mediante resolución ministerial y de acuerdo a las disposiciones del Plan Técnico Fundamental de Numeración, aprobado mediante Resolución Suprema Nº 022-2002-MTCo norma que la modifique o sustituya.

Del Capítulo VII: Acciones de fiscalización y tipificación de infracciones

Los **artículos 17 y 18** del proyecto normativo, comprenden con relación a la **supervisión y fiscalización** que la DGFSC tiene a su cargo la supervisión y fiscalización del cumplimiento de lo establecido en la presente norma, en el marco de sus competencias, para lo cual rige lo establecido en la Ley y su Reglamento; así como, el Reglamento de Fiscalización Sanción y el TUO de la LPAG, y con relación a las **infracciones y sanciones** se dispone que, las infracciones en las que incurra el operador son sancionadas de acuerdo a lo dispuesto por la Ley y el Reglamento (Ley y Reglamento de la Ley de Telecomunicaciones).

Disposiciones Complementarias Finales

De la Primera Disposición Complementaria Final:

Se dispone la adecuación al cumplimiento del presente marco normativo, en un plazo no mayor de noventa (90) días calendario desde la entrada en vigencia del mismo, para que las empresas operadoras y las entidades públicas, dentro de su ámbito de aplicación, se adecúen al cumplimiento de las obligaciones y disposiciones establecidas.

De la Segunda Disposición Complementaria Final:

Se considera pertinente y necesario disponer que el MTC se encuentre facultado para la actualización y/o modificación del presente marco normativo para la lucha contra las llamadas y los mensajes de texto con fines ilícitos, para su optimización. En ese ámbito, se dispone que el MTC mediante resolución ministerial, determine otros sectores o actividades económicas para la aplicación de lo referido en el numeral (1) contenido en el artículo 16 de la propuesta normativa.

En esa misma línea, mediante resolución ministerial, se faculta que el MTC apruebe acciones adicionales en el artículo 8 para cautelar la veracidad del identificador de número A; así como, acciones adicionales en el artículo 13 para cautelar la veracidad del identificador de número A en mensajes de texto.

Disposiciones Complementarias Modificatorias:

La **Primera Disposición Complementaria Modificatoria** del proyecto normativo, establece la modificación del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo Nº 020-2007-MTC, lo que se ha detallado en el literal e) del numeral 5.3 de la presente Exposición de Motivos.

La **Segunda Disposición Complementaria Modificatoria** del proyecto normativo, modifica el Plan Técnico Fundamental de Numeración, aprobado mediante Resolución Suprema Nº 022-2002-MTC, incorporando los numerales 2.16, 2.17, 2.18, 2.19, 2.20, 2.21 y 3.13, dado las disposiciones que se implementaran con el presente marco normativo, según lo siguiente:

*"**2. DEFINICIONES***
Para efectos de la interpretación del presente Plan Técnico Fundamental de Numeración, se adoptan las siguientes definiciones:
(…)
2.16 Llamante: abonado que inicia una llamada o remite un mensaje de texto en un sistema de telefonía móvil o fija.

2.17 Remitente: abonado o usuario que inicia y remite un mensaje de texto en un sistema de telefonía móvil o en un sistema informático.

2.18 Destinatario(s): abonado hacia donde se dirige una llamada o mensaje de texto en un sistema de telefonía móvil o fija.

2.19 Número A: número de abonado asignado al llamante o remitente, generado por el operador donde este abonado se encuentra registrado o ha adquirido su servicio

2.20 Identificador de número A: la cadena numérica o alfanumérica que aparece en la pantalla del destinatario al momento de recibir una llamada o mensaje de texto. El Identificador de número A debe coincidir con el Número A.

2.21 Remitente Alfanumérico: Cuando en el contexto de un mensaje de texto enviado el identificador de número A es una cadena alfanumérica, por ejemplo el nombre de una empresa u organización. El protocolo de mensaje de texto soporta que se pueda colocar una cadena alfanumérica como remitente, aunque esto impide que estos mensajes puedan responderse.

Los operadores solo deben dar progreso a mensaje de texto con remitente alfanumérico siempre que este haya sido previamente validado y autorizado por ellos (el que cursa el mensaje). El operador o entidad que envía un mensaje de texto con remitente alfanumérico es responsable de obtener la autorización por escrito por parte del operador receptor inmediato de dicho mensaje de texto.

3. ESTRUCTURAS DE NUMERACIÓN

(…)

3.13 Para todas las llamadas entrantes desde el exterior del territorio peruano y cuyo destino es un número nacional en territorio peruano, se deberá anteponer el prefijo 00 para el número A, siempre que no cuenten con este prefijo".

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; además, 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.

Teniendo en cuenta, la creciente proliferación de llamadas y mensajes de texto con fines ilícitos (fraudes, extorsiones, vishing, smishing, entre otros) representa un problema de seguridad pública que afecta a millones de usuarios en el país, comprometiendo la confianza en los servicios de telecomunicaciones.

Asimismo, el aumento de la conectividad con mayores usuarios de internet y el uso masivo de redes sociales y otras plataformas han incrementado amenazas a la seguridad y la privacidad de individuos y empresas.

Por lo tanto, para responder de forma efectiva, en esta sección se aborda la identificación de las ventajas y desventajas de cada alternativa de solución, seguida de un análisis detallado de los costos y beneficios asociados; además, concluye con un análisis multicriterio que nos permite seleccionar con mayor efectividad la alternativa más adecuada, no solo en términos de efectividad, sino también de su impacto económico, viabilidad técnica e institucional, y sostenibilidad a largo plazo.

Alternativa 1: Statu quo

Esta opción consiste en mantener la situación actual sin implementar medidas adicionales específicas. La respuesta frente a comunicaciones ilícitas dependería únicamente de los mecanismos ya existentes, como, por ejemplo, denuncias espontáneas de usuarios, procesos judiciales u operativos policiales no coordinados con operadores.

Esta alternativa presenta las siguientes ventajas y desventajas:

	Estado	**Operadores de telecomunicaciones**	**Población**
Ventajas	• No genera gastos adicionales en los procesos de fiscalización y supervisión y sanción	• Se evitan obligaciones de inversiones en mecanismos de control, trazabilidad y monitoreo de tráfico malicioso. • Se evitan costos de adaptación regulatoria.	• No se identifican beneficios para la población.
Desventajas	• Mayor carga para el sistema judicial y policial por denuncias de fraude, extorsión, entre otros. • Incremento de los costos sociales por la limitada capacidad para prevenir delitos. • Incremento de problemas de seguridad pública.	• Mayor vulneración de sus redes. • Pérdida de la confianza en las comunicaciones por parte de sus usuarios. • Incremento en la atención de reclamos.	• Incremento de fraudes, estafas, extorsiones como otros delitos. • Pérdida de confianza en las comunicaciones móviles. • Mayor número de víctimas vulnerables y pérdidas económicas.

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

<u>Para el Estado</u>

Beneficios:

- No requiere nuevas asignaciones presupuestarias inmediatas como gastos adicionales en los procesos de fiscalización, supervisión y sanción, lo que genera un ahorro para el Estado.

Costos:

- Incrementos en el tipo de actividad fraudulenta como smishing, suplantación, extorsión, entre otros que generan perjuicio en la actividad económica del país debido a que el riesgo de implementar una inversión tiene mayor riesgo.

- Incremento progresivo en la carga del sistema judicial y policial por denuncias de fraude, extorsión, entre otros.

- Limitada capacidad para prevenir el delito, por lo que los costos sociales y administrativos aumentan.

- Se incrementan los problemas de seguridad pública como consecuencia de las comunicaciones ilícitas que atenta contra el bienestar de la población.

- Pérdida de confianza ciudadana en el Estado sobre seguridad nacional, ante la inactividad de instituciones y creación de proyectos normativos en favor de la reducción de fraudes.

- Se reduce la capacidad preventiva del sistema de telecomunicaciones, permitiendo que estructuras delictivas utilicen canales legítimos para fines ilegales.

- Se genera una externalidad negativa, en la que los operadores obtienen ingresos por ventas, pero los costos asociados como fraude, pérdidas monetarias, pérdida de confianza, entre otros, son asumidos por la población y el Estado.

- Se debilita la trazabilidad del tráfico, dificultando la investigación y sanción de delitos y fraudes.

Para las empresas operadoras

Beneficios:

- Se generan ahorros al evitar inversiones en mecanismos de control, trazabilidad y monitoreo de tráfico malicioso o irregular.

- Generación de ingresos por ventas de alto volumen a entidades no verificadas que pueden estar inmersas en actividades ilícitas.

- Evitan costos de adaptación tecnológica.

Costos:

- Exposición continua a vulneraciones de red y pérdida de reputación y confianza frente a los usuarios.

- Incremento en la atención de reclamos y costos legales asociados.

- Ausencia de un marco normativo claro incrementa la incertidumbre operativa.

Para la población

Beneficios:

- No se identifican beneficios para la población.

Costos:

- Grandes pérdidas de recursos económicos por fraudes, como consecuencia de transferencias ilícitas, robos, extorsiones generando mayores pérdidas económicas para la población.

- Incremento de costos indirectos por pérdida de confianza en el uso de los servicios de telecomunicaciones de voz y mensajería.

- Aumento en el número de víctimas vulnerables, en mayor medida de adultos mayores, personas con bajo nivel educativo o limitada alfabetización digital que serían las más susceptibles a ser víctimas de fraudes telefónicos o por mensajes de texto.

- Aumento de costos psicológicos y emocionales, como consecuencia de ansiedad, inseguridad y desconfianza al recibir llamadas o mensajes de texto desconocidos.

Alternativa 2: Implementación de STIR/SHAKEN y firewall de mensajes de texto

Esta alternativa supone adoptar soluciones tecnológicas avanzadas como el protocolo STIR/SHAKEN para verificación del número de origen en llamadas, así como un firewall de mensajes de texto para el filtrado de mensajes maliciosos. La implementación del STIR/SHAKEN se basa en la implementación de una tecnología que permite autenticar la información del identificador de llamadas, brindando mayor seguridad y confianza tanto a los usuarios como a las empresas operadoras, siendo una herramienta estratégica para fortalecer la ciberseguridad, proteger a los ciudadanos y alinearse con estándares internacionales. Sin embargo, su eficacia depende de una implantación generalizada entre todos los operadores y durante un período apropiado, por lo que su éxito depende de un despliegue eficaz en todos los países, además es caro en comparación con intervenciones alternativas[70].

Esta alternativa presenta las siguientes ventajas y desventajas:

	Estado	**Operadores de telecomunicaciones**	**Población**
Ventajas	• Fortalece la trazabilidad de las llamadas. • Reduce cargas operativas en justicia y seguridad.	• Mejora su imagen institucional ante los usuarios al prevenir fraudes, estafas, extorsiones a través de	• Limita la generación de pérdidas económicas generadas a través de fraudes, estafas,

[70] Commission for Communications Regulation. (2023). Combatting scam calls and texts. Consultation on network based interventions to reduce the harm from Nuisance Communications.

	• Mejora la situación de seguridad nacional y gobernanza digital	comunicaciones ilícitas. • Favorece la reducción de reclamos y costos de atención. • Mayor control de las llamadas cursadas por su red.	extorsiones, entre otros. • Reducción significativa de llamadas y mensajes fraudulentos. • Protección contra fraudes financieros y robo de datos personales. • Mayor confianza gradual en las comunicaciones a través de mensajes de texto y llamadas. • Beneficio limitado si solo una parte de las operadoras implementa el STIR/SHAKEN.
Desventajas	• Costos de supervisión y fiscalización de su cumplimiento. • Costos de coordinación con operadores, así como para el desarrollo del marco legal para la certificación de llamadas.	• Altos costos de inversión en la implementación y actualización de softwares y servidores. • Mayor complejidad operativa en operadores pequeños. • Problemas de incompatibilidad tecnológica en el corto y mediano para su implementación en la red móvil del Perú.	• Posibilidad de bloqueo erróneo de mensajes legítimos. • Posibles aumentos en tarifas si los costos se trasladan al usuario. • Algunos operadores y equipos compatibles verían beneficios inmediatos.

<u>Para el Estado</u>

Beneficios:

- Fortalecimiento de la trazabilidad de las llamadas, ya que permite rastrear el origen de una llamada de forma más precisa.

- Reducción de la carga operativa en justicia y seguridad, ya que permitiría disminuir los casos de extorsión, suplantación y estafas, al prevenir el spoofing de números.

- Mejora la seguridad nacional y gobernanza digital, puesto que permite al Estado demostrar liderazgo tecnológico en la protección del usuario frente a amenazas digitales.

- Reducción de estafas por mensaje de texto, puesto que se filtra tráfico fraudulento de este tipo de mensajes antes de llegar al usuario.

- Mejora de la percepción pública sobre el compromiso estatal con la ciberseguridad.

Costos:

- Costos de adecuación legal y técnica para la fiscalización, supervisión y sanción de las obligaciones de estos mecanismos.

- Costos de coordinación con operadores y desarrollo de marcos legales para la certificación de llamadas.

- Necesidad de creación de una autoridad certificadora nacional.

Para el Operador

Beneficios:

- Mejora de la imagen institucional de la operadora frente a los usuarios.

- Impulsa el uso de herramientas más sofisticadas para gestionar el fraude en sus redes.

- Fortalece la confianza en las comunicaciones entre sus usuarios.

- Favorece la reducción de reclamos y costos de atención, ya que ante un menor volumen de llamadas y mensajes fraudulentos significa menos usuarios afectados y menor carga operativa en call centers.

Costos

- Inversión elevada en software, servidores, actualizaciones de red y seguridad.

- Se generan costos de interoperabilidad internacional.

- Mayor complejidad operativa en operadores pequeños o de menor escala.

- Adaptación de sistemas legados y desarrollo de interfaces propias para integración con los protocolos.

- STIR/SHAKEN está diseñado para redes IP (VoIP), lo que generaría problemas de incompatibilidad tecnológica en el corto y mediano plazo y retrasaría su implementación en la red móvil del Perú.

- Se podrían generar costos de soporte técnico a usuarios confundidos que no entiendan por qué sus llamadas o mensaje de texto son bloqueados y que podrían recurrir a los operadores, ocasionando costos de atención al cliente y soporte.

Para la población

Beneficios:

- Limita la generación de pérdidas de recursos económicos, como consecuencia de una reducción comunicaciones ilícitas, a través de fraudes, estafas, extorsiones, entre otros.

- Disminución de costos psicológicos y emocionales, como consecuencia de ansiedad, inseguridad y desconfianza al recibir llamadas o mensajes desconocidos.

- Reducción de mensajes fraudulentos y suplantaciones de identidad, ya que, disminuye la posibilidad de recibir llamadas desde números falsos que imitan entidades legítimas.

- Mayor confianza gradual en las comunicaciones a través de mensajes de texto y llamadas, ya que saber que una llamada ha sido verificada reduce el miedo a leer o contestar mensajes o llamadas de números desconocidos.

- Menor saturación de mensajes no deseados, mejorando la experiencia del usuario al recibir solo comunicaciones legítimas.

- Al sentirse protegido, el usuario se motiva a usar servicios digitales que dependen de los mensajes de texto (como One-Time Password (OTP), notificaciones, validaciones).

- Beneficio limitado si solo una parte de las operadoras implementa el STIR/SHAKEN, puesto que, si no todas las operadoras implementan esta tecnología, los usuarios seguirán expuestos a llamadas fraudulentas desde otras redes que no han sido autenticadas, lo que reduce su efectividad.

Costos:

- Posibilidad de bloqueo erróneo de mensajes legítimos.

- Solo los usuarios de ciertos operadores y equipos compatibles verían beneficios inmediatos.

- Posibles aumentos en tarifas si los costos se trasladan al usuario

Alternativa 3: Implementación del Proyecto de Norma propuesto

Consiste en implementar el conjunto de medidas regulatorias desarrolladas en el proyecto de Decreto Supremo. Esta alternativa consiste en implementar un conjunto integral de medidas regulatorias, operativas y tecnológicas, tales como: medidas de verificación de origen de llamadas y mensajes de texto, plataformas de filtrado automatizado para operadores con más de 500 mil líneas, reglas de control de remitentes alfanuméricos, reporte obligatorio de comunicaciones ilícitas,

validación del número remitente de llamadas y mensajes, canales de denuncia ciudadana, entre otros mecanismos de trazabilidad, prevención, fiscalización y sanción.

Esta alternativa presenta las siguientes ventajas y desventajas:

	Estado	**Operadores de telecomunicaciones**	**Población**
Ventajas	• Fortalecimiento del marco normativo nacional para enfrentar las comunicaciones ilícitas. • Fortalece la trazabilidad de las llamadas. • Reduce cargas operativas en justicia y seguridad. • Mejora la situación de seguridad nacional y gobernanza digital	• Mayor seguridad en el uso de sus redes. • Fortalece el canal de mensajes de texto y llamadas como herramientas válidas para negocios serios • Mejora de la imagen institucional de la operadora frente a los usuarios. • Fortalece la confianza en las comunicaciones entre sus usuarios. • Favorece la reducción de reclamos y costos de atención ante comunicaciones ilícitas.	• Limita la generación de pérdidas económicas generadas a través de fraudes, estafas, extorsiones, entre otros. • Reducción significativa de llamadas y mensajes fraudulentos. • Protección contra fraudes financieros y robo de datos personales. • Mayor confianza gradual en las comunicaciones a través de mensajes de texto y llamadas
Desventajas	• Costos de supervisión y fiscalización de su cumplimiento.	• Costos operativos y tecnológicos, así como costos de monitoreo constante y el manejo de reportes. • Se generan costos de coordinación con otras operadoras hasta identificar el origen de la comunicación ilícita.	• Posibilidad de bloqueo erróneo de mensajes legítimos. • Posibles aumentos en tarifas si los costos se trasladan al usuario. • Costos marginales que se podrían generar al proveer evidencia de la investigación de las comunicaciones ilícitas.

Para el Estado

Beneficios:

- Fortalecimiento del marco normativo nacional al establecer reglas claras y obligaciones técnicas con respaldo legal para enfrentar las comunicaciones ilícitas.

- Mejora en la capacidad de fiscalización y supervisión, ya que se contaría con reportes sistemáticos de patrones de tráfico anómalos y podrán actuar preventivamente.

- Permite la reducción de delitos asociados a comunicaciones ilícitas, a través de la disminución de llamadas extorsivas, estafas por mensaje de texto, entre otros.

- Evita la necesidad de crear nuevas entidades técnicas, tales como una autoridad certificadora, permitiendo el aprovechamiento de instituciones ya existentes, reduciendo costos regulatorios.

- Impulsa la trazabilidad de las llamadas, permitiendo rastrear el origen de una llamada o mensaje hasta su origen.

- Reducción de la carga operativa en justicia y seguridad, ya que permitiría disminuir los casos de extorsión, suplantación y estafas, al prevenir el spoofing de números.

- Mejora la seguridad nacional y gobernanza digital, puesto que permite al Estado demostrar liderazgo tecnológico en la protección del usuario frente a amenazas digitales.

- Reducción de estafas por mensaje de texto, puesto que se filtra tráfico fraudulento de este tipo de mensajes antes de llegar al usuario.

- Mejora de la percepción pública sobre el compromiso estatal con la ciberseguridad.

Costos:

- Costos de adecuación legal y técnica para la fiscalización, supervisión y sanción de las obligaciones de estos mecanismos.

Para el Operador

Beneficios:

- Mayor seguridad en el uso de sus redes por lo que permite disminuir el uso indebido que contratan servicios con fines delictivos.

- Mejor segmentación de usuarios corporativos legítimos, lo cual fortalece el canal de mensajes de texto y llamadas como herramientas válidas para negocios serios.

- Evita inversiones masivas en infraestructura VoIP o certificación digital, ya que en este caso las medidas son progresivas, adaptables a la infraestructura existente, lo que reduce costos de implementación.

- Favorece la reducción de reclamos y costos de atención, ya que ante un menor volumen de llamadas y mensajes fraudulentos significa menos usuarios afectados y menor carga operativa en call centers.

- Mejora de la imagen institucional de la operadora frente a los usuarios.

- Fortalece la confianza en las comunicaciones entre sus usuarios.

- Favorece la reducción de reclamos y costos de atención, ya que ante un menor volumen de llamadas y mensajes fraudulentos significa menos usuarios afectados y menor carga operativa en call centers.

Costos

- Adecuación de sistemas para validar remitentes y reportar tráfico sospechoso, lo que implica adaptar plataformas existentes, pero no requiere sustitución de red ni transformación hacia VoIP.

- Implementación de sistemas de control interno, tales como remitente alfanumérico, número A, entre otros que conllevan costos de desarrollo e integración, pero son escalables y compatibles con la infraestructura actual.

- Obligación de no comercializar paquetes masivos sin verificación, lo que podrían disminuir ciertos ingresos en el corto plazo, por ejemplo, de empresas que compraban tráfico masivo sin regulación, pero se compensa con mayor confianza y uso legítimo.

- Se generan costos de coordinación con otras operadoras y entidades, ya que se incrementan los requerimientos de información y respuesta a los rastreos y bloqueos, así como la elaboración de reportes dirigidos a operadoras y entidades.

- Se podrían generar costos de soporte técnico a usuarios confundidos que no entiendan por qué sus llamadas o mensaje de texto son bloqueados y que podrían recurrir a los operadores, ocasionando costos de atención al cliente y soporte.

Para la población

Beneficios:

- Limita la generación de pérdidas económicas, como consecuencia de una reducción comunicaciones ilícitas, a través de fraudes, estafas, extorsiones, entre otros.

- Disminución de costos por daños psicológicos y emocionales, como consecuencia de ansiedad, inseguridad y desconfianza al recibir llamadas o mensajes desconocidos.

- Reducción efectiva de llamadas y mensajes ilícitos, ya que impulsa la disminución del volumen de llamadas falsas, suplantaciones y estafas por mensajes de texto.

- Mayor confianza gradual en las comunicaciones a través de mensajes de texto y llamadas.

- Permite la protección de los usuarios sin necesidad de contar con tecnología de punta. Cualquier usuario, incluso con teléfonos básicos o redes 2G/3G, se beneficia porque la trazabilidad y el control están en la red del operador.

- Menor saturación de mensajes no deseados, mejorando la experiencia del usuario al recibir solo comunicaciones legítimas.

- Al sentirse protegido, el usuario se motiva a usar servicios digitales que dependen del mensaje de texto (como One-Time Password (OTP), notificaciones, validaciones).

Costos

- Posibilidad de bloqueo erróneo de mensajes y llamadas legítimas.

- Posibles aumentos en tarifas si los costos se trasladan al usuario.

- Costos marginales que se podrían generar al proveer evidencias (capturas de información, datos y otros) para hacer efectiva la investigación de las comunicaciones ilícitas.

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 Multicriterio[71]. 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

[71] 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:

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

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.

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

Fuente: Informe N° 00110-GPRC/2020-OISPTEL

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 (Statu quo)	Alternativa 2	Alternativa 3
Efectividad	La alternativa no contempla modificaciones en las normas que impliquen acciones por parte de las empresas operadoras frente a las llamadas y mensajes de texto que puedan ser identificadas como fraudulentas. En ese sentido, en esta situación no mejora ni se deteriora los mecanismos actuales para reducir el problema sobre de las comunicaciones ilícitas.	La segunda alternativa propone la adopción de tecnologías avanzadas para combatir la problemática. STIR/SHAKEN permite autenticar el origen de las llamadas y prevenir el uso fraudulento del identificador de llamadas, mientras que el firewall de mensaje de texto implementa reglas de filtrado automático que pueden detectar y bloquear mensajes no autorizados o masivos sin consentimiento. No obstante, su efectividad puede verse limitada en países con menor adopción de VoIP o VoLTE, con redes mixtas 2G/3G aún en operación y sin interoperabilidad total entre operadores. Además, algunos usuarios con dispositivos básicos o en zonas rurales no tendrían acceso inmediato a sus beneficios. A pesar de ello, representa un salto tecnológico significativo frente al statu quo, al generar una alta mejora en la capacidad técnica de intervención. Además, se debe tener en cuenta que esta tecnología requiere de cambios	Esta alternativa representa la opción regulatoria más robusta y con mayor aplicabilidad al contexto nacional. Por lo que, a través de una combinación de medidas tecnológicas, legales y operativas, el proyecto normativo establece obligaciones claras para los operadores en materia de autenticación del identificador A, validación del remitente alfanumérico, monitoreo del tráfico, verificación de paquetes de mensajes de texto, medidas de bloqueo dirigidas y una arquitectura institucional articulada para la fiscalización. A diferencia de la Alternativa 2, esta propuesta no depende exclusivamente de tecnologías VoIP o dispositivos avanzados, lo que permite una cobertura más inclusiva para zonas rurales y usuarios con menor acceso digital. Asimismo, permite una implementación progresiva y adaptable a la infraestructura nacional, con menor riesgo de exclusión tecnológica. Por estas razones, su nivel de efectividad es igualmente alto, pero con mayor adecuación a la realidad operativa del país, consolidándose como la mejor opción desde el

		tecnológicos para su implementación; coordinación con organismos internacionales, así como actualización del marco normativo. **Puntaje: +2**	punto de vista de impacto y sostenibilidad. **Puntaje: +3**
Costo para las empresas	Esta alternativa no impone nuevas obligaciones regulatorias ni operativas para las empresas de telecomunicaciones. En este sentido, los operadores no asumirían ningún nuevo costo derivado de inversión tecnológica, adecuaciones de red, monitoreo o reportes adicionales.	La implementación del STIR/SHAKEN, representa altos costos de inversión y operación para las empresas operadoras de telecomunicaciones. Estos sistemas requieren equipos especializados capaces de autentificar si el número de origen es legítimo. 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. En ese sentido, la adecuación	La alternativa regulatoria planteada por el Proyecto de Decreto Supremo genera costos para las empresas, pero estos son más razonables y graduales en comparación con los de la Alternativa 2. El proyecto obliga a implementar medidas como el monitoreo de tráfico de red, validación del identificador A, reporte de números con tráfico masivo sospechoso y validación del remitente alfanumérico, entre otros. Si bien estas medidas exigen desarrollos tecnológicos, configuraciones en los sistemas de red y mayor coordinación interinstitucional, su complejidad técnica es menor y no requiere una transformación total del núcleo de la red.

		tecnológica tiene un alto costo de inversión, además de complejidades en su mantenimiento, certificación e integración con equipos heredados. Adicionalmente, el firewall de mensaje de texto exige desarrollar o adquirir herramientas sofisticadas de detección, análisis semántico y bloqueo de tráfico no deseado, lo cual requiere inversiones constantes en software y recursos humanos especializado 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.	Además, la norma contempla disposiciones progresivas y viables que permiten a los operadores ajustar su infraestructura sin disrupciones mayores, y su diseño se adapta mejor a las capacidades tecnológicas actuales de las empresas que operan en el Perú. Por estos motivos, la alternativa 3, representando una carga moderada pero inferior a la Alternativa 2 y más razonable en términos de costos y tiempos de implementación.
	Puntaje: 0	**Puntaje: -3**	**Puntaje: -2**
Costos regulatorios	En esta alternativa, el Estado no incurre en nuevos costos regulatorios, pues no se introducen nuevas obligaciones ni mecanismos de supervisión adicionales. Los procedimientos actuales se mantienen, y aunque eso implica que el problema público persiste, desde una perspectiva estrictamente regulatoria, no hay	La alta dependencia de cooperación internacional para su implementación, así como altos costos de coordinación, supervisión y monitoreo requiere actualización del marco normativo. La implementación de STIR/SHAKEN requiere que el Estado establezca un marco de gobernanza para la emisión y validación de certificados	El proyecto de Decreto Supremo plantea medidas regulatorias que sí requieren seguimiento por parte del Estado, pero en un marco más controlado, progresivo y menos oneroso. Las acciones incluyen verificar el cumplimiento de reportes periódicos por parte de los operadores, revisar el comportamiento de números sospechosos, auditar validaciones de

	un cambio significativo en la carga operativa del aparato estatal. **Puntaje: 0**	digitales, incluyendo posiblemente la creación o habilitación de una Autoridad Certificadora nacional, con infraestructura tecnológica, sistemas de auditoría y personal especializado. En ese sentido, los costos están asociados en la supervisión y fiscalización, ya que se necesitarán herramientas técnicas y personal para verificar el fiel cumplimiento. **Puntaje: -2**	remitentes alfanuméricos y asegurar la implementación de controles sobre el identificador de número A. Sin embargo, estas tareas pueden ser realizadas con las capacidades actuales de supervisión. Además, el enfoque propuesto es gradual, basado en coordinación y responsabilidad compartida con las empresas, lo cual reduce la necesidad de crear nuevas unidades administrativas o tecnologías regulatorias complejas. Por estas razones, esta alternativa sí genera costos, pero estos son leves y más sostenibles. **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%	0	2	3
Costos para las empresas	25%	0	-3	-2
Costos regulatorios	25%	0	-2	-1
Resultado de la evaluación		**0**	**-0.25**	**0.75**

Tras evaluar las tres alternativas propuestas para enfrentar las comunicaciones ilícitas, a través de un análisis integral que incluye un enfoque costo-beneficio y una evaluación multicriterio ponderada por criterios de efectividad, costo para las empresas y costo regulatorio, se concluye que la Alternativa 3, consistente en la implementación del proyecto normativo propuesto, es la más adecuada y costo-efectiva para abordar el problema público identificado.

Esta alternativa presenta un equilibrio óptimo entre impacto, viabilidad y sostenibilidad regulatoria. A diferencia del statu quo (Alternativa 1), que no introduce mejoras sustanciales ni costos adicionales, pero perpetúa el problema, y de la Alternativa 2, que si bien presenta alta efectividad también implica elevados costos económicos, tecnológicos y regulatorios, la Alternativa 3 logra los mismos niveles de efectividad con menores costos para las empresas y una carga regulatoria menor para el Estado.

Por tanto, la Alternativa 3 no solo representa la opción más efectiva desde el punto de vista técnico y operativo, sino también la más adecuada en términos de costo-efectividad para todos los actores involucrados: el Estado, los operadores de telecomunicaciones y la ciudadanía.

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, en el Proyecto de Norma se han incorporado obligaciones específicas y concretas para las empresas operadoras de servicios públicos de telecomunicaciones en relación con las comunicaciones ilegales mediante llamadas y mensajes de texto; así como, que se habilite un identificador único por empresa o grupo de empresas, de modo tal que solo a través del mismo, dichas empresas puedan realizar llamadas para promover productos y/o servicios, así como prestar el servicio de telemercadeo, a fin de que los consumidores o usuarios puedan identificar plenamente dichas llamadas.

Cabe resaltar que el articulado del Proyecto de Norma 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 Proyecto de Norma 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 Proyecto de Norma se ha dispuesto la incorporación del numeral 27 al artículo 258 del Texto Único Ordenado del Reglamento General de la Ley de Telecomunicaciones, aprobado por Decreto Supremo Nº 020-2007-MTC.

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

Texto vigente del TUO del Reglamento General de la Ley de Telecomunicaciones	**Propuesta de modificación del TUO del Reglamento General de la Ley de Telecomunicaciones de acuerdo con el Proyecto de Norma**
"Artículo 258.- Infracciones muy graves *Constituyen infracciones muy graves, además de las tipificadas en el artículo 87 de la Ley, las siguientes:* (…)	***"Artículo 258.- Infracciones muy graves*** *Constituyen infracciones muy graves, además de las tipificadas en el artículo 87 de la Ley, las siguientes:* (…) *27. El incumplimiento de las obligaciones contenidas en el artículo 5, en el artículo 7, en los numerales 8.1 y 8.2 del artículo 8, en los numerales 9.1 y 9.2 del artículo 9, en el artículo 11, en los numerales 12.1, 12.2 y 12.3 del artículo 12, el artículo 13, el artículo 14 y el numeral 16.1 del artículo 16 del Marco normativo para la lucha contra llamadas y mensajes de texto con fines ilícitos."*

Asimismo, se establecido la incorporación al Plan Técnico Fundamental de Numeración de los numerales 2.16, 2.17, 2.18, 2.19, 2.20, 2.21 y 3.13.

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

Texto vigente del Plan Técnico Fundamental de Numeración, aprobado mediante Resolución Suprema Nº 022-2002-MTC	**Propuesta de modificación del Plan Técnico Fundamental de Numeración, aprobado mediante Resolución Suprema Nº 022-2002-MTC**
"2. DEFINICIONES *Para efectos de la interpretación del presente Plan Técnico Fundamental de Numeración, se adoptan las siguientes definiciones:* (…)" ***3. ESTRUCTURAS DE NUMERACIÓN*** ***(…)"***	*"2. DEFINICIONES* *Para efectos de la interpretación del presente Plan Técnico Fundamental de Numeración, se adoptan las siguientes definiciones:* *(…)* *2.16 Llamante: abonado que inicia una llamada o remite un mensaje de texto en un sistema de telefonía móvil o fija.* *2.17 Remitente: abonado o usuario que inicia y remite un mensaje de texto en un sistema de telefonía móvil o en un sistema informático.* *2.18 Destinatario: abonado hacia donde se dirige una llamada o mensaje de texto en un sistema de telefonía móvil o fija.* *2.19 Número A: número de abonado asignado al llamante o remitente, generado por el*

	operador donde este abonado se encuentra registrado o ha adquirido su servicio *2.20 Identificador de número A: la cadena numérica o alfanumérica que aparece en la pantalla del destinatario al momento de recibir una llamada o mensaje de texto. El Identificador de número A debe coincidir con el Número A.* *2.21 Remitente Alfanumérico: Cuando en el contexto de un mensaje de texto enviado el identificador de número A es una cadena alfanumérica, por ejemplo el nombre de una empresa u organización. El protocolo de mensaje de texto soporta que se pueda colocar una cadena alfanumérica como remitente, aunque esto impide que estos mensajes puedan responderse.* *Los operadores solo deben dar progreso a mensajes de texto con remitente alfanumérico siempre que este haya sido previamente validado y autorizado por ellos (el que cursa el mensaje). el operador o entidad que envía un mensaje de texto con remitente alfanumérico es responsable de obtener la autorización por escrito por parte del operador receptor inmediato de dicho mensaje de texto.* ***3. ESTRUCTURAS DE NUMERACIÓN*** *(…)* *3.13 Para todas las llamadas entrantes desde el exterior del territorio peruano y cuyo destino es un número nacional en territorio peruano, se deberá anteponer el prefijo 00 para el número A, siempre que no cuenten con este prefijo".*

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, continuaba 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 Nº 063-2021-PCM.

A propósito de lo anterior, con fecha 25 de febrero de 2025, se publicó el Decreto Supremo Nº 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, Reglamento AIR).

Al respecto, se tiene que, conforme al literal f) del artículo 15 del Reglamento AIR 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 Nº 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 Ente para el MTC a partir del 02 de enero de 2023.

Ahora bien, el Reglamento AIR, señala en el literal g) del artículo 3 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, el numeral 33.2 del artículo 33 del Reglamento AIR 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, en el caso particular del Proyecto de Norma, amerita la realización de un análisis de impacto regulatorio ya que se subsume en lo regulado en numeral 33.2 del artículo 33 del Reglamento AIR, 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.

Por otro lado, es importante mencionar que el Proyecto de Norma 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 Proyecto de Norma para la aplicación del Análisis de Calidad Regulatoria de procedimientos administrativos establecido en el artículo 2 del Decreto Legislativo Nº 1310, Decreto Legislativo que aprueba medidas adicionales de simplificación administrativa, aprobado por Decreto Supremo N° 061-2019-PCM.

X. Publicación del proyecto de Decreto Supremo que aprueba el marco normativo para la lucha contra llamadas y mensaje de texto con fines ilícitos

La obligación de publicar los proyectos normativos se encuentra establecida en el Reglamento que establece disposiciones sobre publicación y difusión de normas jurídicas de carácter general, resoluciones y proyectos normativos, aprobado por Decreto Supremo N° 009-2024-JUS (en adelante, Reglamento de publicación y difusión de normas jurídicas), el cual establece en su artículo 19 que los proyectos de normas jurídicas de carácter general deben ser publicados en las sedes digitales de las entidades de la Administración Pública a cargo de su elaboración o en otro medio, asegurando su debida difusión y fácil acceso.

Asimismo, conforme al literal c) del numeral 20.1 del artículo 20 del Reglamento de publicación y difusión de normas jurídicas, dispone que, en la publicación de los proyectos normativos, debe contemplarse un plazo no menor a quince (15) días calendario para la recepción de los comentarios, aportes u opiniones.

Por su parte, el artículo 19 de los Lineamientos para Desarrollar y Consolidar la Competencia y la Expansión de los Servicios Públicos de Telecomunicaciones en el Perú, incorporados por el Decreto Supremo N° 003-2007-MTC al Decreto Supremo N° 020-98-MTC, establece que el MTC publica para comentarios, por un plazo mínimo de quince (15) días calendario, entre otros, los dispositivos legales referidos a los servicios de telecomunicaciones, los estudios sobre nuevas tendencias y otros que consideren relevantes.

De acuerdo, al numeral 5.1 de la Directiva N° 010-2018-MTC/01 “Directiva que establece el procedimiento para realizar la publicación de proyectos normativos”, aprobada por Resolución Ministerial N° 977-2018-MTC/01 (en adelante, la Directiva que establece el procedimiento para realizar la publicación de proyectos normativos), establece que mediante Resolución Ministerial publicada en el Diario Oficial “El Peruano”, se dispone la difusión de todo proyecto normativo de carácter general, en el portal institucional del MTC o mediante cualquier otro medio, por un plazo no menor de diez (10) días hábiles.
En tal sentido, se considera que resulta necesaria la publicación de la propuesta normativa en el Diario Oficial “El Peruano” y en la página web del MTC, por el plazo de quince (15) días calendario, a efectos de recibir sugerencias y comentarios de la ciudadanía en general y de los agentes involucrados, conforme a lo establecido en el Reglamento de publicación y difusión de normas jurídicas y en la Directiva que establece el procedimiento para realizar la publicación de proyectos normativos

Cabe indicar que, la publicación del proyecto normativo guarda consistencia con la política de transparencia que rige el accionar de esta entidad, en el entendido de que esta medida garantizará la mejor comprensión de la propuesta por parte de los agentes interesados o involucrados, así como de la ciudadanía en general.