San José, 12 de junio 2026
05772-SUTEL-DGM-2026

Señores
Miembros del Consejo.
Superintendencia de Telecomunicaciones

ASUNTO: INFORME DE ATENCIÓN DE LAS POSICIONES DE LA CONSULTA PÚBLICA SOBRE LA IMPLEMENTACIÓN DE MEDIDAS REGULATORIAS CON EL FIN DE MINIMIZAR EL IMPACTO DE CIBERATAQUES MEDIANTE MENSAJES DE TEXTO SMS (SMISHING) Y LLAMADAS (VISHING)

Estimados señores:

En relación con las posiciones presentadas en el marco de la consulta pública convocada según lo dispuesto en el artículo 361 inciso 3) de la Ley General de la Administración Pública respecto al documento denominado "*ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)*", que se tramita en el expediente GCO-DGM-IET-00518-2026, la Dirección General de Calidad (DGC) y la Dirección General de Mercados (DGM) presentan para valoración del Consejo de la Superintendencia de Telecomunicaciones, el siguiente análisis de las posiciones remitidas, el cual no tiene carácter vinculante, de conformidad con lo dispuesto en el artículo 303 de la citada Ley.

1. ANTECEDENTES

1.1. Que mediante oficio número 02238-SUTEL-DGM-2026 con fecha del 6 de marzo de 2026, las citadas Direcciones presentaron ante el Consejo de Sutel la propuesta regulatoria a ser sometida a consulta pública para minimizar el impacto de ciberataques mediante llamadas telefónicas y mensajes SMS denominada: "*ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)*" (Folios 50 al 52).

1.2. Que mediante oficio 02650-SUTEL-SCS-2026 del 18 de marzo del 2026, el Secretario del Consejo de la Sutel, comunicó el Acuerdo N° 029-014-2026 de la sesión ordinaria N° 014-2026 del Consejo de Sutel celebrada el 12 de marzo del 2026, mediante el cual se dio por recibido y aprobado el informe técnico número 02238-SUTEL-DGM-2026 de fecha del 06 de marzo del 2026, adicionalmente, se dispuso, someter a consulta pública dicho informe mediante el cual la DGM y DGC, recomendaron la consulta de la medida regulatoria titulada *"ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)"*. (Folios 53 al 55).

1.3. Que, en fecha del 10 de abril de 2026 , se publicó en el diario oficial La Gaceta N°65; el edicto de consulta pública del oficio número 02238-SUTEL-DGM-2026 denominado *"ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)"* (NI-04737-2026); otorgándose el plazo de 10 días hábiles a partir de tal publicación para recibir observaciones. (Folios 56 al 59).

1.4. Que mediante oficio 03500-SUTEL-DGM-2026 de fecha del 14 de abril del 2026, la Dirección General de Mercados, notificó a los operadores y proveedores con numeración asignada por esta Administración, la apertura de la consulta pública sobre la *"METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)"* (Folios 60 al 114).

1.5. Que mediante oficio número 74_CMW_26 del 22 de abril de 2026 (NI-05367-2026), la empresa **CallMyWay NY S.A. (Call My Way)** por medio del señor Ignacio Prada Prada, en su condición de apoderado generalísimo, presentó su posición a la consulta pública en cuestión. (Folios 117 al 130).

1.6. Que mediante la nota remitida el 24 de abril de 2026 (NI-05496-2026), la empresa **Mitto AG** por medio del señor Andrea Giacomini en su condición de director ejecutivo, presentó su posición a la consulta pública de referencia. (Folios 131 al 146).

1.7. Que por medio del oficio RI-0168-2026 del 24 de abril de 2026 (NI-05526-2026), la empresa **Claro CR Telecomunicaciones S.A. (Claro)** por medio del señor Andrés Oviedo Guzmán, en su condición de gerente regulatorio, presentó su posición a la consulta pública en mención. (Folios 147 al 162).

1.8. Que mediante oficio número 7110-399-2026 del 24 de abril de 2026 (NI-05531-2026), el **Instituto Costarricense de Electricidad (ICE)** por medio del señor Adolfo Arías Echandi, en su condición de apoderado general, presentó su posición a la consulta pública en cuestión. (Folios 162 al 173).

1.9. Que mediante oficio LY-Reg0090-2026 del 24 de abril de 2026 (NI-05533-2026), la empresa **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty)** por medio del señor Donato Rivas Garro, en su condición de apoderado generalísimo, presentó su posición a la consulta pública de referencia. (Folios 174 al 183).

1.10. Que por medio del oficio MICITT-DVT-OF-204-2026 del 24 de abril de 2026 (NI-05536-2026), el **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)** por medio del señor Hubert Vargas Picado, en su condición de Viceministro de Telecomunicaciones, presentó su posición a la citada consulta pública. (Folios 184 al 190).

1.11. Que mediante oficio CIT-0010-2026 del 24 de abril de 2026 (NI-05538-2026) la **Cámara de Infocomunicación y Tecnología (INFOCOM)** por medio de la señora Ana Lucía Ramírez Calderón, en su condición de Directora Ejecutiva, presentó su posición a la consulta pública en mención. (Folios 191 al 196).

1.12. Que mediante oficio CAFF-54-2026 del 28 de abril de 2026 (NI-05678-2026) la empresa **Millicom Cable Costa Rica, S.A. (Tigo)** por medio de la señora Roxana María Sánchez Eguizabal, en su condición de apoderada generalísima, presentó de manera extemporánea su posición a la consulta pública de referencia. (Folios 197 al 200).

2. ANTECEDENTES DE PRÁCTICAS PROHIBIDAS Y LA URGENCIA DE MEDIDAS DE PREVENCIÓN CONTRA SMISHING Y VISHING

El medio de prensa **Teletica** publicó el 16 de mayo de 2026 la noticia ***"MOPT alerta sobre estafas por mensajes de texto cobrando multas"***[1], donde se informa sobre la suplantación de la identidad del Ministerio de Obras Públicas y Trasportes (MOPT) para estafar a los ciudadanos mediante mensajes SMS.

Asimismo, el medio de prensa **Delfino.CR** en fecha 25 de mayo de 2026 publicó la nota ***"UNED advierte sobre aumento de estafas por SMS que buscan robar datos personales y bancarios"***[2], donde la Universidad Estatal a Distancia (UNED) advirtió sobre el aumento de las estafas digitales mediante mensajes de texto SMS en Costa Rica.

Por su parte, el medio **Trivision** también publicó el 25 de mayo de 2026 la nota ***"Expertos alertan riesgos sobre "mensajes urgentes" en fraudes digitales"***[3], donde brinda recomendaciones a la población para evitar ser víctima de ciberataques por smishing.

Además, el medio de prensa **Diario Extra** publicó el 31 de mayo de 2026 la nota ***"Los fraudes digitales continúan en aumento y ahora utilizan mensajes urgentes para engañar a las personas y robar información personal o bancaria."***[4], donde advierte a los usuarios sobre el crecimiento de casos de smishing.

Finalmente, el medio de prensa Noticias Costa Rica (NCR) en fecha 9 de junio de 2026 publicó la nota ***"¿Le llegó este mensaje sobre multas? Podría ser una estafa"***[5], donde se alerta sobre usuarios que han recibidos mensajes SMS fraudulento solicitando el pago de supuestas multas de tránsito pendientes.

Adicional a lo anterior, el señor Jeffrey Cervantes Bermúdez, Director Ejecutivo del Consejo de Seguridad Vial (COSEVI) mediante el oficio CSV-DE-0499-2026 del 26 de mayo de 2026

[1] https://www.teletica.com/multimedia/mopt-alerta-sobre-estafas-por-mensajes-de-texto-cobrando-multas_1253540
[2] https://delfino.cr/2026/05/uned-advierte-sobre-aumento-de-estafas-por-sms-que-buscan-robar-datos-personales-y-bancarios
[3] https://trivisioncr.com/noticias-nacionales/expertos-alertan-riesgos-sobre-mensajes-urgentes-en-fraudes-digitales/
[4] https://www.facebook.com/diarioextra/videos/nacionales-los-fraudes-digitales-contin%C3%BAan-en-aumento-y-ahora-utilizan-mensajes-/1019755380994846/
[5] https://ncrnoticias.com/nacionales/le-llego-este-mensaje-sobre-multas-podria-ser-una-estafa/

(NI-07169-2026) solicitó a esta Superintendencia: *"(…) Con el objetivo de detener la afectación a la ciudadanía y salvaguardar la imagen de COSEVI, agradecemos su apoyo para promover la investigación y suspensión definitiva de los servicios con los operadores involucrados (…) a continuación, se muestra una serie de números telefónicos reportados por la población, desde los cuales se están emitiendo estos mensajes fraudulentos (phishing/smishing) (…)"*.

Es importante mencionar que, los hechos y publicaciones de prensa recientes en lo referente a smishing han evidenciado una tendencia creciente y agresiva en cuanto a esta práctica en el país que ha perjudicado a varios usuarios y continua presente, por lo que, es clara la urgencia de adoptar medidas para mitigar estos ciberataques. Como se indicó en la propuesta regulatoria sometida a consulta pública, durante el año 2025, la Dirección General de Calidad (DGC) solicitó al operador **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty)** en 15 ocasiones la suspensión de más de 30 servicios con numeraciones asignadas a este operador, por prácticas de smishing, sin embargo, solo durante el primer semestre de este 2026, la DGC solicitó al **Instituto Costarricense de Electricidad (ICE)** en 10 ocasiones la suspensión de 35 servicios por esta misma práctica, lo que demuestra el incremento en este tipo de delitos, así como la agresividad de los atacantes, siendo que, los servicios identificados como generadores de smishing durante el primer semestre de este 2026 ya superan la totalidad de estos servicios identificados durante todo el año anterior, por lo que, es indispensable aplicar acciones inmediatas y contundentes contra estas prácticas que ponen en riesgo la seguridad de los usuarios.

Lo anterior evidencia que los delincuentes se encuentran buscando vulnerabilidades de diferentes sistemas para aprovecharlas y generar los ataques, lo que les ha permitido continuar sus prácticas fraudulentas utilizando los recursos numéricos de diferentes operadores, demostrando la urgencia de adoptar medidas contundentes en cuanto al manejo de esta situación por parte de los operadores, la cual ya ha trascendido en prensa e instituciones públicas, por lo que, cada día que transcurre sin una adecuada regulación que aborde por completo estas prácticas, implica un día más donde miles de usuarios se enfrentan al riesgo de ser estafados o ceder su información a terceros. Según lo detallado en el presente apartado, lamentable la realidad actual del mercado de las telecomunicaciones evidencia un aumento en ataques de vishing y smishing que se debe prevenir y abordar de manera directa.

Bajo un análisis de razonabilidad, la regulación propuesta busca mitigar una problemática actual de alto riesgo para la población, por lo que, su urgencia es comprobable con la problemática identificada por la Sutel, a partir de la evidencia señalada anteriormente.

El incremento sostenido y documentado de ataques de smishing y vishing evidencia una amenaza creciente y concreta para los usuarios de servicios de telecomunicaciones, quienes permanecen expuestos ante posibles ciberataques cada vez más sofisticados. En ausencia de un marco regulatorio adecuado y oportuno, se amplifica el riesgo de afectaciones económicas y de seguridad de la información a gran escala. En este contexto, resulta imperativo adoptar medidas regulatorias efectivas sin demoras indebidas, ya que las oposiciones presentadas, si bien forman parte del proceso de consulta pública, no deben

constituirse en un obstáculo que retrase la implementación de acciones necesarias para la protección del usuario final y la integridad de las redes de telecomunicaciones.

3. SOBRE LAS POSICIONES Y ANÁLISIS DE LA CONSULTA PÚBLICA REALIZADA POR ESTE ENTE REGULADOR.

De seguido, se procede con el análisis de las posiciones presentadas sobre la consulta pública del documento denominado *"ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)*", para lo cual, se detallará en qué consiste la observación o aporte, quién la formuló y cuál es la posición de esta Superintendencia al respecto, ya sea para acogerla o rechazarla.

3.1. Posición de CallMyWay NY S.A.:

Mediante oficio 74_CMW_26 del 22 de abril de 2026, (NI-05367-2026) CallMyWay NY S.A. (Call My Way) por medio del señor Ignacio Prada Prada, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
Consultas respecto a la sección de ANTECEDENTES

1. *En el numeral 3 de los ANTECEDENTES, SOBRE LA COMPETENCIA DE LA SUTEL, indica en el último párrafo, textual: "Por ende, en apego al artículo 2 inciso f) de la ley No 8642, Ley General de Telecomunicaciones donde se establece como un objetivo de dicha Ley promover el desarrollo y uso de los servicios de telecomunicaciones como apoyo a la seguridad ciudadanía,* ***es obligación*** *de esta Superintendencia* ***asegurar*** *que los servicios de telefonía y mensajería SMS* ***no sean utilizados para fines ilícitos*** *o que atenten contra la seguridad de los usuarios finales y la ciudadanía en general*

   Comentario: *El inciso f) del artículo 2 de la ley 8642, indica, textual:* ***"Promover el desarrollo y uso de los servicios de telecomunicaciones*** *dentro del marco de la sociedad de la información y el conocimiento y* ***como apoyo*** *a sectores como salud,* ***seguridad ciudadana****, educación, cultura, comercio y gobierno electrónico".*

   *Según dicho inciso no logramos concluir, de que "****es obligación*** *de esta Superintendencia* ***asegurar*** *que los servicios de telefonía y mensajería SMS* ***no sean utilizados para fines ilícitos*** *o que atenten contra la seguridad". No encontramos dicha obligación en la ley 7593 en la ley 8642 ni en alguna otra. Eso por supuesto no nos exime de que hagamos nuestros mayores esfuerzos para evitarlo.*

   Petitoria: *Se solicita ajustar los ANTECEDENTES donde se establezca, con base en la ley y la jurisprudencia de que, si existe tal obligación por parte de la superintendencia y que a su vez esta tiene la potestad de extenderla a los operadores, aun en detrimento de la privacidad de las comunicaciones y el derecho a la intimidad.*

2. *En el numeral 6 de Regulaciones y Recomendaciones Internacionales en el párrafo de Tasa de envío satisfactorio de mensajes, indica textual: "Dado que los mensajes spam se envían a receptores desconocidos de forma aleatoria la* ***tasa de envío satisfactorio de mensajes spam es sustancialmente inferior*** *a la de envío de mensajes móviles"*
   Comentario

- *En estos momentos el operador de SMS Liberty no facilita la confirmación de recepción y entrega del mensaje, por tal motivo no es posible evaluar la tasa de envío satisfactorio de mensajes con dicho operador. La implementación de esta medida permite a los operadores, de manera indirecta y efectiva aislar tráfico de mensajes SMS -y llamadas- sin incurrir en violación al derecho a la intimidad y privacidad de las comunicaciones, siendo esta una medida adecuada para identificar, tráfico, cuando menos sospechoso.*

Petitoria

- *Que, en la resolución a emitir, se solicita, se imponga que, dentro del protocolo de envío de mensajes se obligue a todos los operadores a cumplir con la normativa y práctica aceptada, y que se incluya el comprobante de entrega y recepción del mensaje SMS*

Consultas respecto al servicio de SMS:

3. *En el punto 9.1.A se indica, textual "Dicha relación comercial le brinda al operador o proveedor la **potestad de inspeccionar y revisar la totalidad del tráfico de mensajes SMS** que recibe por sus rutas de interconexión internacional o local para garantizar la seguridad de sus usuarios finales*

   Comentario:

   - *Como se comentó en el numeral 1. hasta donde conocemos, por motivos de intimidad y derecho a la privacidad de las comunicaciones, los operadores no contamos con potestad de inspeccionar ni de revisar, total ni parcialmente el tráfico de mensajes SMS, ni de voz.*

   Petitoria:

   - *Incluir el fundamento legal ampliamente desarrollado respecto a la mencionada potestad, de manera que cuando los operadores inspeccionemos y revisemos la totalidad del tráfico de mensajes SMS -y de voz- requeriremos dicho fundamento legal para así evitarnos demandas legales por parte de los usuarios finales al ser violentada su derecho a la privacidad e intimidad. Dentro de dicho fundamento legal solicitamos se incluya la potestad de la superintendencia de endosar dicha potestad a los operadores con recurso numérico asignado.*

4. *En el punto 9.1.C se indica, textual: "deben implementar en sus redes sistemas de firewall para mensajería SMS con capacidades adaptativas de identificación, análisis y filtrado, apoyados con **Inteligencia Artificial, para realizar una Inspección Profunda de Paquetes (DPI) en todos los mensajes SMS**, con el único objetivo de buscar enlaces maliciosos o reconociendo patrones y comportamientos que identifiquen dichos mensajes como maliciosos".*

   Petitoria:

   - *Dado que la IA no es sencilla ni económica, se solicita se nos facilite el modelo y versión de IA que se debe utilizar, así como su entrenamiento, protocolo y la norma internacional para poder ejecutar la Inspección Profunda de Paquetes (DPI) para la respectiva identificación y análisis.*
   - *Se solicita que se considere el costo de la IA a utilizar para realizar la Inspección Profunda de Paquetes en las finanzas de los operadores de telecomunicaciones con recurso numérico asignado.*

5. *En el punto 9.1.C se indica, textual: "**cuyo número de origen haya sido enmascarado con un número local**, de forma similar a las disposiciones establecidas en la resolución RCS-294-2023 para el tráfico de voz"*

   ***Comentario:** Para el Caso de CallMyWay, contamos con clientes internacionales, aun así, dado que los operadores locales no nos permiten enviar tráfico de SMS con identificadores internacionales, se les asigna numeración local a esos clientes, por lo que tenemos duda de cómo será considerado dicho tráfico, ya que el mismo no se encuentra enmascarado y es*

trazable de extremo a extremo, aun cuando es un cliente internacional, opera como local, con identificador nacional sin enmascaramiento.
***Petitoria:** Se solicita que, en la futura resolución a emitir, se definan los escenarios de cuando un mensaje SMS con identificador local y que aparenta ser internacional, no debe de ser considerado como enmascarado.*

6. *En el punto 9.1.C.2, se indica, textual: "Capacidad para detectar y bloquear la totalidad del tráfico de tipo A2P o P2P **con origen internacional, cuyo número de origen haya sido enmascarado con un número local**.*
   ***Comentario:** Aplica la misma petitoria, respecto al punto 9.1.C, anterior*

7. *En el punto 9.1.C.4 se indica, textual: "Validación del Título Global (GT, Global Title) y verificación en tiempo real del origen del mensaje"*
   Petitorias:
   - *Se solicita que en la futura resolución a emitir se indique*
     - *Como se valida el Título Global*
     - *Cuál es la entidad encargada de asignar los Títulos Globales*
     - *Se indique, que es, como y bajo que protocolo, se verifica en tiempo real el origen del mensaje y si esa verificación se debe de ejecutar de extremo a extremo.*
     - *Como se deben de operar los mensajes, y llamadas, internacionales que por su naturaleza no cuentan con un Título Global y que a su vez no son ni spam ni maliciosos, como los que son por naturaleza A2P o los que vienen de aplicaciones OTT*

8. *En el punto 9.1.C.6 se indica, textual: "**Uso de Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP)** para detectar variaciones en la ortografía del mensaje o el uso de caracteres especiales para evitar filtros. Además de realizar **Análisis Heurístico** con el fin de detectar malware o cualquier otra amenaza contenida en el mensaje"*
   Petitoria:
   - *Se solicita que en la próxima resolución a emitir se indique la inteligencia artificial con Procesamiento de Lenguaje Natural (NLP) y el respectivo modelo y entrenamiento a utilizar*
   - *Se solicita que en la próxima resolución a emitir se indique el modelo y normativa del Análisis Heurístico a utilizar*
   - *Se solicita que se considere el costo de la IA a utilizar para realizar el Procesamiento de Lenguaje Natural y el Análisis Heurístico en las finanzas de los operadores de telecomunicaciones con recurso numérico asignado.*

9. *En el punto 9.1.C.9 se indica, textual: "**Capacidad de traducir y analizar automáticamente mensajes** en formato binario y cualquier otro formato técnico de codificación aplicable a los servicios de mensajería móvil que puedan utilizarse para instalar malware u otras amenazas en los dispositivos de los usuarios finales"*
   Petitoria:
   - *Se solicita que en la próxima resolución a emitir se indique:*
     - *Como se debe de operar ante mensajes, binarios, encriptados, con los que no se cuente con capacidad de desencriptarlos o traducirlos.*
     - *Como se debe de operar ante mensajes binarios que, aunque se pueden traducir o analizar no se encuentra información inteligible, como por ejemplo un string de caracteres que bien puede ser un token de autenticación y que resulte que, efectivamente el receptor la requiere.*

10. *En el punto 9.1.C.12 se indica, textual: "Detección de **ráfagas de spam** (Spam Burst) e identificación de campañas de smishing rápidas que intentan entregar gran cantidad de mensajes en cortos períodos de tiempo"*

    ***Petitoria:** Se solicita que en la futura resolución a emitir se incluya el criterio de como se debe de actuar cuando se detecta de una ráfaga de spam (Spam Burst) y el criterio para saber cuándo es maliciosa o no. A su vez se solicita indicar los criterios a actuar ante los falsos positivos y los falsos negativos cuando se presenten.*

11. *En el punto 9.1.C.13 se indica, textual: "Análisis de **simetría en las comunicaciones** que permita identificar de manera bidireccional el tráfico que nunca recibe respuesta, es decir servicios que generan grandes cantidades de comunicaciones, pero nunca reciben respuesta, correspondiente al comportamiento de bots"*

    ***Petitoria:** Se solicita que en la próxima resolución a emitir se indique en que casos mensajes unidireccionales deban ser considerados spam o malware, ya que contamos con clientes cuyo patrón es de solo envío de mensajes, como por ejemplo los bancos con claves de doble factor y no por ser unidireccionales se convierten en tráfico malicioso, spam o malware.*

12. *En el punto 9.1.D se indica, textual: "Los operadores y proveedores deben utilizar **sistemas de reputación de enlaces** para bloquear mensajes que contengan enlaces WEB maliciosos o de dudosa procedencia"*

    ***Petitoria:** Se solicita que en la próxima resolución a emitir se indique como operan los sistemas de reputación de enlaces, si existen librerías o sitos donde puedan ser consultados para que así puedan ser bloqueados los respectivos mensajes.*

13. *En el punto 9.1.E se indica, textual: "Los operadores y proveedores realizarán **Inspección Profunda de Paquetes (DPI) en la totalidad del tráfico de mensajes SMS** únicamente con el objetivo de identificar comunicaciones maliciosas que amenacen la seguridad de los usuarios"*

    ***Petitoria:** Se solicita que en la próxima resolución a emitir se incluya:*

    - *El criterio, la normativa, la IA su modelo y su entrenamiento para aplicar la Inspección Profunda de Paquetes (DPI).*
    - *La regulación completa que nos permite a los operadores realizar Inspección Profunda de Paquetes (DPI) en la totalidad del tráfico de mensajes SMS -y voz- aunque sea solo para identificar comunicaciones maliciosas que amenacen la seguridad de los usuarios.*
    - *Se solicita que se considere el costo de la IA a utilizar para realizar la Inspección Profunda de Paquetes en la totalidad del tráfico de mensajes SMS en las finanzas de los operadores de telecomunicaciones con recurso numérico asignado.*

Consultas respecto a los servicios de llamadas de Voz:

14. *En el punto 9.5.A. se indica textual: "en los servicios de voz que minimicen el impacto de los ataques tipo vishing a usuarios finales*

    Petitoria:

    - *Se solicita que en la próxima resolución a emitir*
        - *Se indique como se va a evaluar el éxito o fracaso de cada una de las medidas ordenadas, de manera que le brinde criterio a la superintendencia para incluir más medidas o por el contrario eliminarla por carecer de utilidad.*
        - *Se indique cual es la tasa actual de llamadas tipo vishing o su efecto en el sector, de manera que se tenga criterio para las futuras evaluaciones*

15. *En el punto 9.5.A.(a) se indica textual: "Procesamiento masivo de registros de llamadas (CDRs) para la trazabilidad de las comunicaciones"*

Comentario:

- *Consideramos esta medida como necesaria y suficiente para detectar no solo llamadas de vishing, sino todo un amplio compendio de llamadas maliciosas, estafas y tráfico no deseado.*
- *Con el fin de que funcione llevamos años desarrollando, algoritmos informáticos de análisis de CDRs donde hemos aislado bastantes patrones de uso malicioso*
- *Utilizando nuestros algoritmos informáticos logramos bajar de 36 denuncias durante el año 2021 por parte del Poder Judicial a 2 en 2025*
- *Esta medida nos permite minimizar el tráfico malicioso todo en concordancia con el artículo 42 de la ley 8642*

Petitoria

- *En la medida que este procesamiento masivo de registros de llamada demuestre su capacidad de minimizar las llamadas maliciosas a niveles razonables, se solicita que se establezca como única medida parte de la resolución a emitir tanto para llamadas de voz como SMS*

16. *En el punto 9.5.A.(b) se indica textual: "Procesamiento de información de señalización obtenida de las comunicaciones y por puntos de recopilación"*

Petitoria:

- *Se solicita que en la próxima resolución a emitir se indique que, y como debemos analizar de la información de la señalización obtenida de las comunicaciones, ya que hasta la fecha no le hemos encontrado utilidad a procesar dicha información respecto a la prevención de tráfico de spam o malicioso.*

17. *En el punto 9.5.A.(c) se indica textual: "Detección de patrones de comportamiento sospechoso como frecuencia de llamadas, tasa de conexiones exitosas, duración de las llamadas, duración de tonos, estadísticas de llamadas entre otras."*

Petitoria:

- *Consideramos que esta medida junto con la 9.5.A.(a) son complementarias, necesarias y suficientes para minimizar las llamadas maliciosas.*

18. *En el punto 9.5.A.(d) se indica textual: "Identificación de llamadas automatizadas que utilizan grabaciones de voz o voz sintética (robollamadas o robocalls)"*

Petitoria:

- *Se solicita que en la próxima resolución a emitir se indique:*
  - *Cual es el método que debemos utilizar para identificar las llamadas automatizadas que utilizan grabación de voz o sintética (robollamadas o robocalls)*
    - *Al respecto conocemos dos métodos de identificación: en tiempo real mediante derivación del tráfico y análisis instantáneo o retrospectivamente mediante grabación de las llamadas para su posterior análisis.*
    - *Si la superintendencia conoce de algún otro solicitamos sea indicado e incluido en la respectiva resolución*
  - *Si es en tiempo real se solicita indicar la IA, versión, entrenamiento y el respectivo costo de la que debemos utilizar*

- *Si es mediante grabación de llamadas se solicita indicar la IA, versión, entrenamiento y el respectivo costo de la que debemos utilizar*
- *Para ambos casos por favor indicar como deben operar estas derivaciones o grabaciones respecto a lo indicado en el artículo 42 de la ley 8642*
- *Para ambos casos se solicita se considere el costo de la IA, costos de servidores para grabación y análisis y el nuevo personal que debemos contratar, para analizar la totalidad de las llamadas -y SMS- y el efecto que dicho costo va a tener en las finanzas de los diferentes operadores.*
  - *Hasta donde conocemos el costo de analizar con IA una grabación telefónica tiene un costo de entre US$0.06 a US$0.1 por minuto, según la IA y modelo a utilizar y la profundidad del análisis que se ejecute, lo que es más oneroso de lo que actualmente se cobra por el tráfico telefónico, tanto al cliente final como los cargos de interconexión*
- *Para ambos casos se solicita que se considere se incluya el análisis del efecto que va a tener en el mercado en el momento que los usuarios conozcan que la totalidad de sus llamadas -y mensajes de SMS- van a ser analizadas con inteligencia artificial de inspección profunda y Procesamiento de Lenguaje Natural*

19. *En el punto 9.5.D se indica textual: "Los operadores y proveedores deben adoptar e implementar el estándar Out-of-Band SHAKEN (OOBS) para autenticación de todas las llamadas".*
    ***Petitoria:** Se solicita incluir en la futura resolución a emitir:*
    - *Se solicita indicar cuál va a ser la entidad encargada de certificar a los operadores y facilitar las firmas digitales*
    - *Se solicita indicar el estudio de muestreo que se ejecutó con los actuales operadores para conocer su factibilidad de implementar el Out-of-Band SHAKEN (OOBS) y cual va a ser su tiempo de implementación y costo, así quien lo debe de asumir.*
    - *Se solicita indicar como debemos actuar los operadores cuando recibimos llamadas internacionales de operadores que no tienen implementado el estándar Out-of-Band SHAKEN (OOBS)*
    - *Se solicita indicar como debemos actuar los operadores cuando recibimos llamadas internacionales de operadores de países donde no se ha implementado el estándar Out-of-Band SHAKEN (OOBS) ni el STIR SHAKEN ya sea que tengan o no planes de que se implemente*
    - *Se solicita indicar como debemos actuar los operadores cuando recibimos llamadas internacionales de operadores que no utilizan el E.164 como identificador de llamada como es el caso de los OTT y que adicionalmente no van a contar con Out-of-Band SHAKEN (OOBS), STIR SHAKEN ni Título Global.*
    - *Se solicita indicar que otras posibles alternativas tecnologías existen para resolver la problemática planteada*
      - *Nota: Como se indicó anteriormente, con la regulación vigente y la RCS-294-2013 ya se encuentra cubierto el tema de la suplantación de identidad para llamadas con numeración local. Aun así, no se está cubriendo ni mencionando como se van a tratar las llamadas con identificador internacional*
    - *Se solicita indicar que utilidad tiene implementar el Out-of-Band SHAKEN (OOBS) cuando la totalidad de las interconexiones en Costa Rica se ejecutan mediante el protocolo SIP*

20. *En el punto 9.6 se indica textual: "Otorgar 180 días naturales a los proveedores y operadores con numeración asignada por esta Superintendencia, una vez publicada la presente metodología regulatoria en el diario Oficial La Gaceta para que se proceda a su implementación, plazo en el cual, deberán realizar las configuraciones necesarias a nivel de sus sistemas para proceder con los ajustes técnicos e implementación de las medidas regulatorias dispuestas en los apartados "9.1.SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P; .9.2. ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS P2P Y A2P.; 9.3. SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P y 9.4. ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS A2P".*
    Petitoria:
    - *Por favor indicar cuál es el plazo de implementación para el apartado 9.5 correspondiente a los servicios de llamadas de voz*
    - *Se solicita analizar el plazo de implementación en función de las diferentes soluciones tecnológicas que se deban implementar y que antes de emitir un plazo al respecto se realice una consulta fluida, con todos los operadores para conocer sus posibilidades y costos de implementación ya que inicialmente 180 días parece mucho, pero implementar muchas de las medidas indicadas puede resultar no tri vial.*
    - *Se solicita a la superintendencia conocer las dificultades que tuvo la FCC en implementar el STIR SHAKEN*

Consulta sobre los reportes:

21. *La resolución RCS-294-2023 ordena a los operadores de telefonía que deben de reportar cuatrimestralmente respecto a la cantidad de llamadas bloqueadas*
    Petitoria: *Favor indicar en la resolución a emitir por la superintendencia con que frecuencia se deben emitir reportes sobre los SMS bloqueados*
    Nota: *Se solicita considerar la gran cantidad de reportes que debemos emitir los operadores a la superintendencia, por lo que apreciamos si dicha frecuencia se hace anual o incluso ante solicitud expresa de la superintendencia*

(…)
Petitoria General
(…)

Sugerimos y solicitamos respetuosamente a la superintendencia que ajuste el alcance de la mediad planeada y lo limite al análisis de los registros de llamadas (COR) según criterios predefinidos ya que en caso contrario la medida planteada puede tener tales costos que harán inviable todo el servicio de telefonía y SMS locales

(…)".

Las observaciones a la propuesta presentadas por CallMyWay NY S.A. (Call My Way) se interpusieron dentro del plazo brindado por la Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por CallMyWay NY S.A. (Call My Way) se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

2.1.1 Análisis de las observaciones realizadas por CallMyWay NY S.A.:

Con respecto al **punto 1** de las observaciones planteadas, sobre la competencia de la Sutel, solicita el operador que se corrija la propuesta de regulación para que se incluya como parte

de los antecedentes la obligación de esta Superintendencia y de los operadores de asegurar que los servicios de telefonía y mensajería SMS no sean utilizados para fines ilícitos o que atenten contra la seguridad.

En este sentido se tiene que en el oficio número 02238-SUTEL-DGM-2026 del 06 de marzo de 2026, en el punto 4.7 específicamente se establece que se aboga por un desarrollo de las telecomunicaciones que contribuya con la seguridad ciudadana, conforme el régimen de protección a la intimidad y los derechos de los usuarios establecidos en los numerales 42 y 45 inciso 29) de la Ley General de Telecomunicaciones, sin embargo, no se citan expresamente dichos numerales, por lo que en aras de reforzar la motivación del acto deberán incluirse los citados artículos para que se lea dentro de los antecedentes de la siguiente manera:

> *"a) El artículo 42 de la LGT señala que*: *"(...) Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios (...)."*
>
> *b) Además, con lo dispuesto en el artículo 45 inciso 29) de la LGT que dispone que también son derechos de los usuarios "Los demás que se establezcan en el ordenamiento jurídico vigente" tal y como corresponde a lo dispuesto en el RPUF, razón por la cual, resulta aplicable las disposiciones que apoyan la seguridad ciudadana en el CAPITULO XVIII. PRÁCTICAS PROHIBIDAS EN LOS SERVICIOS DE TELECOMUNICACIONES."*

Lo anterior considerando, que en búsqueda de la seguridad ciudadana se emite la propuesta de regulación objeto de análisis, la cual busca la implementación de medidas con el fin de minimizar el impacto de ciberataques mediante el uso de llamadas telefónicas y mensajes de texto SMS, dentro de las cuales tanto la Sutel como los operadores son responsables. Por las razones anteriores se recomienda acoger la solicitud del operador.

Sobre la observación **número 2** respecto a la confirmación de recepción para medir la tasa de envío satisfactorio de mensajes y la petición sobre que *"(…) se imponga que, dentro del protocolo de envío de mensajes se obligue a todos los operadores a cumplir con la normativa y práctica aceptada, y que se incluya el comprobante de entrega y recepción del mensaje SMS (…)"*, esta Superintendencia coincide que la remisión del comprobante de entrega de mensajes SMS por parte de todos los operadores que brindan el servicio de mensajería de texto SMS es fundamental para medir la tasa de envíos satisfactorios e identificar servicios con comportamientos sospechosos en cuanto a la remisión de grandes campañas de mensajes. De modo que, se recomienda acoger lo requerido por CallMyWay NY S.A. (Call My Way) en el punto 2, por lo que, se propone requerir a todos los operadores y proveedores de mensajería SMS la inclusión del comprobante de entrega y recepción de mensaje SMS, así como cualquier configuración necesaria para el éxito de la presente propuesta regulatoria y su coordinación entre operadores.

En cuanto a las consultas planteadas en el **punto 3** sobre la privacidad de la información de los usuarios, el operador solicita que se incluya el fundamento legal que habilita a los operadores a inspeccionar y revisar la totalidad del tráfico de los mensajes SMS. En este sentido debe considerarse que actualmente por medio del Ministerio de Ciencia, Tecnología

y Telecomunicaciones (MICITT) se está llevando a cabo la Estrategia Nacional de Ciberseguridad[6] (2023-2027), la cual, enfatiza la importancia de identificar y evaluar los riesgos cibernéticos para implementar medidas de protección y se centra en los siguientes enfoques rectores: a) Enfoque de toda la sociedad, b) Enfoque de gestión y mitigación de riesgos, c) Enfoque de Derechos Humanos, d) Enfoque centrado en el ser humano.

Específicamente en el sector de telecomunicaciones, artículo 2 inciso f) de la Ley General de Telecomunicaciones establece como objetivo promover el desarrollo y uso de los servicios de telecomunicaciones como apoyo a la seguridad ciudadana, y el artículo 42 de la citada Ley señala que los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. Además, se adoptaron medidas regulatorias, a partir de la publicación del Reglamento sobre el Régimen de Protección al Usuario Final publicado en el Alcance N°200 de La Gaceta N°180 del 22 de setiembre de 2022 y, que entró en vigor a partir del 23 de setiembre de 2023, que establece dentro de las obligaciones de los operadores y proveedores de servicios de telecomunicaciones conforme al numeral 11 del mencionado reglamento, las siguientes: *"(...)**15.**Implementar los sistemas y medidas técnicas y administrativas necesarias, que permitan la detección y prevención de intromisiones no autorizadas en la red. (…) **27.** Verificar la autenticidad y registrar, adecuadamente, los datos y documentos de identificación de los clientes, al momento de realizar la suscripción o comercialización del servicio. (…) **30.** Suspender de forma temporal o definitiva los servicios de telecomunicaciones, de conformidad con las disposiciones del presente reglamento. (…) **32.** Acreditar, mediante documento idóneo, el consentimiento otorgado por el cliente, para su representación o acceso a información sensible o confidencial (…)"*.

En este mismo sentido, el artículo 5 incisos 1), 4), 7) y 8) del citado Reglamento establece dentro de las obligaciones de los usuarios finales, las siguientes: *"(…) **1.** Actuar de buena fe de previo a la contratación y durante el uso del servicio. (…) **4.** Hacer uso lícito y responsable de las redes, equipos y servicios de telecomunicaciones. (…) **7.** Evitar el envío de comunicaciones que puedan perjudicar los derechos de los demás usuarios finales y la seguridad de las redes de los operadores/proveedores. **8.** Abstenerse de realizar prácticas prohibidas o de utilizar los servicios de telecomunicaciones para fines distintos del contratado (…)."* Además, el numeral 47 inciso 4) del mismo cuerpo normativo dispone que los contratos de servicios de telecomunicaciones se extinguirán cuando se compruebe la comisión de prácticas prohibidas.

En la misma línea, el citado reglamento establece como prácticas prohibidas por parte de los usuarios finales al amparo del numeral 106 incisos 1), 2), 7) y 8) del Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF): *"**1.** Alterar o poner en riesgo la operación normal de la red y su seguridad, así como degradar la calidad del servicio. **2.** Acciones que provoquen interferencias, interrupciones, congestión o daños a la red y a otros usuarios de los servicios de telecomunicaciones. (…) **7.** Actuar con engaño, fraude, mala fe, dolo en la suscripción o uso del servicio. **8.** Utilizar los servicios de telecomunicaciones para fines distintos del contratado. (…) faculta al operador/proveedor para suspender el servicio de forma temporal y en caso de que no se corrija dicha condición en el plazo de dos meses, se procederá con la suspensión definitiva, liquidación contable y la disposición del recurso numérico"*.

Por las anteriores consideraciones, de forma oficiosa, este órgano regulador ha remitido solicitudes a los operadores para que procedan de conformidad con la citada normativa para la suspensión de los servicios telefónicos en los que se identifiquen el envío de

[6] *Disponible en el sitio WEB https://www.micitt.go.cr/sites/default/files/2023-11/NCS%20Costa%20Rica%20-%2010Nov2023%20SPA.pdf*

mensajes fraudulentos de smishing y la implementación de acciones preventivas y correctivas para evitar este tipo de prácticas irregulares.

En todo caso el objeto de la normativa no está enfocado en que se intervengan las comunicaciones y que un tercero lea o acceda al contenido o información de un mensaje, sino más bien se pretende adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios de conformidad con el artículo 42 de la Ley N°8642, por medio de algoritmos computacionales y el análisis de Inteligencia Artificial, es decir, que sin intervención humana, se apliquen reglas de filtrado de mensajes maliciosos, por lo que, no se estaría ante la violación señalada por el operador, ya que las técnicas propuestas no constituyen una violación a la privacidad de las comunicaciones. En virtud de las consideraciones anteriores, se tiene que existe un marco normativo que sustenta la obligatoriedad que se está imponiendo a los operadores y procede la inclusión del numeral 42 de la Ley General de Telecomunicaciones como parte del sustento normativo de la regulación sometida a consulta pública, por lo que recomienda acoger la solicitud del operador en este sentido.

Como referencia comparativa al respecto, es posible tomar en consideración los mecanismos *"cortafuegos"* o *"firewall"* que se tienen implementados tanto a nivel de empresas o corporaciones, así como a nivel domiciliar, para filtrar el acceso a algunos sitios Web y conexiones riesgosas, con el fin proteger a las personas que acceden a Internet de amenazas y ciberataques, los cuales se basan en un análisis en tiempo real a partir de una serie de reglas establecidas para prevenir riesgos de seguridad; esto es exactamente lo que pretende la regulación propuesta, de hecho los mecanismos que se implementan en los centros de mensajería son comúnmente denominados *"firewall SMS"* siendo la lógica equivalente, donde un sistema informático incluso asistido por la Inteligencia Artificial analiza en tiempo real los mensajes a partir de una serie de reglas definidas para filtrar aquellos que puedan implicar riesgos a la seguridad de los usuarios. Por lo anterior no se está ante una vulneración del régimen de privacidad y confidencialidad de las comunicaciones y mucho menos ante una intervención de éstas, dado que no se presenta el acceso a esta información por parte de terceros, sino que se realiza de forma automatizada por sistemas informáticos.

Respecto a las solicitudes realizadas en los **puntos 4**, **8** y **13** sobre indicar el modelo y versión de Inteligencia Artificial a utilizar, así como su entrenamiento, protocolo, normativa y costo, es importante mencionar que, el artículo 3 inciso h) de la Ley N°8642 Ley General de Telecomunicaciones, dispone el principio de neutralidad tecnológica, el cual, les brinda a los operadores y proveedores la posibilidad de escoger a discreción las tecnologías a utilizar para brindar sus servicios, siempre y cuando, cumplan con los requerimientos mínimos establecidos en la regulación, y se garanticen las condiciones de calidad, por lo que, esta Superintendencia no tiene la potestad para imponer un modelo específico de Inteligencia Artificial, siendo que, le corresponde a los operadores y proveedores elegir a su criterio la tecnología que mejor se ajuste a su infraestructura y presupuesto, para garantizar la seguridad de las redes y sus servicios y así cumplir con la regulación sometida a consulta pública, de modo que, se recomienda rechazar estas observaciones.

Sobre la observación señalada en los **puntos 5** y **6** respecto al trato de tráfico de mensajes SMS internacionales con números enmascarados, cabe señalar que, esta normativa busca cerrar la posibilidad de delitos por suplantación de identidad, de modo que, bajo el mismo principio de la resolución RCS-294-2023 respecto al enmascaramiento de llamadas, los operadores no deben enmascarar ni permitir el tráfico de comunicaciones que provienen de orígenes internacionales con números enmascarados. Asimismo, respecto a la afirmación sobre que "*los operadores locales no nos permiten enviar tráfico de SMS con identificadores internacionales, se les asigna numeración local a esos clientes*", se debe destacar que existen las herramientas regulatorias a través del Régimen de Acceso e Interconexión para que la SUTEL intervenga, en aquellos casos en los que no haya un acuerdo entre las partes, de modo que, se recomienda rechazar estas observaciones.

Con respecto a la observación del **punto 7** sobre la validación del Título Global (GT, Global Title) y verificación en tiempo real del origen del mensaje, de acuerdo con el desarrollador de plataformas de comunicación en la nube Infobip[7], los Títulos Globales son direcciones únicas que se refieren a un solo destino para enrutar mensajes SMS a través de diferentes redes en todo el mundo.

La estructura del Título Global se define mediante la recomendación de la Unión Internacional de Telecomunicaciones **UIT-T Q.713: *Formatos y códigos de la parte control de la conexión de señalización***. El valor de un Título Global es una secuencia de atributos que modifican el valor de la dirección. La longitud de una dirección de Título Global oscila entre 1 y 21 dígitos y funciona dentro del protocolo SS7 (Signaling System #7) para el enrutamiento de mensajes, por lo que, el Título Global es configurado por el operador en su red, con el fin de verificar la coherencia del origen del mensaje con la ruta recibida. Cabe señalar que el enlace a esta información fue citado en el pie de página número 19 de la citada propuesta regulatoria sometida a consulta pública.

Adicionalmente, siendo que el Título Global aplica en las redes SS7, se requirió la verificación en tiempo real del origen del mensaje y su trazabilidad, lo cual no se limita exclusivamente a comunicaciones mediante SS7, además implica validar la coherencia del origen del mensaje con la ruta desde la cual proviene y el operador que lo envía, para garantizar la trazabilidad de los mensajes SMS y validar su identidad, como se requirió en la regulación sometida a consulta pública.

Es decir, independientemente de usar Títulos Globales con redes SS7 o no, los operadores deben validar la identidad y trazabilidad del mensaje, así como la coherencia de las comunicaciones, de modo que, el origen del mensaje coincida con la ruta y el operador correspondiente, siendo que, los operadores no deberían recibir un mensaje con origen de un operador A desde una ruta asignada a un operador B. Un mensaje originado en la red de un operador A debe coincidir con la ruta de interconexión correspondiente al operador A. Para esto los operadores pueden basarse en los mecanismos que mejor se ajusten a su infraestructura, según el principio de neutralidad tecnológica citado anteriormente.

[7] https://www.infobip.com/glossary/global-title

Ahora bien, respecto al trato de mensajes A2P providentes de plataformas OTT (Over The Top), cabe señalar que, la mayoría de estos mensajes enviados por las aplicaciones OTT a los usuarios corresponden a claves de autenticación de cuentas personales, por lo que, es información confidencial de alto valor para los usuarios, de modo que, es indispensable que se apliquen métodos de análisis rigurosos sobre estos mensajes con el fin de asegurar su integridad. Las aplicaciones a menudo utilizan tokens web JSON (JWT) para administrar sesiones de usuario y autenticación, de modo que, estos tokens también contienen datos de usuario, lo que significa que si un token es robado o comprometido, los hackers tendrán acceso completo a la cuenta del usuario[8], además, es conocido que existen ataques de tipo Man-in-the-Middle (MitM), donde un hacker roba información confidencial espiando las comunicaciones entre dos objetivos en línea, como un usuario y una aplicación Web[9], por lo que, para estos mensajes es indispensable que se garantice la integridad de la información de extremo a extremo y por ende su trazabilidad, además, como fue señalado en la regulación sometida a consulta pública los operadores deben utilizar únicamente rutas y agregadores autorizados con el fin de cerrar la posibilidad de utilizar *"rutas grises"*.

Al respecto, a partir de la observación anterior, se nota la necesidad de homologar y brindar mayor claridad sobre la definición de trazabilidad. La trazabilidad de las comunicaciones debe entenderse como la capacidad del operador de identificar, autenticar, correlacionar y registrar de forma confiable el origen, la ruta de transmisión y el destino de cada comunicación, en cumplimiento con el Plan Nacional de Numeración y los esquemas autorizados de interconexión.

En mensajería SMS, un mensaje se considerará trazable cuando su origen pueda ser inequívocamente determinado y validado, ya sea como tráfico P2P asociado a un usuario final legítimo, correctamente autenticado en la red, o como tráfico A2P proveniente de un agregador, proveedor o entidad previamente registrado, validado y autorizado por el operador.

La trazabilidad implica, como mínimo, la verificación de la consistencia de la numeración de origen, la integridad de los parámetros de señalización, la validación de la ruta de entrada como puntos de interconexión, agregadores o proveedores internacionales, así como la correlación con registros de comunicaciones y perfiles de tráfico conocidos. Asimismo, el destino de la comunicación deberá corresponder a una numeración válida y coherente con el plan de numeración vigente.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o filtrar aquellos mensajes SMS cuya trazabilidad no pueda ser garantizada, incluyendo, entre otros, casos de manipulación o suplantación de identidad, incongruencias en la señalización, rutas de origen no autorizadas, ausencia de registro o validación del emisor A2P, o imposibilidad de asociar el tráfico a un usuario o entidad legítima. Estas medidas podrán implementarse mediante mecanismos técnicos tales como firewalls SMS, sistemas

[8] https://www.cm.com/es-es/blog/a2p-mensajeria-fraude-y-prevencion/
[9] https://www.ibm.com/es-es/think/topics/man-in-the-middle

de reputación, análisis de patrones de tráfico y validaciones en tiempo real de señalización y numeración.

En el caso de los servicios de llamadas, se entenderá por trazabilidad la capacidad del operador de identificar y validar de forma confiable el origen, la ruta de señalización y el destino de cada comunicación, en concordancia con el Plan Nacional de Numeración y los acuerdos de interconexión vigentes. Una llamada se considerará trazable cuando el identificador de origen pueda ser verificado como perteneciente a un usuario legítimo o a una entidad autorizada, y cuando la ruta de entrada y los parámetros de señalización sean consistentes y no presenten indicios de manipulación o suplantación.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o etiquetar aquellas llamadas cuya trazabilidad no pueda ser garantizada, incluyendo casos de vishing, rutas internacionales no autorizadas o inconsistencias en la señalización, mediante el uso de mecanismos técnicos como validación de identidad de origen, análisis de patrones de tráfico y controles en puntos de interconexión.

Por lo anterior, se recomienda acoger parcialmente esta observación con el fin de incorporar un apartado sobre la definición de trazabilidad en la resolución que se emita a partir de este informe, con el objetivo de brindar mayor claridad y comprensión sobre este término.

Por otro parte, sobre el **punto 9** respecto a contar con un firewall de SMS con capacidad de traducir y analizar automáticamente mensajes en formato binario y cualquier otro formato técnico de codificación aplicable a los servicios de mensajería móvil que puedan utilizarse para instalar malware u otras amenazas en los dispositivos de los usuarios finales, es importante aclarar que, los mensajes en estos tipos de formatos no se deben bloquear por el hecho de no entender el contenido del mensaje con información inteligible, sino por el riesgo que estos representan. Como se indicó en la regulación sometida a consulta pública, se requiere que los operadores cuenten con sistemas de firewall de SMS con capacidad de analizar mensajes binarios en busca de amenazas, de modo que, no se está imponiendo a los operadores que bloqueen los mensajes con información inteligible, sino que bloqueen únicamente los mensajes identificados como maliciosos, de modo que, se recomienda rechazar esta observación.

Con respecto al **punto 10** sobre las acciones que deben realizar los operadores ante la detección de ráfagas de spam (Spam Burst) e identificación de campañas de smishing, los operadores como responsables de su infraestructura deben investigar los comportamientos anómalos y proceder según las disposiciones del Reglamento sobre el Régimen de Protección al Usuario Final en aquellos casos donde se compruebe la comisión de prácticas prohibidas por parte de usuarios que generen tráfico malicioso, asimismo, como se indicó en el informe sometido a consulta pública, los operadores deben identificar en los mensajes patrones, malwares o enlaces fraudulentos, que permitan catalogarlos como maliciosos para su correspondiente bloqueo. Asimismo, sobre la posibilidad de falsos positivos o falsos negativos en la detección de ráfagas de spam (Spam Burst) e identificación de campañas de smishing, como se indicó anteriormente, le corresponde al operador investigar los casos donde se sospeche de la comisión de prácticas prohibidas por parte de sus clientes, de

modo que, dicha investigación debe determinar si los suscriptores de los servicios investigados y asociados a ráfagas de spam (Spam Burst) o campañas de smishing están incurriendo en prácticas prohibidas, al remitir mensajes con contenido malicioso o que atente contra la seguridad de otros usuarios, en cuyo caso debe proceder conforme el citado reglamento, de modo que, se recomienda rechazar esta observación.

Sobre la consulta planteada en el **punto 11** respecto al análisis de simetría en las comunicaciones para identificar servicios que generan grandes cantidades de comunicaciones, pero nunca reciben respuesta, CallMyWay NY S.A. (Call My Way) solicitó: *"(…) se indique en que casos mensajes unidireccionales deban ser considerados spam o malware, ya que contamos con clientes cuyo patrón es de solo envío de mensajes, como por ejemplo los bancos con claves de doble factor y no por ser unidireccionales se convierten en tráfico malicioso, spam o malware (…)"*. Al respecto, es importante mencionar que, la propuesta sometida a consulta pública requiere como una de las capacidades del firewall de SMS poder analizar la simetría de las comunicaciones identificando comportamientos correspondientes a bots, por lo que, no debe entenderse de forma incorrecta que la regulación en estudio disponga el bloqueo de todo el tráfico bajo este comportamiento. Como se indicó en el punto 9.3 inciso E. los operadores deben establecer registros de los clientes autorizados para enviar mensajes A2P, por lo que, basado en estos registros cada operador sabe cuáles clientes están autorizados a remitir grandes volúmenes de mensajes sin recibir respuestas, por lo que, al ser un usuario autorizado bajo una relación contractual con el operador no corresponde su investigación y posible bloqueo, de modo que, se recomienda rechazar esta observación.

En cuanto a la consulta **número 12** sobre los sistemas de reputación de enlaces para bloquear mensajes que contengan enlaces maliciosos o de dudosa procedencia, estos funcionan asignando una puntuación basada en factores como la antigüedad del sitio Web, cambios de ubicación históricos y los indicios de actividades sospechosas detectadas mediante el análisis del comportamiento del malware o del contenido del sitio Web[10]. Asimismo, existen gran variedad de librerías con enlaces maliciosos identificados o sitios Web donde cualquier usuario puede consultar si un enlace especifico es malicioso, sin embargo, por el principio de neutralidad tecnología, le corresponde a cada operador utilizar los sistemas de reputación de enlaces que mejor se ajusten a su infraestructura. Se recomienda rechazar esta observación.

Sobre lo indicado en el **punto 13** respecto a que en la presente actualización regulatoria se incluya la regulación que permite a los operadores realizar Inspección Profunda de Paquetes (DPI) en la totalidad del tráfico de mensajes SMS, resulta redundante e incoherente dicha solicitud, dado que, la regulación propuesta es la que habilitaría a los operadores a realizar Inspección Profunda de Paquetes (DPI) para la detección de smishing, de modo que esta observación ya estaría contenida en la propuesta regulatoria.

Respecto de lo solicitado en el **punto 14** sobre la forma de evaluar el éxito o fracaso de cada una de las medidas ordenadas para minimizar el impacto de los ataques tipo vishing, en coherencia con los reportes solicitados mediante la resolución RCS-294-2023 sobre bloqueo de llamadas enmascaradas, los cuales son remitidos por los operadores de forma

[10] https://docs.trendmicro.com/en-us/documentation/article/trend-micro-web-security-online-help-about-web-reputation

cuatrimestral, es correcto que los reportes relacionados a la cantidad de llamadas identificadas como vishing y sus respectivos bloqueos se realice de la misma forma, por lo que, estos deberán ser remitidos por cuatrimestre, de la misma forma que se requirió en la resolución RCS-294-2023, con lo que, se podrá medir el éxito del conjunto de medidas planteadas en la regulación propuesta, y no se evaluarán dichas medidas de forma separada. Adicionalmente, en este punto el operador solicitó se indique la tasa actual de llamadas tipo vishing, no obstante, esta información no ha sido recopilada, ya que, dicha estadística sería posible hasta la puesta en operación de los sistemas contra vishing que plantea la presente propuesta regulatoria. Por lo anterior, se recomienda rechazar estas observaciones.

Respecto de lo solicitado en el **punto 15** sobre que la única medida para la prevención de ataques de vishing sea el procesamiento masivo de registros de llamadas (CDRs) para trazabilidad de las comunicaciones, es importante mencionar que, el objetivo de la regulación propuesta es cerrar la mayor cantidad de brechas de seguridad que permitan que este tipo de ataques lleguen hasta los usuarios, por lo que, la implementación de una única medida no es consistente con el objetivo de esta actualización regulatoria, ya que, es bien conocido que los atacantes no utilizan un único método de ataque, sino que, aprovechan todos los recursos a su alcance, así como nuevas tecnologías en el mercado, de modo que, contrario a lo solicitado por el operador, la regulación sometida a consulta pública debe abarcar la mayor cantidad de escenarios y proponer medias de prevención robustas y ajustadas a las tecnologías emergentes, máxime considerando la rapidez de reacción de los atacantes, por lo que, se recomienda el rechazo de la solicitud de este operador.

Sobre la petitoria del **punto 16** respecto a cómo los operadores deben analizar la información de señalización obtenida de las comunicaciones, de la misma forma que se indicó anteriormente sobre la validación del origen de mensajes SMS, la información de señalización en las comunicaciones de voz permite conocer detalles sobre el origen de la comunicación, permitiendo así analizar la coherencia entre la red de origen de la llamada, la ruta de interconexión por la que ingresa y el operador correspondiente, o si la llamada ingresó por una ruta autorizada, en el caso de comunicaciones internacionales. Esto con el fin de cerrar la posibilidad de utilizar rutas grises, siendo que, la red de origen de la llamada debe coincidir con la ruta interconexión y su respectivo operador, y utilizar únicamente rutas oficiales y autorizadas. Por lo anterior, se recomienda rechazar esta observación.

En relación con lo requerido en el **punto 17** sobre que la detección de patrones de comportamiento sospechoso como frecuencia de llamadas, tasa de conexiones exitosas, duración de las llamadas, duración de tonos, estadísticas de llamadas entre otros, se consideren medidas suficientes para minimizar las llamadas maliciosas, al igual que se respondió para la observación del punto 15, el objetivo principal de la regulación propuesta es abarcar la mayor cantidad de escenarios ya conocidos que facilitan los casos de smishing y vishing, por lo que, se requiere de medias de prevención robustas, complementarias y ajustadas a las nuevas tecnologías que están al alcance de los atacantes, por lo que, se recomienda el rechazo de esta petición.

San José, 12 de junio 2026
05772-SUTEL-DGM-2026

Con respecto a la solicitud del **punto 18** sobre método de identificación de robollamadas o robocalls, si bien la regulación propuesta no impone un método especifico como los mencionados por CallMyWay NY S.A. (Call My Way) *"(…) en tiempo real mediante derivación del tráfico y análisis instantáneo o retrospectivamente mediante grabación de las llamadas para su posterior análisis. (…)"*, es importante señalar que, este requerimiento planteado en la regulación propuesta corresponde a una capacidad mínima que deben tener los sistemas de firewall de voz de los operadores, específicamente identificación de llamadas automatizadas que utilizan grabaciones de voz o voz sintética (robollamadas o robocalls), sin embargo, es claro que un análisis en tiempo real contribuirá en mayor medida a proteger a los usuarios de posibles casos de vishing, siendo que, este tipo de llamadas serán identificadas con mayor rapidez, de modo que, se recomienda utilizar un método de identificación en tiempo real, ya que este puede brindar mayor efectividad en cuanto al objetivo que busca la propuesta de regulación, sin embargo, respetando el principio de neutralidad tecnológica, le corresponde a cada operador seleccionar las tecnologías que mejor se ajusten a su infraestructura para cumplir con los requerimientos de la actualización regulatoria. En cuanto a indicar la Inteligencia Artificial a utilizar para esta tarea, como se ha mencionado anteriormente, con base en el principio de neutralidad tecnológica, Sutel no tiene la potestad para imponer un modelo especifico, siendo que, los operadores cuentan con la discreción de implementar las medidas técnicas idóneas para garantizar la seguridad de las redes y sus servicios que mejor se ajusten a su infraestructura y presupuesto.

Asimismo, respecto al análisis de grabaciones, conforme el principio de neutralidad tecnológica es decisión de cada operador y proveedor seleccionar la herramienta que mejor se ajuste a su infraestructura y presupuesto, siempre y cuando, le permita cumplir a cabalidad con la propuesta regulatoria. Además, cabe señalar que, las herramientas de seguridad propuestas no implican la intervención de terceros, ya que, un análisis de llamadas mediante sistemas informáticos apoyados con Inteligencia Artificial para filtrar comunicaciones maliciosas no implica la intervención de un tercero ni el acceso indiscriminado a las comunicaciones por parte de un humano, de modo que, se recomienda rechazar esta observación.

Finalmente, sobre el requerimiento de un análisis del efecto que va a tener en los usuarios sobre la aplicación de medidas como Inspección Profunda de Paquetes (DPI) y Procesamiento de Lenguaje Natural (NLP), es importante, aclarar que, estos mecanismos no atentan contra la privacidad de las comunicaciones de los usuarios, por el contrario, buscan protegerlos, ya que, estos mecanismos no implican la intervención de un humano para la lectura de los mensajes ni un acceso indiscriminado al contenido de estos por parte de humanos, sino que, corresponden a procesos automatizados, ejecutados por sistemas informáticos diseñados específicamente para identificar patrones previamente definidos asociados a conductas irregulares, como enlaces maliciosos, estructuras y firmas digitales conocidas típicas de smishing. Este análisis se limita a elementos estrictamente necesarios para detectar amenazas en enlaces maliciosos o patrones sintácticos, y no se realiza almacenamiento permanente del contenido de los mensajes, ya que, el análisis se realiza en tiempo real y con fines exclusivos de ciberseguridad, garantizando la destrucción de los datos una vez cumplan su cometido con el sistema de firewall.

Por lo anterior, el uso de DPI o NLP para la detección de smishing, cuando se implementa bajo principios de privacidad, transparencia y proporcionalidad, no constituye una vulneración a la privacidad de los usuarios, sino una herramienta legítima y necesaria para su protección en el entorno digital actual, tomando en cuenta el nivel de intrusión mínimo al no involucrar intervención humana ni almacenamiento del contenido, y a su vez, ajustarse a los preceptos del artículo 42 de la Ley General de Telecomunicaciones que dispone que los operadores y proveedores deben adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. Además, la Unión Internacional de Telecomunicaciones (UIT) mediante sus recomendaciones ITU-T X.1247 y ITU-T X.1245 promueven utilizar mecanismos adaptativos de análisis de contenido en tiempo real, como las funciones APr y CAS establecidas en dichas especificaciones respectivamente. Por lo anterior, se recomienda el rechazo de esta observación.

Respecto de lo solicitado en el **punto 19** sobre la implementación del estándar Out-of-Band SHAKEN (OOBS) para autenticación de todas las llamadas, el operador cuestiona cuál será la entidad encargada de emitir certificados y facilitar las firmas digitales. Es importante aclarar que dicho estándar no requiere necesariamente la creación de una entidad única centralizada a nivel nacional para la emisión de certificados, sino que, la certificación puede ser realizada por una o varias Autoridades de Certificación que cumplan con estándares internacionales y sean reconocidas mutuamente dentro del ecosistema de operadores. En este contexto, los operadores no deben depender de una única entidad nacional para obtener sus certificados, sino que pueden acudir a certificadores que cumplan con los requisitos técnicos y de validación definidos para este estándar. Lo fundamental es que dichos certificadores verifiquen de manera rigurosa la identidad del operador y su derecho de uso sobre los recursos de numeración que pretende firmar.

Asimismo, la facilitación de firmas digitales no constituye un servicio externo independiente, sino una capacidad intrínseca de cada operador, habilitada mediante los certificados emitidos por las Autoridades de Certificación. La implementación de OOBS no depende de la designación previa de una entidad certificadora específica, sino de la adopción coordinada de un modelo de confianza interoperable entre operadores. La certificación y provisión de firmas digitales en el contexto de OOBS puede ser gestionada mediante un modelo distribuido de Autoridades de Certificación reconocidas, donde los operadores asumen un rol activo en la generación de firmas, sin que ello requiera la creación de una única entidad certificadora nacional como condición previa para su implementación.

Por otra parte, sobre la solicitud de un estudio de muestreo previo con operadores para determinar la factibilidad, tiempos y costos de implementación del estándar Out-of-Band SHAKEN (OOBS), cabe señalar que, esta solicitud no es consistente con el principio de neutralidad tecnológica dispuesto en la Ley N°8642 Ley General de Telecomunicaciones, el cual, implica que los operadores son responsables de seleccionar, implementar y desarrollar las soluciones técnicas que les permitan cumplir con sus obligaciones regulatorias. En todo caso, debe considerarse la urgencia de adoptar medidas que permitan mitigar la situación de alto riesgo en que se encuentran los usuarios de las redes de telecomunicaciones nacionales dada la tendencia de aumento en ataques de vishing y smishing que se ha registrado.

Es importante mencionar que, la obligación relevante no es la adopción de una tecnología específica en términos de implementación, sino el cumplimiento de un objetivo funcional, que corresponde a la autenticación confiable de la identidad del origen de las llamadas. El estándar OOBS es reconocido para cumplir este objetivo, sin embrago, su implementación puede materializarse de diversas formas según la arquitectura de cada operador.

Cada operador cuenta con conocimiento detallado de su propia red e infraestructura que le permiten evaluar internamente la mejor estrategia de implementación y los costos correspondientes.

Cabe indicar que, OOBS ha sido diseñado precisamente para operar en entornos heterogéneos, incluyendo redes modernas y heredadas, así como escenarios donde la señalización no es completamente confiable de extremo a extremo. Esto reduce significativamente las barreras de entrada para su implementación, ya que, no exige transformaciones estructurales completas de la red, sino la incorporación de capacidades específicas de firma y verificación.

Respecto a los tiempos de implementación, estos dependen directamente del grado de madurez tecnológica de cada operador, su infraestructura existente y sus decisiones de priorización interna. Cabe señalar que, únicamente un operador presentó una propuesta de cronograma gradual de implementación para OOBS, según se amplía más adelante en este informe, el cual contempla un plazo de 540 días (18 meses) para la puesta en operación de estas capacidades, por lo que, al ser la única manifestación específica para implementar este requerimiento se recomienda aceptar dicho plazo.

La mitigación de prácticas prohibidas, la protección de los usuarios, la seguridad de la red y la preservación de la integridad del servicio son responsabilidades inherentes a la actividad de los operadores, por lo que, los costos asociados a la implementación de mecanismos de autenticación forman parte de las inversiones necesarias para la operación de redes seguras y confiables. Cada operador debe asumir estos costos como parte de su modelo de negocio y de su obligación de garantizar la calidad y seguridad del servicio.

Cabe señalar que la implementación de Out-of-Band SHAKEN (OOBS), busca la coexistencia de diversas tecnologías para la generación de comunicaciones como se presenta en el mercado costarricense, donde no todas las comunicaciones aplican el protocolo SIP extremo a extremo, lo que permite la coexistencia entre tecnologías del servicio telefónico de voz y a su vez brinda los beneficios de autenticación del protocolo inicial STIR/SHAKEN. No está de más señalar que el OOBSS es técnicamente sólida, madura y adecuada para tal fin, siendo que, no se cuenta con alternativas similares que permitan esta coexistencia.

En cuanto al trato de llamadas internacionales provenientes de redes que no cuentan con el estándar OOBS, esto no debe interpretarse como una limitante para la adopción del estándar a nivel local, ni como una justificación para retrasar su implementación, por el contrario, refuerza la necesidad de que los operadores que sí implementan el estándar OOBS adopten criterios claros de tratamiento de tráfico no autenticado.

En este sentido, las llamadas internacionales sin autenticación OOBS deben ser tratadas explícitamente como tráfico no verificado. Esto implica que, en ausencia de un certificado válido OOBS, el operador que recibe la comunicación no cuenta con garantías sobre la legitimidad del identificador de origen, por lo que, dichas llamadas deben ser sujetas a medidas de gestión de riesgo como, clasificar dichas llamadas como no autenticadas o de bajo nivel de confianza, aplicar análisis preventivo (detección de patrones dudosos o irregulares, reputación de origen, volúmenes de tráfico anómalo), agregar etiquetas para advertir al usuarios sobre una llamada internacional no verificada o priorizar su monitoreo o bloqueo en casos de comportamientos sospechosos.

En ese sentido, no todas las llamadas deben ser bloqueadas por no contar con OOBS, pero aquellas que no pueden ser autenticadas deben ser tratadas con un nivel de desconfianza proporcional al riesgo que representan, de acuerdo con los análisis de tráfico realizados.

Cabe señalar que, el análisis de tráfico ya se encuentra definido de forma análoga en el artículo 65 del Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF), a nivel de tráfico telefónico excesivo, donde se dispuso el bloqueo del tráfico cuando se determine un consumo atípico mediante la verificación de la frecuencia, duración, volumen, horarios o destinos identificados de alto riesgo, según la experiencia del operador/proveedor o mejores prácticas internacionales de prevención.

Es importante destacar que este estándar no exige una adopción global simultánea para su correcto funcionamiento, sino que, su efectividad aumenta progresivamente conforme más operadores implementan esta autenticación, permitiendo distinguir de manera cada vez más clara entre tráfico confiable y no confiable. Por lo tanto, la existencia de tráfico internacional no autenticado no representa un impedimento técnico ni operativo para la implementación de OOBS por parte de los operadores. Al contrario, mantener redes sin autenticación frente a un entorno internacional cambiante incrementa la probabilidad de ataque y debilita la capacidad de proteger a los usuarios.

Por lo anterior, es responsabilidad de cada operador implementar mecanismos que le permitan gestionar adecuadamente este tráfico, integrando el estándar OOBS con sistemas de análisis antifraude, así como reputación y control de llamadas. La adopción de este estándar establece un piso mínimo de confianza para el tráfico nacional y permite introducir gradualmente incentivos para que el tráfico internacional evolucione hacia esquemas de autenticación equivalentes.

Así las cosas, las llamadas internacionales provenientes de redes sin OOBS deben ser aceptadas bajo un esquema de no autenticadas y gestionadas en función de su riesgo, sin que ello retrase o condicione la implementación de este estándar por parte de los operadores.

Respecto a que, la RCS-294-2023 ya cubre el tema de la suplantación de identidad para llamadas, es importante mencionar que, dicha normativa contempla únicamente el escenario de suplantación de identidad mediante enmascaramiento de llamadas, sin embargo, esto no significa que dicho método sea el único utilizado por los ciberdelincuentes

para cometer prácticas irregulares, por el contrario, los ciberdelincuentes aprovechan todos los métodos a su disposición para lograr sus objetivos y obtener información sensible de los usuarios, por lo que, señalar que las medidas establecidas en la resolución RCS-294-2013 son suficientes es incorrecto, ya que, deja abiertas otras brechas que pueden ser aprovechadas por los delincuentes, además, la implementación de este estándar no sustituye las disposiciones de esta regulación, sino que, busca complementar y fortalecer las medidas ya impuestas.

En lo que respecta a la solicitud de indicar la utilidad de implementar OOBS cuando la totalidad de las interconexiones en Costa Rica se ejecutan mediante el protocolo SIP, si bien es cierto que este protocolo permite el uso de mecanismos de autenticación, esto no garantiza por sí mismo la integridad de la identidad de origen a lo largo de toda la cadena de señalización, ya que, incluso en redes completamente interconectadas mediante este protocolo, existen escenarios donde la información de identidad puede perderse, degradarse o ser manipulada, como lo es en interconexiones indirectas a través de múltiples operadores, pasarelas que se interconectan con redes heredadas, incluso fuera del ámbito nacional, o equipos intermedios que no mantienen encabezados SIP de identidad.

En estos casos, mecanismos como el encabezado de identidad SIP pueden no ser confiables o incluso no estar presentes al momento de la terminación de la llamada. Es precisamente en este contexto donde OOBS aporta valor, al permitir que la información de autenticación viaje por un canal independiente de la señalización SIP.

Asimismo, cabe señalar que, el estándar OOBS no compite o reemplaza la autenticación SIP, sino que lo complementa y lo refuerza, ya que, OOBS garantiza la verificación de la identidad incluso cuando la señalización SIP ha sido modificada en el tránsito, y permite la autenticación en entornos heterogéneos donde coexisten redes modernas y heredadas. Asumir que un entorno SIP elimina la necesidad del estándar OOBS implica no contemplar que, la suplantación de identidad no depende del protocolo de transporte, sino de la falta de mecanismos de validación de identidad confiables de extremo a extremo.

De modo que, limitar la implementación a únicamente mecanismos como el protocolo SIP introduce una fragilidad estructural en la cadena de transporte, ya que, basta con que un único elemento en la cadena no soporte o preserve correctamente la información SIP para que se pierda la capacidad de autenticación, por lo que, OOBS elimina esta dependencia, proporcionando un mecanismo robusto y verificable independientemente de la integridad de la señalización. La implementación de OOBS no solo mantiene su utilidad en entornos SIP, sino que resulta altamente funcional como mecanismo complementario para garantizar la autenticación de llamadas en condiciones reales de operación, donde existen múltiples dominios y tecnologías, además, permite establecer un esquema de autenticación resiliente, preparado para escenarios mixtos y evolución futura de la red, evitando soluciones parciales que pueden ser fácilmente evadidas por ciberdelincuentes. Por lo anterior, se recomienda rechazar esta petición.

Sobre la petitoria del **punto 20** respecto al plazo otorgado inicialmente de 180 días, con base en esta petitoria y otras que serán analizadas más adelante en este informe, es que esta Superintendencia se encuentra anuente a establecer un cronograma escalonado para la implementación de la totalidad de capacidades solicitadas en la regulación sometida a consulta pública, iniciando con un plazo de 180 días para implementar medidas que únicamente requieran de configuraciones y ajustes básicos en su infraestructura, y gradualmente ir incluyendo capacidades de Inteligencia Artificial y análisis en tiempo real, tanto en mensajería SMS como en llamadas de voz, según se detalla más adelante. Por lo anterior, se recomienda acoger esta petición respecto a ajustar el plazo de implementación.

Respecto a la solicitud de conocer las dificultades que tuvo la Federal Communications Commission (FCC) en cuanto a implementar el estándar STIR/SHAKEN en los Estados Unidos, es importante mencionar que, si bien este escenario otorgó lecciones valiosas que deben ser tomadas en consideración, no deben verse como una justificación para retrasar o impedir su adopción, sino como elementos que han sido precisamente abordados y mitigados mediante la evolución de este estándar, por lo que, utilizar las dificultades iniciales de la implementación en Estados Unidos como argumento para postergar la adopción del estándar OOBS carece de sustento técnico. Al contrario, dichas experiencias han permitido madurar el estándar y definir mejores prácticas que facilitan su implementación en otros mercados. Las lecciones aprendidas en cuanto al proceso liderado por la FCC refuerzan la necesidad de implementar mecanismos de autenticación de llamadas de manera obligatoria y consistente. La incorporación de OOBS permite precisamente superar las limitaciones identificadas, evitando repetir los mismos desafíos y acelerando la efectividad del sistema en la mitigación del fraude telefónico. Por lo anterior, se recomienda rechazar esta petición.

Finalmente, respecto a la petitoria **número 21** sobre indicar la frecuencia de remisión de reportes con información de la cantidad de mensajes SMS bloqueados, esta Superintendencia considera que dicha información representa gran valor para el análisis de la efectividad y alcance de las medidas impuestas en la regulación sometida a consulta pública, por lo que, en coherencia con los reportes solicitados mediante la resolución RCS-294-2023 sobre bloqueo de llamadas enmascaradas, los cuales son remitidos por los operadores de forma cuatrimestral, es apropiado que los reportes relacionados a la cantidad de mensajes SMS bloqueados se realice de la misma forma, por lo que, estos deberán ser remitidos por cuatrimestre, de la misma forma que se requirió en la resolución RCS-294-2023.

Si bien este operador propone que los informes sean presentados de forma anual, es importante mencionar que, recibir un informe cuatrimestral amplia las capacidades de análisis y permite disponer de resultados recientes, en lugar de esperar un año para conocer nuevos resultados que permitan implementar oportunamente acciones correctivas. Por lo que, se recomienda acoger parcialmente esta observación.

Así las cosas, del análisis anterior se recomienda acoger la solicitud realizada en los puntos 1 y 3 respecto a incluir y reforzar el fundamento jurídico que motiva la aplicación de las

medidas dispuestas en la regulación sometida a consulta pública y habilita a los operadores a tomar acciones al respecto.

Por otro lado, las consultas realizadas por CallMyWay NY S.A. (Call My Way) sobre la validación del Título Global y la verificación en tiempo real del origen del mensaje demuestran la necesidad de homologar y brindar mayor claridad sobre la definición de trazabilidad por lo que, se recomienda acoger parcialmente esta observación.

Además, se recomienda acoger parcialmente lo requerido por CallMyWay NY S.A. (Call My Way) respecto a requerir a todos los operadores de mensajería SMS la inclusión del comprobante de entrega y recepción de mensaje SMS, ya que es una configuración necesaria para el éxito de la presente propuesta regulatoria y su coordinación entre operadores.

Además, se recomienda acoger parcialmente las observación respecto a indicar la frecuencia de remisión de reportes, de modo que, igual como fue requerido en la resolución RCS-294-2023, se incluya en la resolución que se emita el deber de los operadores de telefonía sobre aportar un informe de forma cuatrimestral, con la cantidad de llamadas identificadas como vishing y sus respectivos bloqueos, y de igual manera, los operadores de mensajería SMS deben presentar un informe de forma cuatrimestral sobre la cantidad de mensajes SMS identificados como maliciosos y sus respectivos bloqueos.

En cuanto a las observaciones restantes, se recomienda su rechazo con base en los puntos analizados anteriormente.

3.2. Posición de Mitto AG:

Mediante la respuesta remitida el 24 de abril de 2026 (NI-05496-2026) Mitto AG por medio del señor Andrea Giacomini, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
3. Propuesta: una estrategia a nivel país mediante un Gateway Nacional A2P
Con base en el análisis precedente, Mitto AG propone que Costa Rica considere complementar el marco regulatorio propuesto en el numeral 9 del oficio con el establecimiento de un Gateway Nacional de SMS A2P, bajo la coordinación de la SUTEL como ente regulador competente.

Este modelo no sustituye las obligaciones de los operadores descritas en el oficio; las hace más efectivas, uniformes y auditables. Su lógica central es la siguiente: en lugar de requerir que cada operador construya y opere de forma independiente sus propios sistemas de control, se establece un punto nacional único de gestión del tráfico A2P internacional, desde el cual se aplican de manera centralizada todas las funciones de seguridad, autenticación, filtrado y visibilidad que el propio oficio de la SUTEL ya identifica como necesarias. Este enfoque garantiza además condiciones de acceso equitativas para todos los operadores del mercado, eliminando asimetrías que en otros mercados han derivado en distorsiones competitivas.

Un aspecto central de este modelo es que preserva y fortalece la soberanía del ente regulador sobre el tráfico de telecomunicaciones en el país. El Gateway Nacional no transfiere poder de decisión a ningún actor privado ni a ningún operador en particular; al contrario, sitúa a la SUTEL en la posición de garante activo de las condiciones del mercado y de la soberanía digital del Estado costarricense. Es el Estado quien define las reglas

de acceso, los criterios de autenticación, los estándares de seguridad y los términos de participación de todos los actores. Esta arquitectura de gobernanza es precisamente lo que distingue al modelo de un simple acuerdo comercial entre operadores: es una política pública de gestión del tráfico digital, con el interés nacional como objetivo central (…)"

Las observaciones a la propuesta presentadas por Mitto AG se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por Mitto AG se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.2.1. Análisis de las observaciones realizadas por Mitto AG:

Con respecto a la propuesta realizada por la empresa Mitto AG sobre la implementación de un gateway nacional para el tráfico de mensajes SMS A2P bajo la coordinación de la Sutel, como punto nacional único para la gestión del tráfico A2P internacional, si bien esta propuesta tiene sus puntos positivos en cuanto a la seguridad del tráfico de mensajes A2P internacionales, es importante mencionar que, la Unión Internacional de Telecomunicaciones (UIT) en su recomendación ITU-T X.1247 promueve que el marco metodológico contra el spam, en este caso smishing, debe basarse en diversas conexiones e interfaces entre múltiples dominios antispam descentralizados correspondiente a cada operador o proveedor que colaboran entre sí, y no mediante la imposición de un nodo nacional único.

Además, el objetivo de la regulación sometida a consulta pública es establecer las bases de un marco regulatorio robusto para la lucha contra el smishing y el vishing, y disponer a los operadores y proveedores de métodos y mecanismos para mejorar la seguridad de sus comunicaciones, por lo que, esta propuesta va más allá de los alcances de la regulación en consulta y requiere de valoraciones sobre elementos que aún no se han ponderado en nuestro país, justamente por la falta de una regulación base, que requiere información para analizar posibles nuevas estrategias para luchar contra el smishing y el vishing, por lo que, no estamos en el momento idóneo ni se cuenta con los datos necesarios para analizar una propuesta como la enunciada por Mitto AG, no obstante, se reconoce el valor de la citada propuesta para un análisis futuro.

Por lo anterior, se recomienda rechazar la propuesta realizada por Mitto AG al exceder el alcance de los análisis y requerimientos dispuestos en la regulación sometida a consulta pública.

3.3. Posición de Claro CR Telecomunicaciones S.A. (Claro):

Por medio del oficio RI-0168-2026 del 24 de abril de 2026 (NI-05526-2026) Claro CR Telecomunicaciones S.A. (Claro) por medio del señor Andrés Oviedo Guzmán, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
I. Consideraciones generales sobre proporcionalidad y gradualidad
(…)
Solicitamos que la SUTEL incorpore un análisis de impacto regulatorio que cuantifique los costos estimados de implementación para los operadores.

En este sentido, la experiencia internacional demuestra que la diferenciación tarifaria entre el tráfico A2P y el tráfico P2P constituye un mecanismo económico disuasorio de alta efectividad contra el envío masivo ilegítimo. Cuando las tarifas de interconexión para SMS son suficientemente bajas, como en el caso de Costa Rica, se crea un incentivo económico para que los remitentes de tráfico A2P utilicen rutas grises de interconexión en lugar de los canales autorizados de agregadores, dado que estos últimos aplican tarifas significativamente superiores. Un análisis de impacto regulatorio completo debería incluir la evaluación de mecanismos tarifarios como alternativa o complemento a las medidas puramente técnicas, ya que estos atacan la raíz económica del problema y pueden ser más efectivos y menos onerosos que la imposición simultánea de las 15 capacidades técnicas de firewall.
(…)
Solicitamos que la regulación incorpore un enfoque escalonado, comenzando por las medidas de mayor impacto y menor costo (registro de remitentes, validación de rutas, bloqueo de tráfico enmascarado) y dejando las medidas de mayor complejidad técnica (IA con NLP, DPI, geolocalización) como requisitos progresivos sujetos a evaluación de resultados.

(…)

Un análisis comparado de mejores prácticas internacionales permite identificar que los marcos regulatorios más exitosos contra el tráfico A2P malicioso no se limitan a medidas técnicas de detección e intervención en la red, sino que combinan al menos seis palancas complementarias: (A) identidad y autorización del remitente; (B) consentimiento, exclusión voluntaria y elección del consumidor (opt-in/opt-out); (C) restricciones de contenido y registro de campañas; (D) detección, integridad de enrutamiento e intervención técnica en la red; (E) mecanismos para reportes y reclamos de usuarios; y (F) precios alineados con el valor agregado del tráfico A2P. La mayor efectividad se logra combinando múltiples palancas tanto en la red de origen como en la de destino.
La propuesta de la SUTEL se concentra casi exclusivamente en la palanca D (detección e intervención técnica), sin abordar las palancas B (consentimiento y exclusión voluntaria del usuario), C (restricciones de contenido y aprobación previa de campañas) ni F (incentivos económicos y diferenciación tarifaria entre tráfico A2P y P2P). Esta concentración en la medida más costosa y técnicamente compleja, omitiendo herramientas complementarias de menor costo y alta efectividad comprobada. Solicitamos que la regulación adopte un enfoque integral que combine múltiples palancas de protección y no descanse exclusivamente en la intervención técnica en la red.

En particular, mecanismos de consentimiento expreso previo (opt-in) para la recepción de mensajes publicitarios, exclusión voluntaria mediante respuesta directa al remitente (opt-out, por ejemplo mediante palabras clave como "ALTO" o "BAJA"), y listas de no molestar con verificación obligatoria antes del envío, constituyen alternativas menos invasivas que la inspección profunda de todo el contenido de los mensajes. Colombia, que el propio documento de la SUTEL cita como referencia, complementa el bloqueo técnico con medidas de preferencia del usuario. La adopción de estos mecanismos reduciría la necesidad de DPI generalizada al permitir que los usuarios ejerzan control directo sobre los mensajes que reciben, protegiendo así tanto la privacidad como la autonomía del usuario final.

II. Observaciones sobre las medidas relativas a los servicios de mensajería SMS (secciones 9.1 a 9.4)

CLARO se encuentra actualmente en proceso de migración de su solución de firewall SMS a un proveedor. Según las funcionalidades documentadas, este firewall tiene la capacidad técnica de realizar los tipos de bloqueos descritos en la propuesta regulatoria; no obstante, se requiere confirmar con el proveedor si la plataforma cuenta con funcionalidad nativa de inteligencia artificial sobre el firewall SMS.
(…)

En consecuencia, la empresa solicita que la regulación permita un periodo de transición durante el cual los operadores que ya cuenten con firewalls con capacidades de bloqueo reactivo puedan continuar operando bajo ese esquema, mientras completan la incorporación de funcionalidades de IA, sin que ello constituya un incumplimiento sancionable. Asimismo, solicitamos que se establezca un mecanismo para que los operadores puedan acreditar ante la SUTEL el cumplimiento progresivo de las 15 capacidades mínimas de manera escalonada.

Proponemos que la SUTEL considere como alternativa estructural al firewall con 15 capacidades simultáneas el modelo de registro de campañas A2P implementado exitosamente en Estados Unidos a través de The Campaign Registry (TCR), establecido en 2020. Bajo este modelo, las empresas que desean enviar mensajes A2P deben registrar cada campaña, asociar un identificador a la misma y procesar sus mensajes a través de agregadores aprobados. Las empresas no registradas no pueden enviar mensajes A2P. Los operadores móviles utilizan los datos del registro para bloquear campañas no registradas y determinar volúmenes y tarifas según un "puntaje de confianza de marca". El resultado reportado fue que el spam a gran escala se volvió impráctico y los operadores pasaron de un modelo de "filtrado reactivo" a una "gestión proactiva del tráfico". Si bien la propuesta de la SUTEL ya contempla un registro de entidades A2P en la sección 9.3.E, un modelo de registro robusto de remitentes y campañas con aprobación previa del contenido puede ser más efectivo que un firewall con 15 capacidades de IA, dado que ataca el problema en el origen —quién envía y qué envía— y no solo en el tránsito. Solicitamos que la SUTEL evalúe la adopción de un modelo de registro de campañas similar como medida prioritaria y escalonada, complementaria a las capacidades técnicas más complejas.

5. Sobre la inspección profunda de paquetes (DPI) y la protección de la privacidad (sección 9.1.E)
(…)
Como alternativa complementaria a la DPI generalizada, se propone la implementación de modelos de aprobación previa de contenido. Bajo este esquema, los remitentes A2P registrados someten plantillas de contenido que el operador valida previamente; en tiempo real, el sistema verifica la coincidencia del mensaje enviado con las plantillas autorizadas, sin necesidad de inspeccionar el contenido sustantivo de cada mensaje. Esta alternativa protege la privacidad del usuario al eliminar la necesidad de lectura del contenido y resulta más eficiente operativamente. La combinación de un registro robusto de remitentes con aprobación previa de plantillas y mecanismos de consentimiento y exclusión voluntaria (opt-in/opt-out) permitiría limitar la DPI exclusivamente al tráfico no registrado o no autorizado, reduciendo significativamente el volumen de mensajes sujetos a inspección profunda y, con ello, los riesgos de privacidad asociados.

6. Sobre los canales de atención al usuario para reporte de SPAM
(…)
Manifestamos nuestra disposición a establecer canales de atención al cliente para que los usuarios reporten tráfico SPAM. No obstante, la implementación de esta logística requiere una coordinación interna significativa entre las áreas de Servicio al Cliente (SAC) y Sistemas para definir los canales adecuados (portales web, aplicaciones, líneas telefónicas u otros medios), los flujos de atención y los mecanismos de retroalimentación al sistema de filtrado. Solicitamos que la regulación establezca lineamientos generales sobre los canales aceptables, dejando la definición de la logística específica a cada operador según su estructura y capacidad operativa, y que se otorgue un plazo diferenciado para la puesta en marcha de estos canales.

En relación con lo anterior y asociado a la recomendación UIT-T X.1242, las configuraciones de reglas por usuario pueden ser muy complejas de controlar y de operar en el respectivo equipo, por lo que se sugiere que al igual que en el caso anterior se establezcan lineamientos generales de forma tal que sea el operador de acuerdo a sus capacidades operativas quien pueda implementar las reglas.

7. Sobre el intercambio de información entre operadores
(…)
Coincidimos con la importancia de la colaboración interoperador. Sin embargo, los mecanismos concretos para compartir información entre operadores deben ser validados tanto con la SUTEL como con las áreas de interconexión de los distintos operadores, a fin de establecer el canal correcto de comunicación, los protocolos de intercambio de datos, las responsabilidades de cada parte y los procedimientos aplicables, todo ello en cumplimiento de la normativa de protección de datos personales. Solicitamos que la SUTEL facilite la definición

de estos protocolos de colaboración, estableciendo un marco de referencia claro que evite conflictos entre operadores y garantice el cumplimiento de la Ley N°8968.

8. Sobre el análisis de simetría y bloqueo de tráfico A2P sin respuesta (sección 9.1.C, numeral 13)
(…)
Observamos que este criterio debe aplicarse con cautela y excepciones claramente definidas, dado que existen múltiples escenarios legítimos en los que el tráfico A2P es unidireccional por naturaleza y no genera respuesta del usuario receptor. Entre estos se encuentran:

- *Mensajes de autenticación de dos factores (2FA) y contraseñas de un solo uso (OTP) enviados por instituciones bancarias y financieras.*
- *Notificaciones transaccionales (confirmaciones de compra, alertas de movimiento en cuenta, avisos de entrega).*
- *Comunicaciones informativas de entidades gubernamentales.*
- *Alertas de seguridad de plataformas tecnológicas.*
- *Recordatorios de citas médicas, vencimiento de servicios u otros avisos automatizados.*

En todos estos casos, la empresa que envía la información actúa mediante un servicio unidireccional legítimo, y la falta de respuesta del usuario no constituye un indicador de comportamiento malicioso ni de actividad de bots. Bloquear este tráfico basándose únicamente en la ausencia de respuesta podría afectar gravemente servicios esenciales para los usuarios finales y generar reclamos masivos ante la SUTEL, vulnerando los derechos de los usuarios que el artículo 45 de la Ley N°8642 protege.

Solicitamos que la regulación incorpore una lista de excepciones para el análisis de simetría, de manera que el tráfico A2P legítimo proveniente de entidades registradas ante el operador (conforme al registro previsto en la sección 9.3.E de la propuesta) no sea objeto de bloqueo por el solo hecho de no generar respuesta del usuario destinatario.

9. Sobre el control de tráfico multimedia IP (recomendación ITU-T X.1244)
(…)
Creemos que algunos de los estándares citados hacen referencia directa a internet o la red IP en general, lo cual excede el ámbito objetivo de la presente regulación, cuyo propósito declarado es la seguridad en los servicios de voz y mensajería SMS. El control de tráfico multimedia IP involucra servicios y protocolos sustancialmente distintos a los de telefonía y SMS, con implicaciones técnicas, económicas y de privacidad diferenciadas.

Solicitamos que la regulación delimite con mayor precisión su ámbito de aplicación, excluyendo expresamente el tráfico multimedia IP de las obligaciones contenidas en esta actualización regulatoria, o bien, que se trate este tema de manera separada en un instrumento regulatorio específico que aborde adecuadamente su complejidad particular.

10. Sobre la socialización de obligaciones a los agregadores de SMS
(…)
Consideramos indispensable que, una vez aprobada la regulación definitiva, la SUTEL establezca un proceso formal de socialización con los agregadores de SMS que operan en el mercado costarricense, a fin de que estos puedan adecuar sus sistemas y filtros conforme a los nuevos requerimientos. La eficacia de las medidas de trazabilidad depende en gran medida de que toda la cadena de transporte del mensaje cumpla con los requisitos de identificación y control, y los agregadores constituyen un eslabón crítico en esa cadena.

En este contexto, la experiencia internacional demuestra que los agregadores frecuentemente implementan controles de seguridad más robustos que los disponibles por interconexión directa, incluyendo validación de identidad del remitente, registro de empresas emisoras, trazabilidad completa de mensajes y filtros antifraude propios. La regulación debería reconocer y aprovechar estos controles existentes, diferenciando las obligaciones según el canal de ingreso del tráfico A2P: los mensajes que ingresan a través de agregadores

autorizados con controles acreditados deberían estar sujetos a requisitos de filtrado menos intensivos que el tráfico que ingresa por interconexión directa sin garantías de trazabilidad. Asimismo, la implementación de un modelo de registro de campañas como el descrito en el punto 5 de estas observaciones facilitaría la labor de los agregadores al establecer un marco uniforme de requisitos para los remitentes.

11. Sobre la participación del equipo de auditoría y fraudes
Sugerimos, como buena práctica interna, que la regulación contemple expresamente la necesidad de que los operadores involucren a sus áreas de auditoría y prevención de fraudes en la gestión de los firewalls de SMS. Estos equipos son los que actualmente tienen documentadas las reglas del firewall SMS y poseen mayor experiencia en la identificación y bloqueo de rutas grises. Su participación desde la fase de diseño y configuración del sistema es esencial para garantizar la eficacia de las medidas.

III. Observaciones sobre las medidas relativas a los servicios de llamadas de voz (sección 9.5)

12. Sobre el procesamiento masivo de registros de llamadas CDR (sección 9.5.A, literal a)
(…) la propuesta no indica un límite de tiempo para el resguardo de estos registros. La ausencia de un plazo definido genera incertidumbre respecto al volumen de almacenamiento requerido y las obligaciones de retención de datos.

Solicitamos que la regulación establezca plazos claros y razonables para la retención de CDRs, en concordancia con las disposiciones de la Ley N°8968 sobre protección de datos personales y el principio de minimización de datos, de manera que los operadores puedan dimensionar adecuadamente su infraestructura de almacenamiento.

13. Sobre el procesamiento de información de señalización (sección 9.5.A, literal b)
(…)
CLARO actualmente no cuenta con una herramienta que almacene la información de señalización de manera histórica. En los diferentes nodos de la red se pueden tomar trazas en línea (en tiempo real), pero no se dispone de una plataforma que guarde la señalización para la revisión de eventos pasados. En consecuencia, si la SUTEL requiriera revisar un histórico de señalización, no sería posible proporcionarlo con la infraestructura existente.

La implementación de una plataforma de captura y almacenamiento de señalización constituye una inversión significativa que debe ser planificada, presupuestada y ejecutada con plazos realistas. Solicitamos que la regulación contemple un plazo diferenciado y extendido para la implementación de esta capacidad específica, dado que se trata de infraestructura nueva que no forma parte de los sistemas convencionales de un operador de telecomunicaciones.

14. Sobre la detección de patrones de comportamiento sospechoso (sección 9.5.A, literal c)
(…)
Al igual que en el caso del literal b, se requiere la implementación de una plataforma especializada que realice este análisis y tome acciones de manera automatizada. La propuesta de la SUTEL indica que estos equipos o firewalls deben contar con inteligencia artificial para ejecutar estas acciones, lo que confirma que se trata de tecnología avanzada que no es estándar en la infraestructura actual de los operadores.

Solicitamos que la regulación diferencie entre las capacidades de detección que pueden implementarse con ajustes a los sistemas existentes y aquellas que requieren la adquisición de plataformas completamente nuevas, estableciendo plazos proporcionales a la complejidad de cada implementación.

15. Sobre la identificación de robollamadas (robocalls) con voz sintética (sección 9.5.A, literal d)
(…)
Esta capacidad requiere la implementación de una plataforma especializada con funcionalidades de reconocimiento de voz basadas en inteligencia artificial que permita identificar y tomar las acciones correspondientes frente a llamadas automatizadas. Esta tecnología se encuentra en desarrollo a nivel global y su disponibilidad comercial para operadores de la escala del mercado costarricense puede ser limitada.

Solicitamos que la regulación contemple la posibilidad de cumplir esta obligación de manera progresiva, comenzando por la detección de robocalls basada en patrones de comportamiento (frecuencia, duración, tasa de respuesta) y avanzando hacia la detección por análisis de contenido de voz conforme la tecnología esté disponible y sea económicamente viable.

16. Sobre la prevención del vishing en general (sección 9.5.A, literal e)
(…) para cubrir las cinco capacidades que la SUTEL solicita en la sección 9.5 para los servicios de voz, la empresa ha identificado que será necesaria la implementación de dos componentes tecnológicos principales:

(i) una plataforma de captura y almacenamiento de señalización, y
(ii) un firewall de voz con inteligencia artificial.

Ambos componentes requieren procesos de evaluación, adquisición, integración y puesta en marcha que exceden significativamente el plazo de 180 días propuesto.

17. Sobre la implementación del estándar OOBS (sección 9.5.D)
(…)
Solicitamos que la SUTEL facilite un proceso de coordinación interoperador para la adopción del estándar OOBS, estableciendo una hoja de ruta conjunta con hitos intermedios verificables, y que el plazo de implementación se defina de manera realista tras la evaluación técnica conjunta de todos los operadores involucrados.

IV. Observaciones sobre el plazo de implementación (sección 9.6)

18. Insuficiencia del plazo de 180 días naturales
(…) solicitamos que la regulación establezca plazos diferenciados y escalonados, por ejemplo:

- ***Fase 1 (180 días):** Medidas de bloqueo básico (enmascaramiento, tráfico no trazable), registro de entidades A2P, validación de rutas e identificación de remitente.*
- ***Fase 2 (360 días):** Firewalls SMS con capacidades de IA, DPI con limitación de finalidad, sistemas de reputación de enlaces, canales de atención para reporte de SPAM e intercambio de información entre operadores.*
- ***Fase 3 (540 días):** Plataforma de señalización para voz, firewall de voz con IA, detección de robocalls, análisis de patrones avanzados y adopción del estándar OOBS.*

(…)
V. Solicitud final
(…)

1. *Se incorpore un análisis de impacto regulatorio cuantificado que sustente la proporcionalidad de las medidas.*
2. *Se precisen los parámetros técnicos de la DPI para garantizar la minimización de datos y el cumplimiento de la Ley N°8968.*
3. *Se incorporen excepciones al análisis de simetría para el tráfico A2P legítimo unidireccional.*
4. *Se delimite el ámbito de aplicación excluyendo el tráfico multimedia IP.*
5. *Se establezcan plazos de retención de CDRs y señalización concordantes con la normativa de protección de datos.*
6. *Se facilite un proceso de coordinación interoperador para la adopción del estándar OOBS.*
7. *Se sustituya el plazo único de 180 días por un esquema de implementación escalonado en al menos tres fases, con hitos verificables y plazos diferenciados según la complejidad de cada medida.*
8. *Se adopte un enfoque regulatorio integral que combine múltiples palancas de protección (identidad del remitente, consentimiento del usuario, restricciones de contenido, intervención técnica, mecanismos de reporte y diferenciación de precios), en lugar de concentrar las obligaciones exclusivamente en medidas técnicas de detección e intervención en la red.*

9. *Se evalúen mecanismos de diferenciación tarifaria entre el tráfico A2P y P2P como herramienta económica complementaria para desincentivar el uso de rutas grises, tomando en consideración la experiencia internacional exitosa en esta materia.*
10. *Se considere la implementación de un modelo de registro de campañas A2P con aprobación previa de contenido, como alternativa estructural de menor costo y alta efectividad comprobada internacionalmente.*
11. *Se incorporen mecanismos de consentimiento expreso (opt-in) y exclusión voluntaria (opt-out) como alternativas complementarias que reduzcan la necesidad de inspección profunda generalizada del contenido de los mensajes.*

(…)"

Las observaciones a la propuesta presentadas por Claro CR Telecomunicaciones S.A. (Claro) se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por CLARO se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.3.1. Análisis de las observaciones realizadas por Claro CR Telecomunicaciones S.A. (Claro):

Sobre lo señalado en la sección *"**I. Consideraciones generales sobre proporcionalidad y gradualidad**"*, específicamente que la Sutel incorpore dentro de la regulación sometida a consulta pública un análisis de impacto regulatorio que cuantifique los costos estimados de implementación para los operadores, esta Superintendencia considera necesario destacar que la presente iniciativa regulatoria responde a un enfoque de regulación basada en evidencia**,** sustentado en hechos objetivos y verificables que demuestran la existencia de una problemática actual y creciente que afecta a los usuarios de los servicios de telecomunicaciones.

En efecto, tal y como se desarrolla ampliamente en el apartado "2. ANTECEDENTES DE PRÁCTICAS PROHIBIDAS Y LA URGENCIA DE MEDIDAS DE PREVENCIÓN CONTRA SMISHING Y VISHING", la propuesta regulatoria no surge de una hipótesis o de un riesgo potencial abstracto, sino de una necesidad debidamente documentada a partir de múltiples eventos de fraude detectados por esta Superintendencia, reportes de operadores, solicitudes de instituciones públicas, así como publicaciones recientes que evidencian el incremento sostenido de ataques de smishing y vishing en el país.

La información recopilada por la SUTEL demuestra que los ataques se han intensificado durante el año 2026, siendo incluso el período en el que se ha documentado la mayor cantidad de incidentes y solicitudes de suspensión de servicios asociados a prácticas de smishing. Asimismo, se ha constatado que los delincuentes aprovechan vacíos regulatorios y vulnerabilidades existentes para utilizar las redes de telecomunicaciones como mecanismo para la comisión de fraudes, afectando directamente a los usuarios mediante la obtención ilícita de información personal, credenciales bancarias y otros datos sensibles.

En ese sentido, la regulación no se formula sobre escenarios hipotéticos o riesgos potenciales abstractos, sino sobre una problemática existente y debidamente acreditada, que evidencia la exposición actual de los usuarios de las redes de telecomunicaciones a comunicaciones fraudulentas que aparentan ser legítimas, mediante las cuales se procura obtener información personal, credenciales bancarias y otros datos sensibles, con los consecuentes perjuicios patrimoniales y de seguridad asociados.

La implementación de medidas avanzadas para la detección de smishing y vishing constituye una herramienta técnicamente viable y ampliamente utilizada a nivel internacional, además, la propuesta no impone una única solución, sino un conjunto de capacidades que los operadores deben adoptar para cumplir con el objetivo de proteger a los usuarios frente a prácticas irregulares en el tráfico de llamadas y mensajería de texto SMS.

Desde esta perspectiva, la regulación propuesta constituye una respuesta proporcional y necesaria frente a un riesgo cierto y actual, orientada a cumplir con los objetivos de la Ley General de Telecomunicaciones, particularmente aquellos relacionados con la protección de los derechos de los usuarios, la seguridad de las redes y el apoyo a la seguridad ciudadana. La medida procura establecer obligaciones preventivas mínimas para los operadores y proveedores, con el fin de reducir la exposición de los usuarios a este tipo de amenazas y fortalecer la confianza en los servicios de telecomunicaciones.

Considerando lo anterior y ante el riesgo presente debidamente identificado, resulta urgente la adopción de las medidas regulatorias propuestas, en aplicación del principio de beneficio al usuario y de los objetivos previstos en la Ley General de Telecomunicaciones, particularmente aquellos vinculados con la protección de los usuarios y el apoyo a la seguridad ciudadana. En este contexto, retrasar la implementación de medidas preventivas mientras se desarrolla un análisis regulatorio de mayor amplitud implicaría mantener a los usuarios expuestos a una amenaza creciente y plenamente documentada.

En consecuencia, la urgencia y naturaleza de la problemática identificada justifican la adopción inmediata de la propuesta regulatoria, por cuanto no resultaría razonable ni proporcional posponer la implementación de acciones preventivas oportunas, especialmente cuando la evidencia recopilada por esta Superintendencia demuestra que el año 2026 ha presentado un incremento significativo en la cantidad de ataques de smishing y vishing detectados. Bajo estas circunstancias, el interés público asociado a la protección de los usuarios y la seguridad de las redes de telecomunicaciones prevalece sobre los costos de implementación de las medidas propuestas, los cuales resultan proporcionados frente a los beneficios esperados.

Los costos asociados a la implementación de mecanismos de seguridad deben considerarse parte integral de la operación de servicios de telecomunicaciones. La protección contra prácticas irregulares como el smishing y el vishing es un componente esencial de la calidad y confiabilidad del servicio. En consecuencia, estos costos forman parte de las inversiones habituales asociadas a la operación de redes seguras y confiables, por lo que, corresponde a los operadores asumirlos como parte de sus obligaciones

inherentes, sin trasladarlos ni condicionarlos a procesos previos de cuantificación regulatoria.

Por lo anterior, la mitigación de prácticas prohibidas, la protección de los usuarios, la seguridad de la red y la preservación de la integridad del servicio son responsabilidades inherentes a la actividad de los operadores. Bajo el principio de neutralidad tecnológica, corresponde a cada operador definir e implementar las soluciones técnicas idóneas que le permitan garantizar la calidad y seguridad del servicio, asumiendo los costos asociados como parte de su responsabilidad operativa y de su compromiso con la protección de los usuarios.

Sobre el precio de los mensajes SMS, se le recuerda a Claro CR Telecomunicaciones S.A. (Claro), que por medio de la resolución del Consejo de la Sutel número RCS-313-2023 "*REVISIÓN DEL MERCADO DEL SERVICIO DE TERMINACIÓN EN REDES MÓVILES INDIVIDUALES, ANÁLISIS DEL GRADO DE COMPETENCIA EN DICHO MERCADO, DETERMINACIÓN DE OPERADORES Y PROVEEDORES IMPORTANTES E IMPOSICIÓN DE OBLIGACIONES",* se dispuso que dicho operador tiene poder sustancial en el mercado del servicio mayorista de terminación en la red móvil, consecuentemente es objeto de presentar, ante la Superintendencia, una oferta de interconexión por referencia (OIR), en la cual se deben justificar, entre otros, los cargos mayoristas de terminación de voz móvil y SMS, para su revisión y aprobación ante esta Superintendencia. En línea con lo anterior, mediante la resolución RCS-266-2025 *"REVISIÓN Y APROBACIÓN DE LA OFERTA DE INTERCONEXIÓN POR REFERENCIA (OIR) DE LA EMPRESA CLARO CR TELECOMUNICACINES, S.A."* la SUTEL, aprobó dicha OIR, incluyendo los cargos para estos servicios, tomando en consideración los costos remitidos por el operador, pero también la metodología establecida por la SUTEL en la resolución RCS-200-2020, la cual desarrolla el cumplimiento del principio de orientación a costos establecido en nuestra legislación. Por lo anterior, valorar un aumento en los cargos de terminación, sin la debida justificación técnica y económica, como una herramienta regulatoria, podría ser contrario a este principio. Amén de lo anterior, en este momento la SUTEL tiene en curso un proceso de revisión del mercado relevante de terminación en redes móviles individuales, siendo que será el resultado de dicha revisión el que determine el proceder regulatoria en esta materia.

Los precios de interconexión internacional se encuentran sujetos a condiciones de libre oferta y demanda dentro del mercado de telecomunicaciones, razón por el cual como lo señala en su documento *"(…) bloquear cualquier tráfico A2P proveniente de rutas no oficiales (rutas grises) usadas para la terminación de mensajes SMS A2P, incluyendo rutas de interconexión, en las cuales no puedan verificar la trazabilidad de la comunicación hasta el emisor."*, es necesario la implementación de una medida regulatoria con la finalidad de que el operador pueda identificar las ruta y el origen de la comunicación.

Además, los acuerdos comerciales pactados a nivel internacional entre operadores, proveedores y agregadores para oficializar rutas de tráfico A2P pueden incluir mecanismos tarifarios específicos para el trato de esta información, aplicando penalizaciones económicas a la parte que realice un uso incorrecto de la ruta de interconexión, como por ejemplo intentar simular tráfico A2P como P2P, lo cual implica que necesariamente exista

una correcta identificación y filtrado de los mensajes A2P por parte de cada operador. Por lo que, mediante dichos acuerdos de nivel internacional los operadores tienen plena potestad de negociar tarifas para el manejo de tráfico A2P por una ruta oficial, sin embargo, esta medida no debe verse como una alternativa ante lo requerido en la regulación propuesta, sino más bien como un complemento, siendo que, adicional a los mecanismos tarifarios establecidos entre operadores a nivel internacional, la regulación propone el requerimiento de bloquear todo el tráfico de mensajes A2P que ingrese por rutas no oficiales y sin información de trazabilidad.

Por lo que, además de cualquier mecanismo tarifario pactado entre operadores a nivel internacional, proveedores o agregadores, para el manejo de mensajes A2P, se debe garantizar que el tráfico A2P transite exclusivamente por rutas oficiales, de modo que, se debe bloquear todo el tráfico A2P que ingrese por una ruta distinta o no autorizada.

En cuanto a lo señalado por el operador sobre que, la regulación propuesta se enfoca exclusivamente en detección e intervención técnica, sin abordar el consentimiento y exclusión voluntaria del usuario, restricciones de contenido y aprobación previa de campañas, ni incentivos económicos y diferenciación tarifaria entre tráfico A2P y P2P, con base en lo señalado por el operador, cabe indicar que la regulación propuesta también contempla los puntos (A) identidad y autorización del remitente, (C) restricciones de contenido y registro de campañas, (E) mecanismos para reportes y reclamos de usuarios y (F) precios alineados con el valor agregado del tráfico A2P, siendo que, es conocido que el uso de rutas grises para la terminación de tráfico A2P conllevan una pérdida económica para los operadores, por cuanto, los remitentes utilizan rutas inseguras de menor costo para la entrega de los mensajes, evitando rutas oficiales con tarifas definidas donde se garantiza la seguridad de la información.

En cuanto a los mecanismos de consentimiento expreso previo por parte del usuario para la recepción de mensajes publicitarios o exclusión voluntaria mediante respuesta directa al remitente, es importante mencionar que, el Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF) ya considera y establece reglas claras sobre la recepción de mensajes y comunicaciones con fines de venta directa de bienes y servicios, donde efectivamente se requiere de previo la autorización y consentimiento expreso del usuario, como lo disponen los artículos 102 y 104 de citado reglamento:

> *"(…)*
> ***Artículo 102. Sobre la información comercial con fines de venta directa***
>
> *Los operadores/proveedores de servicios de telecomunicaciones deben asegurar que únicamente los usuarios finales que hayan brindado su consentimiento expreso podrán recibir información comercial con fines de venta directa de sus bienes y servicios, la cual se deberá realizar por medios que permitan la identificación del remitente, así como, finalizar tales comunicaciones.*
>
> *Los operadores/proveedores deben registrar y almacenar hasta dos meses después de finalizada la contratación, constancia de la voluntad expresa para la recepción de la información con fines de venta directa. En caso de no contar con la citada información, se considerará una práctica prohibida.*

> *(…)*
> ***Artículo 104. Implementación de medidas técnicas y administrativas***
> *Los operadores/proveedores de servicios de telecomunicaciones, deben implementar las medidas técnicas y administrativas necesarias, para garantizar que sus usuarios finales no reciban comunicaciones con fines de venta directa de sus bienes y servicios, cuando éstos no hayan brindado su consentimiento previamente o hayan solicitado su remoción de las listas de comunicación. Estas gestiones, por parte del usuario final, no tendrán costo alguno.*
>
> *La manifestación por parte del usuario final en el registro de la Sutel para no recibir comunicaciones no solicitadas tendrá preponderancia sobre otras suscripciones y automáticamente será tomado como una petición expresa para que se ponga fin a tales comunicaciones. Dicha manifestación, estará vigente durante el plazo en que el usuario final mantenga su numeración registrada en dicha base de datos.*
> *(…)"* (Destacado intencional)

Asimismo, el artículo 4 de este reglamento en sus incisos 15) y 16) establece como derechos de los usuarios finales: *"(…)* ***15.*** *Recibir, únicamente comunicaciones con fines de venta directa de bienes y servicios por parte de los operadores/proveedores de servicios, por llamadas o mensajes, cuando medie su consentimiento expreso.* ***16.*** *Ser excluido por los operadores/proveedores de servicios en cualquier momento sin costo adicional el envío de comunicaciones con fines de venta directa de bienes y servicios. (…)"*, y, además, el artículo 107 inciso 2) de este mismo reglamento dispone como práctica prohibida por parte de los operadores *"(…)* ***2.*** *Toda acción donde se remita información con fines de venta directa, comercial y/o publicitaria a los usuarios finales sin contar de previo con su consentimiento, se utilicen sistemas de llamada o suscripción automática, se oculte o falsee el remitente de la comunicación o no se cuente con una alternativa para finalizar dichas comunicaciones. (…)"*, de modo que, la regulación vigente ya faculta la implementación de mecanismos de consentimiento previo para que los usuarios puedan establecer sus propias reglas de filtrado, no obstante, esta medida es complementaria y no debe interpretarse como una opción que sustituya los requerimientos planteados en la regulación propuesta, ya que, la aplicación de una única medida no cierra todas las brechas que actualmente utilizan los ciberdelincuentes para llegar a los usuarios. Por lo anterior, se recomienda el rechazo de esta observación.

Por otra parte, sobre las observaciones de la sección ***"II. Observaciones sobre las medidas relativas a los servicios de mensajería SMS (secciones 9.1 a 9.4)"***, específicamente sobre la implementación de un periodo de transición que permita de manera gradual alcanzar la totalidad de requerimientos para los firewalls de SMS, este operador señaló que actualmente se encuentra en proceso de migración a una nueva solución de firewall de SMS que tiene la capacidad técnica de realizar los tipos de bloqueos descritos en la propuesta regulatoria, sin embargo, requiere consultar con el proveedor de dicha solución el alcance de la capacidad de Inteligencia Artificial para cumplir a cabalidad con la regulación sometida a consulta pública, por lo que, este operador solicita que se establezca un cronograma gradual para la implementación de funcionalidades que permitan cumplir con los requisitos planteados en la regulación propuesta.

Al respecto, esta Superintendencia se encuentra anuente a establecer un cronograma escalonado para la implementación de la totalidad de capacidades solicitadas en la regulación sometida a consulta pública, iniciando con un plazo de 180 días para implementar medidas que únicamente requieran de configuraciones y ajustes básicos en

su infraestructura, como lo es la trazabilidad de las comunicaciones, restricciones por enmascaramiento, registro de entidades autorizadas para envío de mensajes A2P, validación de rutas e identificación de remitentes, y de manera posterior y gradualmente ir incluyendo capacidades de Inteligencia Artificial y análisis en tiempo real. Este cronograma se analiza con mayor detalle más adelante, con base en otra propuesta planteada por este mismo operador.

Sobre la propuesta de implementar como alternativa al firewall requerido en la regulación sometida a consulta pública, un modelo de registro de campañas A2P, similar a *The Campaign Registry* (TCR) utilizado en Estados Unidos[11], donde solo las empresas incluidas en este registro pueden enviar campañas de mensajes A2P. Al respecto, debe destacarse que, tal y como lo indicó el mismo operador, la regulación propuesta por esta Superintendencia ya contempla un registro de entidades A2P en la sección 9.3 inciso E. donde se requirió: *"(…) establecer registros de las entidades desde las cuales se envía y recibe tráfico de SMS A2P (…) donde se indique el nombre de la empresa y el segmento de numeración que hace uso. (…)"*, no obstante, la propuesta del operador busca robustecer el registro de campañas y remitentes autorizados para enviar mensajes A2P, de modo que, se bloquee todo el tráfico de mensajes A2P generado desde servicios que no se encuentren debidamente registrados y autorizados para tráfico A2P.

The Campaign Registry (TCR) utilizado en Estados Unidos funciona como una entidad central donde cualquier empresa que desee realizar campañas de mensajes A2P debe estar registrada, a través de proveedores de servicios de mensajería A2P, es decir, la empresa interesada en este servicio debe solicitar a un operador su inclusión en este registro, de modo que, una empresa no puede registrase por sí sola. Esto permite que los operadores tengan total control y conocimiento sobre los clientes autorizados a realizar campañas de mensajes A2P.

Además, según *The Campaign Registry* (TCR), a cada campaña registrada se le asigna una puntuación de confianza, que se basa en diversos factores, como el contenido y el propósito de la campaña. Una puntuación de confianza más alta indica que es menos probable que la campaña de mensajería sea una fuente de spam o actividades fraudulentas, lo que mejora aún más la seguridad del usuario final[12].
Sin embargo, es importante que este proceso vaya de la mano con la adecuada verificación de la identidad para cada empresa que desee enviar mensajes de tipo A2P, con el objetivo de confirmar que la empresa y sus actividades de mensajería son legítimas, acción que recae en el operador al verificar correctamente la identidad de cada uno de sus clientes autorizados para realizar campañas de mensajes A2P.

Cabe aclarar que, la implementación del citado registro, así como el bloqueo de remitentes A2P no autorizados lo deberá realizar cada operador para sus respectivos clientes que envían tráfico A2P, de modo que, se garantice que para el tráfico A2P generado localmente, los demás operadores solo recibirán mensajes A2P de empresas o entidades autorizadas

[11] https://www.campaignregistry.com/
[12] https://telnyx.com/resources/10dlc-compliance

e incluidas en el registro que llevará cada operador, y en caso de determinar la comisión de prácticas prohibidas por parte de estos usuarios, proceder conforme lo dispone la normativa vigente.

Por lo anterior, se evidencia el valor en seguridad que ofrece la propuesta de este operador respecto a robustecer lo requerido en la sección 9.3 inciso E. de la regulación sometida a consulta pública, donde se requirió a todos los operadores y proveedores establecer registros de las entidades desde las cuales se envía y recibe tráfico de SMS A2P, por lo que, se debe adicionar la propuesta regulatoria para que, además los operadores y proveedores de mensajería SMS A2P deban verificar adecuadamente la identidad de sus clientes de mensajería A2P y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas legitimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de servicios no incluidos en dicho registro. Asimismo, los operadores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios.

Sin embargo, esta medida debe verse como un refuerzo a la implementación del firewall requerido en la regulación sometida a consulta pública y no como una alternativa a los requerimientos propuestos como lo sugiere este operador, ya que de lo contrario, limitaría la prevención de smishing a la verificación y registro de remitentes A2P autorizados por parte del operador, sin revisar el contenido de los mensajes A2P en tiempo real, los cuales pueden incluir intentos de smishing, enlaces maliciosos o malwares, independientemente de la empresa o entidad que los envíe, por lo que, es importante que ambas medidas se implementen de forma conjunta para cerrar en mayor medida los intentos de estafa mediante mensajes SMS A2P.

Por lo anterior, se recomienda acoger parcialmente la propuesta de este operador, sobre robustecer lo requerido en la **sección 9.3 inciso E.** de la propuesta sometida a consulta pública, adicionando que, los operadores y proveedores de mensajería SMS A2P deben verificar adecuadamente la identidad de sus clientes de mensajería A2P y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas legítimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no registrados. Estos registros se deben compartir entre operadores y proveedores interconectados.

Por otro lado, en el **punto 5** el operador propone que, los clientes autorizados para el envío de campañas de mensajes A2P, remitan de forma previa una o varias plantillas con los mensajes que serán enviados a los usuarios, de esta forma, el operador puede validar en tiempo real que el contenido del mensaje enviado coincide con la plantilla sometida a revisión, con el objetivo de no realizar Inspección Profunda de Paquetes (DPI) sobre este tráfico.

Al respecto, si bien dicha propuesta constituye un mecanismo válido como medida complementaria de control, no puede considerarse una alternativa que elimine la necesidad de análisis de contenido, ni sustituye completamente capacidades como el DPI.

Cabe señalar que, la verificación de coincidencia entre un mensaje A2P enviado y una plantilla previamente registrada implica necesariamente el análisis de similitud del contenido del mensaje. Es decir, el sistema debe inspeccionar el texto del mensaje, procesarlo y compararlo con una referencia. Esto constituye, en esencia, una forma de validación de contenido, aunque con un alcance más limitado que el que promueve la presente propuesta regulatoria.

Por lo tanto, este enfoque no evita el uso de análisis de contenido, sino que, lo restringe al caso específico de comparación contra plantillas, lo que representa limitaciones sustanciales desde el punto de vista de seguridad, ya que, se podrían adaptar mensajes para cumplir formalmente con una plantilla, pero incorporar elementos maliciosos variables como enlaces dinámicos, y pequeñas modificaciones en el contenido del mensaje que pueden evadir controles si el sistema no es suficientemente robusto, además, la revisión previa de plantillas no garantiza que el contexto de uso posterior sea legítimo, siendo que, utilizar los servicios de telecomunicaciones para fines distintos del contratado se considera práctica prohibida..

En contraste, los mecanismos basados en análisis más amplios en cuanto a la revisión del contenido y comportamiento, como lo es DPI, permiten identificar además patrones maliciosos en tiempo real, independientemente de si el mensaje fue previamente revisado.

El uso de plantillas puede ser parte de la solución, pero no puede limitar el alcance de las medidas requeridas ni sustituir capacidades necesarias para abordar el problema de forma integral. Este enfoque de verificación de plantillas puede crear una falsa sensación de seguridad, mientras deja abiertos múltiples opciones de ataque que hoy son ampliamente utilizados por actores maliciosos.

El registro y validación de plantillas A2P puede ser una herramienta útil como mecanismo complementario de control, pero no sustituye el análisis de contenido ni las capacidades de detección en tiempo real. Por el contrario, debe integrarse dentro de un enfoque más amplio que incluya análisis de patrones, comportamiento y contenido, a fin de garantizar una mitigación efectiva del smishing, por lo que, se recomienda acoger de forma complementaria la propuesta del operador.

Por otra parte, respecto a lo indicado en el **punto 6** sobre especificar los canales de atención al usuario aceptables para el reporte de spam, es importante señalar que, el Reglamento sobre el Régimen de Protección al Usuario Final (RPUF) en su artículo 3 inciso 7) ya define los centros de atención al usuario final:

> *"(…)*
> ***7. Centro de Atención al Usuario Final**: es un conjunto de canales gratuitos soportados en una plataforma que, a través de medios telefónicos, electrónicos, aplicaciones o de forma presencial, provee las vías y condiciones para otorgar información a los usuarios, recibir y atender de forma efectiva reclamaciones y solicitudes respecto a la prestación de servicios y derechos de usuarios finales, así como, cualquier otra que facilite el trámite de los usuarios finales en relación con los servicios prestados por el operador/proveedor. Se excluye de esta definición a los comercializadores y distribuidores contratados por los operadores/proveedores únicamente para la venta de servicios.*

(…)"

Por lo que, los canales disponibles se encuentran detallados en dicha definición del reglamento, de modo que, se recomienda el rechazo de esta observación. Adicionalmente, de conformidad con el principio de beneficio al usuario dispuesto en el artículo 3 de la Ley N°8642, Ley General de Telecomunicaciones, se recomienda poner a disposición de los usuarios la mayor cantidad de canales disponibles para que los usuarios reporten tráfico SPAM.

Sobre el requerimiento planteado en el **punto 7** respecto a que, para el intercambio de información entre operadores, la Sutel valide las áreas de interconexión entre operadores y establezca los protocolos y procedimientos para el intercambio de dicha información, es importante mencionar que, si bien la regulación sometida a consulta pública se basó en las recomendaciones de la Unión Internacional de Telecomunicaciones ITU-T X.1247 y UIT-T X.1237, las cuales entre otras cosas resaltan la importancia de establecer mecanismos de intercambio de información anti-spam entre operadores, es importante aclarar que, en la propuesta regulatoria sometida a consulta pública no se hicieron requerimientos respecto a compartir información entre operadores. Si bien esta medida puede aportar de forma positiva a la lucha contra el smishing, lo solicitado por el operador no se ajusta con los requerimientos dispuestos en la propuesta de regulación sometida a consulta pública. En todo caso, el artículo 3 inciso h) de la Ley N°8642 Ley General de Telecomunicaciones, dispone el principio de neutralidad tecnológica, el cual, les brinda a los operadores y proveedores la posibilidad de escoger a discreción las tecnologías a utilizar para brindar sus servicios, siempre y cuando, cumplan con los requerimientos mínimos establecidos en la regulación, y se garanticen las condiciones de calidad, por lo que, esta Superintendencia no tiene la potestad para imponer un método o protocolo específico de intercambio de información, siendo que, le corresponde a los operadores y proveedores escoger a su criterio la tecnología que mejor se ajuste a su infraestructura y presupuesto, para cumplir con la regulación sometida a consulta pública.

Asimismo, el artículo 75 inciso b) subinciso vi. de la Ley N°7593, Ley de la Autoridad Reguladora de los Servicios Públicos (ARESEP) dispone dentro de las obligaciones de los operadores importantes: *"vi. Proporcionar a otros operadores y proveedores, servicios e información de la misma calidad y en las mismas condiciones en las que proporciona a sus filiales o asociados y a sus propios servicios"*, lo cual puede hacerse extensivo a todos los demás operadores según el párrafo final del mismo artículo, de modo que, se recomienda rechazar esta observación respecto a que Sutel defina los canales de intercambio de información.

Respecto de la propuesta planteada en el **punto 8** sobre el análisis de simetría de las comunicaciones y bloqueo de tráfico A2P sin respuesta correspondiente al comportamiento de sistemas automatizados (bots), establecido en la sección 9.1 inciso C. subinciso 13 de la regulación sometida a consulta pública; el operador manifestó que, existe la posibilidad de bloquear campañas de mensajes legitimas realizadas por clientes autorizados, los cuales, por la naturaleza de sus negocios generan grandes cantidad de mensajes que no reciben respuesta como los *"Mensajes de autenticación de dos factores (2FA) y contraseñas de un solo uso (OTP) enviados por instituciones bancarias y financieras",* de modo que, el operador propone la

implementación de un registro de excepciones para evitar el bloqueo del tráfico A2P legítimo sin respuesta proveniente de entidades registradas ante el operador.

Al igual que se indicó anteriormente, para la implementación de un registro de servicios autorizados para el envío de mensajes informativos masivos sin recibir respuesta, le corresponderá al operador verificar adecuadamente la identidad de sus clientes y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas o entidades legitimas se encuentren en dicho registro de excepciones, y bloquear todo el tráfico que presente un comportamiento similar y no se encuentre en el citado registro. Por lo que, se recomienda acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Sin embargo, se aclara que este requerimiento aplica tanto para mensajes A2P como P2P.

Respecto a la propuesta indicada en el **punto 9** sobre excluir el tráfico multimedia IP de las obligaciones contenidas en esta actualización regulatoria, cabe señalar que, si bien la recomendación ITU-T X.1244 fue sustento para la presente propuesta regulatoria, los requerimientos finales planteados se enfocan específicamente en el tráfico de mensajes SMS (A2P y P2P) y llamadas de voz, sin incluir servicios multimedia IP, de modo que, es consistente acoger la propuesta del operador sobre delimitar la presente actualización regulatoria a la exclusión del tráfico multimedia IP, por lo que, se recomienda acoger esta observación.

En lo relativo a lo requerido en el **punto 10** acerca de que la Sutel establezca un proceso de socialización con los agregadores de SMS que operan en el mercado nacional, para que adecúen sus sistemas y filtros conforme a los nuevos requerimientos, es importante mencionar que, empresas como agregadores de SMS que no brindan específicamente servicios de telecomunicaciones se encuentran fuera del ámbito de regulación de esta Superintendencia, por lo que, la Sutel no tiene potestad para establecer procedimientos sobre agregadores de SMS, no obstante, una vez publicada la presente disposición regulatoria será de conocimiento general a nivel nacional, por lo que, estará disponible para agregadores y cualquier otra empresa que desee conocer los requerimientos establecidos para los operadores y proveedores de servicios de telecomunicaciones. De modo que, durante el periodo inicial otorgado de 180 días para el ajuste e implementación de las medidas requeridas, los operadores deben revisar y de ser necesario ajustar las condiciones pactadas entre operadores, proveedores y agregadores para garantizar la información mínima de trazabilidad establecida en la propuesta regulatoria.

En cuanto a la propuesta indicada en el mismo punto sobre que, la actualización regulatoria diferencie las obligaciones por canal de ingreso A2P, aplicando medidas de filtrado menos intensivas al tráfico proveniente de agregadores internacionales autorizados y filtrados más complejos al tráfico A2P que ingresa por interconexión directa sin garantía de seguridad, es importante mencionar que, como se indicó anteriormente, gran parte de los mensajes A2P que ingresan por rutas internacionales corresponden a mensajes de autenticación con información sensible para el acceso a cuentas personales de los usuarios, de modo que, es indispensable que se garantice la integridad de la información de extremo a extremo y

por ende su trazabilidad, por lo que, dejar la seguridad de los mensajes A2P en manos de un tercero fuera del territorio nacional, no es adecuado para el objetivo que busca la regulación propuesta. Por lo anterior, no es de recibo la propuesta del operador, de modo que, únicamente se debe permitir el tránsito de mensajes A2P con información de trazabilidad, independientemente si proviene de rutas internacionales o por interconexión directa, así como analizar la coherencia en las comunicaciones, es decir, verificar en tiempo real que el origen de la comunicación coincida con la ruta por la que ingresa y el operador conectado a dicha ruta, de modo que, debe bloquear cualquier comunicación que no muestre esta coherencia en la trazabilidad. Por lo anterior, se recomienda el rechazo de esta solicitud.

Asimismo, sobre el requerimiento planteado en el **punto 11** relativo a que la regulación propuesta contemple la necesidad de que los operadores involucren a sus áreas de auditoría y prevención de fraudes en la gestión de los firewalls de SMS, si bien representa alto valor para el objetivo de esta propuesta, dicha disposición corresponde a coordinaciones internas del operador fuera del alcance de esta Superintendencia, por lo que, se recomienda el rechazo de esta solicitud.

Respecto a la solicitud señalada en el **punto 12** sobre que la propuesta no indica en la **sección 9.5.A, literal a)** un límite de tiempo para el resguardo de los registros de llamadas (CDR), debe señalarse que, aplica lo dispuesto en el artículo 52 del RPUF el cual establece un plazo mínimo de cuatro (4) años para conservar los registros detallados de las comunicaciones (llamadas y SMS) que cursen los usuarios finales dentro o fuera de sus redes. Por lo anterior, en la misma línea que lo señalado por **CallMyWay NY S.A. (Call My Way)** en sus puntos 1 y 3, se recomienda acoger esta solicitud y reafirmar en la propuesta regulatoria las disposiciones del citado artículo.

En lo relativo a la propuesta indicada en el **punto 13** sobre contemplar en la presente actualización regulatoria un plazo diferenciado y extendido para la implementación del procesamiento de información de señalización obtenida de las comunicaciones y por puntos de recopilación, ya que, según el operador constituye una inversión significativa que debe ser planificada, presupuestada y ejecutada con plazos mayores, se aclara que, esta Superintendencia en la resolución que se emita modificará el plazo de ejecución para que la totalidad de capacidades requeridas sean implementadas de forma gradual, considerando las observaciones recibidas, brindando un plazo inicial de 180 días para la implementación de ajustes y configuraciones al alcance de los operadores y posterior y gradualmente ir incluyendo análisis más complejos, por lo que, se acoge la propuesta del operador sobre ampliar el plazo para la puesta en marcha de esta capacidad.

Esto aplica de igual manera para el requerimiento del **punto 14** sobre ajustar el plazo de implementación según la complejidad de cada característica del firewall detallado en la **sección 9.5.A, literal c)** de la propuesta regulatoria.

En cuanto a lo indicado en el **punto 15**, sobre los firewalls con capacidad de identificación de robollamadas (robocalls) con voz sintética en tiempo real basados en Inteligencia Artificial, el operador manifiesta que esta tecnología se encuentra actualmente en desarrollo

a nivel global y su disponibilidad para operadores de la escala del mercado costarricense puede ser limitada, de modo que, propone un cumplimiento progresivo para la totalidad de características solicitadas en la regulación propuesta, y de esta forma, prolongar la implementación de la identificación de robollamadas (robocalls) con voz sintética en tiempo real a futuro, cuando la tecnología esté disponible y sea más económica. Al respecto, de la misma forma que se ha abordado anteriormente, Sutel contempla que la totalidad de capacidades requeridas sean implementadas de forma gradual, considerando las observaciones recibidas, brindando un plazo inicial de 180 días para la implementación de ajustes y configuraciones al alcance de los operadores y posterior y gradualmente ir incluyendo análisis más complejos como el uso de Inteligencia Artifical para revisiones en tiempo real, por lo que, es razonable la propuesta del operador sobre prolongar el plazo para la puesta en marcha de esta capacidad. Esto también aplica para el requerimiento para la prevención del vishing señalado en el **punto 16**. Por lo que, se recomienda acoger estos puntos.

En cuanto a la solicitud planteada en el **punto 17** sobre la implementación del estándar OOBS para autenticación de todas las llamadas y que la Sutel facilite un proceso de coordinación interoperador para la adopción de este estándar mediante una hoja de ruta conjunta con hitos intermedios verificables y con un plazo de implementación acorde a la evaluación técnica conjunta de todos los operadores involucrados, es importante mencionar que cada operador cuenta con responsabilidad individual sobre sus redes.

Resulta relevante destacar que, como se detalla más adelante, este mismo operador ha propuesto un plazo de implementación de 540 días (18 meses), el cual, se considera proporcional, suficiente y razonable para que cada operador planifique, desarrolle e implemente internamente las capacidades requeridas, sin necesidad de retrasar el inicio o avance del proceso a ejercicios adicionales de coordinación centralizada o validaciones conjuntas.

Condicionar la implementación a la construcción de una hoja de ruta común o a procesos de alineamiento colectivo introduce un riesgo innecesario de demora, particularmente cuando ya existe un plazo definido y razonable (18 meses) para implementar la totalidad de medidas requeridas. Debe reiterarse que, cada operador es responsable de implementar mecanismos de autenticación de llamadas que cumplan con estándares internacionales, incluyendo OOBS como una solución técnicamente robusta. La forma específica de implementación, así como la gestión de los hitos intermedios, corresponde a cada operador en función de su red y sus decisiones tecnológicas.

Asimismo, cabe señalar que la interoperabilidad no requiere coordinaciones previas exhaustivas, sino el cumplimiento de especificaciones técnicas comunes, como las definidas para el estándar OOBS. El plazo de 18 meses permite precisamente este enfoque progresivo, donde cada operador puede avanzar según su propio plan de implementación, sin comprometer el objetivo global.

Por lo anterior, no resulta necesario ni conveniente establecer procesos de coordinación centralizada ni hojas de ruta conjuntas adicionales. Tomando en consideración la existencia

de un plazo definido de 18 meses, propuesto por este mismo operador, corresponde a cada uno asumir la responsabilidad de cumplir con la implementación de OOBS dentro de ese plazo, adoptando las soluciones técnicas que mejor se ajusten a su red, en línea con el principio de neutralidad tecnológica y según su obligación de garantizar y fortalecer de manera oportuna la seguridad de sus redes y servicios de telecomunicaciones. Por lo anterior, se recomienda el rechazo de este punto.

Por su parte, respecto a lo señalado en el **punto 18** sobre la insuficiencia del plazo de 180 días otorgado para la implementación de los requerimientos de la presente propuesta regulatoria, el operador propone el siguiente calendario con plazos diferenciados y escalonados:

"(…)
- ***Fase 1 (180 días):** Medidas de bloqueo básico (enmascaramiento, tráfico no trazable), registro de entidades A2P, validación de rutas e identificación de remitente.*
- ***Fase 2 (360 días):** Firewalls SMS con capacidades de IA, DPI con limitación de finalidad, sistemas de reputación de enlaces, canales de atención para reporte de SPAM e intercambio de información entre operadores.*
- ***Fase 3 (540 días):** Plataforma de señalización para voz, firewall de voz con IA, detección de robocalls, análisis de patrones avanzados y adopción del estándar OOBS.*

(…)"

Según lo anterior, los plazos se dividen en 3 fases, iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas en cuanto a servicios de mensajería SMS y posteriormente 2 fases adicionales para medidas avanzadas con plazos para puesta en operación de 12 meses (360 días) para completar las mediadas aplicables a los servicios de mensajería SMS y 18 meses (540 días) para la implementación de los requerimientos de seguridad para servicios de voz. Cabe señalar que, si bien ante la presente consulta pública se recibieron otras observaciones respecto a un plazo de implementación escalonado, Claro CR Telecomunicaciones S.A. (Claro) fue el único que aportó una propuesta detallada de calendario gradual de implementación con plazos razonables y proporcionales para la puesta en funcionamiento de cada uno de los requerimientos dispuestos en la propuesta sometida a consulta pública, razón por la cual se recomienda acoger dicha recomendación. No obstante, cabe reiterar que, el Reglamento sobre el Régimen de Protección al Usuario Final (RPUF) en su artículo 3 inciso 7) ya define los centros de atención al usuario final, por lo que, estos pueden ser parte de la fase 1 de implementación. Además, la propuesta de este operador incorpora el intercambio de información entre operadores para la fase 2 del cronograma, de modo, se recomienda acoger la incorporación de este requerimiento para ser implementado por parte de los operadores y proveedores en la fase 2.

Basado en el análisis anterior, se recomienda acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Este requerimiento aplica tanto para mensajes A2P como P2P, además, estos registros se deben compartir entre operadores y proveedores interconectados.

Además, se recomienda acoger la observación de este operador respecto a excluir el tráfico multimedia IP de las obligaciones contenidas en esta propuesta regulatoria.

Además, se recomienda acoger parcialmente la propuesta de Claro CR Telecomunicaciones S.A. (Claro) sobre robustecer lo requerido en la **sección 9.3 inciso E.** de la propuesta sometida a consulta pública, donde se requirió a todos los operadores y proveedores establecer registros de las entidades desde las cuales se envía tráfico de SMS A2P, adicionando que, los operadores y proveedores de mensajería SMS A2P deben verificar adecuadamente la identidad de sus clientes de mensajería A2P y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas legitimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no registrados. Esto aplica de igual forma para las rutas de interconexión, de modo que, solo se enviará a otros operadores el tráfico A2P de remitentes autorizados y previamente verificados. Asimismo, los operadores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios.

Por otra parte, se recomienda acoger de forma complementaria la propuesta del operador sobre permitir a los operadores el registro y validación de plantillas para mensajes A2P.

Asimismo, se recomienda acoger la solicitud del operador sobre indicar el límite de tiempo para el resguardo de los registros de llamadas (CDR), para lo cual aplica lo dispuesto en el artículo 52 del RPUF, el cual establece un plazo mínimo de cuatro (4) años para conservar los registros detallados de las comunicaciones (llamadas y SMS) que cursen los usuarios finales dentro o fuera de sus redes.

Finalmente, se recomienda acoger la propuesta de este operador sobre dividir la implementación de la presente propuesta regulatoria en 3 fases de la siguiente manera, cuyos plazos máximos corren a partir de la entrada en vigor:

- **Fase 1 de 180 días (6 meses):** implementación de medidas básicas de bloqueo en cuanto a servicios de mensajería SMS, como restricciones por enmascaramiento, reglas para tráfico no trazable, registro de entidades autorizadas para envío de mensajes A2P, validación de rutas e identificación de remitentes, centros de atención al usuario final[13] para reporte de SPAM y la implementación de un registro de excepciones para clientes autorizados a enviar grandes cantidades de mensajes informativos tanto en A2P como P2P.

- **Fase 2 de 360 días (12 meses):** implementación de medidas avanzadas con capacidades de Inteligencia Artificial para detección y bloqueo en tiempo real de mensajes SMS maliciosos, con Inspección Profunda de Paquetes (DPI),

[13] Según el artículo 3 inciso 7) del RPUF, estos corresponden al conjunto de canales gratuitos soportados en una plataforma que, a través de medios telefónicos, electrónicos, aplicaciones o de forma presencial, provee las vías y condiciones para otorgar información a los usuarios, recibir y atender de forma efectiva reclamaciones y solicitudes respecto a la prestación de servicios y derechos de usuarios finales, así como, cualquier otra que facilite el trámite de los usuarios finales en relación con los servicios prestados por el operador/proveedor.

Procesamiento de Lenguaje Natural (NLP), Análisis Heurístico, sistemas de reputación de enlaces e intercambio de información entre operadores. Esta fase incluye la implementación de la totalidad de requerimientos establecidos en la normativa para mensajes SMS tanto A2P como P2P.

- **Fase 3 de 540 días (18 meses):** implementación de la totalidad de los requerimientos de seguridad dispuestos en el apartado 9.5 de la propuesta regulatoria para servicios de voz.

En cuanto a las observaciones restantes, se recomienda su rechazo con base en los puntos analizados anteriormente.

3.4. Posición del Instituto Costarricense de Electricidad (ICE).

Por medio del oficio 7110-399-2026 del 24 de abril de 2026 (NI-05531-2026) el Instituto Costarricense de Electricidad (ICE) por medio del señor Adolfo Arias Echandi, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
I. OBSERVACIONES GENERALES
(…)
1. La SUTEL solicita la inspección del 100% del contenido de los mensajes SMS, ante esta iniciativa se recomienda que el regulador valore la legalidad de dicha situación, o bien dimensione dicho requerimiento, dado que se estaría revisando información confidencial sin autorización expresa del cliente y sin media una orden judicial que lo habilite.

2. SUTEL solicita "...Contar con mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados en la red, que envían tráfico masivo…". Esta solicitud, en el caso del ICE, necesariamente requiere de la adquisición de una plataforma en específico, lo cual implica una fuerte erogación, de ahí es importante que el regulador si existe otra medida que, cumpliendo con el objetivo, no implique un alto costo regulatorio.

3. Para el punto de geolocalización (solicitado en el Apartado 9.1. Inciso C, Punto 5), se sabe, por el Oficio Nº 24-CJIC-2026, emitido por el Centro Judicial de Intervención de las Comunicaciones del Poder Judicial, el 24 de febrero del 2026, que esa entidad está en proceso de implementar un sistema denominado Location Based Services (LBS) el cual podría atender la iniciativa que SUTEL propone. Por lo tanto, se debe recomienda al Regulador que se comunique con el Centro Judicial de Intervención de las Comunicaciones para valorar si dicha plataforma puede cumplir con sus requerimientos.

4. No están definidos los parámetros que caracterizan un SMS como maliciosos, ni las reglas para alimentar dichos sistemas de protección. Asimismo, los requisitos descritos por SUTEL, no pueden ser considerados como un "filtro de seguridad" ni de una funcionalidad puntual, sino que es necesario implementar un ecosistema de seguridad, control y monetización SMS a nivel operador.

5. La implementación de lo pretendido por SUTEL, que es todo un ecosistema, requiere inversiones, actualización de versiones y rediseños de red, va más allá de aplicar "configuraciones" con lo cual el plazo de implementación propuesto para los operadores en general podría no se razonable ni proporcional, debiendo también considerarse los costos que esto implementan, así como su recuperación necesariamente en las tarifas asociadas a los servicios.

6. A partir del análisis funcional, técnico y operativo realizado, se determina que la implementación de los controles requeridos para la inspección, bloqueo, trazabilidad y mitigación de SMS maliciosos no puede abordarse como una integración simple ni como un filtro adicional sobre la infraestructura existente.

7. Los requisitos planteados que incluyen la inspección del 100 % del tráfico, la clasificación P2P/A2P, el control de rutas locales e internacionales, la validación de remitentes y entidades autorizadas, la detección avanzada de smishing, SIM Boxes, A2P bypass y tráfico artificialmente inflado exceden ampliamente las capacidades de soluciones puntuales o de corto plazo. Este nivel de control implica intervenir flujos críticos de red, introducir mecanismos de análisis profundo (DPI), inteligencia artificial, gestión de identidades de remitente, correlación de rutas y trazabilidad extremo a extremo.

8. Bajo parámetros de razonabilidad, proporcionalidad, no es técnicamente viable ni operativamente responsable implementar estas capacidades en un período de tiempo corto, ni mediante un componente aislado, dado que su correcta adopción requiere el diseño e integración de un ecosistema de seguridad SMS completo, de nivel operador, que involucra múltiples componentes interdependientes (SMS Firewall carrier-grade, módulos de IA/NLP, gestión de Sender ID, control de interconexión, threat intelligence y gobernanza A2P), así como la participación coordinada de áreas planificación, diseño, ciberseguridad, interconexión, B2B y cumplimiento regulatorio.

9. Debido a que la solución impacta directamente el plano de señalización, la entrega del tráfico y la experiencia del usuario final, su despliegue demanda fases de planificación, diseño, integración, pruebas, ajuste operativo y maduración, minimizando riesgos de falsos positivos, afectación de servicios críticos (como OTP o notificaciones) y desviaciones regulatorias.

10. En consecuencia, la iniciativa debe considerarse un proyecto estructural y estratégico, no una acción puntual o inmediata. Solo mediante un enfoque integral, progresivo y debidamente gobernado es posible alcanzar los objetivos de seguridad, trazabilidad y control exigidos, garantizando al mismo tiempo la estabilidad de la red, la conformidad normativa y la continuidad del negocio.

11. La metodología regulatoria contenida en la RCS-294-2023 fue concebida y aprobada con un alcance claramente delimitado a los servicios de voz y al fenómeno específico del enmascaramiento de llamadas. En ese sentido, la extensión de dicho marco hacia los servicios de mensajería SMS (P2P y A2P) no constituye una simple actualización o ajuste incremental, sino un cambio sustancial del régimen regulatorio aplicable, que introduce nuevos sujetos, riesgos, tecnologías y efectos operativos. Bajo principios de buena regulación, proporcionalidad y seguridad jurídica, dicha ampliación debería ser tratada como una nueva regulación, precedida de un análisis de impacto regulatorio integral que valore sus efectos técnicos, económicos, operativos, legales y de mercado.

12. Proporcionalidad de las medidas de bloqueo: La imposición de medidas de bloqueo absoluto sobre la totalidad del tráfico A2P no trazable, sin mecanismos claros de diferenciación entre tráfico legítimo e ilegítimo, introduce un riesgo significativo de afectación a servicios esenciales, tales como autenticaciones, notificaciones bancarias, servicios empresariales y comunicaciones críticas. Desde una perspectiva de proporcionalidad regulatoria, las medidas deberían permitir enfoques graduados y basados en riesgo, evitando afectaciones indiscriminadas a servicios que no presentan evidencia de comportamiento fraudulento.

II. OBSERVACIONES ESPECÍFICAS
(…)
APARTADO 9. SOBRE LA REGULACIÓN PROPUESTA
9.1. SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P

INCISO A.

Observaciones:

A efectos de tener claridad sobre el alcance de dicho inciso, es importante que se valoren el establecimiento de parámetros que permitan establecer en qué casos el tráfico se puede considerar o no malicioso.

En este sentido, por ejemplo: Si todo el tráfico ordinario de SMS sigue el mismo flujo ¿a qué se refiere con tráfico que intente evadir los controles? ¿tráfico que inicie con 506 (sin el +) o que no cumpla la NAI Internacional con CC?

Adicionalmente, debe considerarse que la problemática descrita por la propuesta se concentra primordialmente en el tráfico A2P y en el uso de rutas grises o no autorizadas.

En ese contexto, la aplicación de controles intensivos y homogéneos sobre el tráfico SMS P2P podría resultar innecesaria y desproporcionada, sin una correlación directa con el riesgo que se pretende mitigar.

INCISO C. PUNTO 5

Observaciones:

En dicho punto no se mencionan funciones de geolocalización ni densidad de señal dentro de la solución propuesta por la ITU, por lo que no indica cuál recomendación ITU se utilizó para la definición del requerimiento. Además, no se identifican esas necesidades en las implementaciones realizadas en otros países. Además, este tipo de planteamiento debe ser especificado, lo que probablemente incremente los costos de la solución por contratar por parte de los operadores.

Esto, por ejemplo, tendría la siguiente limitante: ¿Cómo podría un operador hacer un despliegue con cobertura a nivel nacional y funciones de geolocalización, para detectar que en determinado momento hay personas con Sin Boxes o con Fake-BTS/NodeB/eNodeB como los IMSI Catchers?

INCISO C. PUNTO 6

Observaciones:

En este punto es recomendable valorar si necesita algún complemento dado que a este tipo de función no se ha hace referencia dentro de la solución propuesta por la ITU.

INCISO C. PUNTO 14

Observaciones:

En cuanto a este punto, favor aclarar si el alcance está o no limitado a verificar la profundidad de todos los países para identificar que ninguno cumpla con 11 dígitos, dado que, por ejemplo, puede ser "basura". Además, ¿con esto se refieren a tráfico que inicie con 506 (sin el +) o que no cumpla la NAI Internacional con CC?

INCISO D

Observaciones:
A efectos de tener claridad sobre el alcance de dicho inciso, es importante que se defina sobre quien caería la responsabilidad de determinar cuándo un sitio es o no malicioso.

Por ejemplo: ¿Si un banco envía una campaña y por error se bloquean dichos mensajes, de quién es la responsabilidad?

Asimismo, debe detallarse el tipo de reporte y la solución a la que se debe integrar el operador para la entrega.

9.2 ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS P2P Y A2P

Observaciones:

La validación que plantea la propuesta SUTEL, se recomienda valorar que controlada por un tercer participante que asuma como de forma imparcial y rigurosa la ejecución de las validaciones. Se recomienda que dicha

propuesta sea puesta a discusión en el comité técnico de SUTEL (conformado por los operadores móviles y representantes del regulador).

En cuanto al diagrama de flujo para la normativa se hace la observación de que con RCS no se puede filtrar desde la capa de CS, seria en PS, por lo cual, bajo parámetros de razonabilidad técnica se solicita la perspectiva de SUTEL en cuanto si ¿habría que implementar filtros en la RAI? esto para el tráfico que no pase por la red móvil, por ejemplo, redes Wi-Fi que vienen de conexiones fijas, para envío de RCS).

9.3. SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P
INCISO A

Observaciones

La responsabilidad que se pretende establecer en dicho inciso debe ser compartida con los proveedores del servicio, contemplando, por ejemplo, que se les obligue a colocar un SMS Firewall para que esta mensajería no entre en la red del operador.

En el caso particular del tráfico A2P internacional, intervienen múltiples actores en la cadena de valor (agregadores, carriers internacionales, plataformas externas), cuyas operaciones y controles no se encuentran bajo el control efectivo del operador local. En consecuencia, no resulta razonable ni técnicamente viable exigir al operador garantizar trazabilidad "extremo a extremo" en toda la cadena global, debiendo la regulación reconocer los límites objetivos del control operacional y distribuir responsabilidades de forma acorde.

9.4. ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS A2P

Observaciones

En conjunto tanto los operadores y SUTEL pueden establecer los alcances y responsabilidades de los diferentes actores para determinar si las comunicaciones son legítimas o no, así como su participación en el proceso de validación por parte del tercero que se estaría encargando de entregar dicha legitimidad.

9.5. SERVICIOS DE LLAMADAS DE VOZ

Observaciones

Se solicita aclarar la funcionalidad de los números "señuelo" que el operador debe implementar.

Finalmente, en lo que respecta a los servicios de voz, se considera que no se justifica, en esta etapa, la imposición de nuevas obligaciones regulatorias adicionales, dado que la RCS-294-2023 ha demostrado resultados relevantes en la mitigación de llamadas fraudulentas mediante enmascaramiento, por lo que cualquier ajuste adicional debería sustentarse en evidencia objetiva y análisis específico de brechas persistentes.

9.6. SOBRE EL PLAZO DE IMPLEMENTACIÓN.

Observaciones
(…)
En los Apartados precedentes (9.1. a 9.5.) del documento en consulta SUTEL presenta una serie de requerimientos como: geolocalización, capacidad de inspección de 100% tráfico SMS, validación de MSISDN, validación de entidades A2P, plataformas de inteligencia Artificial, en otros; para los cuales el ICE no cuenta actualmente con infraestructura capaz de atender dichos requerimientos, ni licenciamiento para cumplir lo solicitado.

Bajo dichos términos y condiciones para el ICE no es viable cumplir con dicha implementación en el plazo de 180 días naturales, debido a que es necesario iniciar diversos procedimientos de contratación administrativa

que podrían exceder dicho plazo, siendo una condición particular del operador estatal el cual, contrario a los competidores privados, está sujeto a dicho régimen de contratación pública.

Por lo cual, y sin perjuicio de las observaciones técnicas realizadas en cuanto a los Apartados 9.1. a 9.5., se propone que ese plazo originario, se pueda ampliar, o prorrogar, en al menos 180 días naturales adicionales.

III. OSBERVACIONES COMPLEMENTARIAS

La propuesta de implementación y la definición de alcances que SUTEL le define a los operadores móviles provoca que, por errores materiales de la implementación tecnológica, comunicaciones fraudulentas sean total responsabilidad de los operadores, del mismo modo, un fallo en las definiciones del proceso de validación afectaría mensajería corta legítima que actualmente no presenta problemas. Los operadores no deben ser los responsables de generar los criterios técnicos que sean utilizados para el bloqueo de los mensajes sospechosos. Para garantizar la inocuidad de estos procesos lo correcto es que exista un tercer participante que asuma como de forma imparcial y rigurosa la ejecución de estas validaciones."

Las observaciones a la propuesta presentadas por el Instituto Costarricense de Electricidad (ICE) se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por el Instituto Costarricense de Electricidad (ICE) se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.4.1. Análisis de las observaciones realizadas por el Instituto Costarricense de Electricidad (ICE):

Respecto a lo indicado en la sección "***I. OBSERVACIONES GENERALES***" **punto 1** sobre la legalidad de realizar Inspección Profunda de Paquetes (DPI) en la totalidad del contenido de los mensajes SMS y su posible afectación a la privacidad de los usuarios, es importante mencionar que, esta Superintendencia es responsable respecto al cumplimiento del principio rector sobre privacidad de la información de los usuarios dispuesto en el artículo 3, inciso j) de la Ley N°8642 Ley General de Telecomunicaciones, que obliga a los operadores y proveedores a garantizar la intimidad y confidencialidad de la información de los usuarios de telecomunicaciones, por lo que, debe aclararse que la propuesta de realizar Inspección Profunda de Paquetes (DPI) en los mensajes SMS, no atenta contra dicho principio, ya que, en este contexto no implica la intervención de un humano para la lectura de los mensajes ni un acceso indiscriminado al contenido de estos por parte de humanos, sino que, corresponde a la implementación de una serie de reglas y controles que son aplicados por algoritmos informáticos y por medio de la Inteligencia Artificial para identificar patrones previamente definidos asociados a prácticas irregulares en el uso del servicio, como enlaces maliciosos, estructuras y firmas digitales conocidas típicas de smishing, por lo que, no se está ante una vulneración de la intimidad y confidencialidad de la información, sino ante un mecanismo automatizado, que de hecho más bien protege a la población de la recepción de mensajes malintencionados.

Este análisis se limita a elementos estrictamente necesarios para detectar amenazas en enlaces maliciosos o patrones sintácticos, y no se realiza almacenamiento permanente del

contenido de los mensajes, ya que, el análisis se realiza en tiempo real y con fines exclusivos de ciberseguridad, garantizando la destrucción de los datos una vez cumplan su cometido con el sistema de firewall.

Tal y como se describió en el documento sometido a consulta pública, la regulación propuesta contempla las mejores prácticas internacionales para la seguridad y protección de los usuarios, y no responde a alguna arbitrariedad u ocurrencia, dado que, la forma en que se propone en la regulación mitigar la problemática es la forma en que se aplica a nivel internacional, incluso reconocida por la Unión Internacional de Telecomunicaciones (UIT).

Es importante destacar que, la ausencia de este tipo de mecanismos deja a los usuarios expuestos a un incremento significativo de fraudes digitales, lo cual constituye una afectación directa a la seguridad de los usuarios, siendo que, la implementación de controles automatizados no debe entenderse como una vulneración a la privacidad, sino como una medida proporcional y necesaria para mitigar riesgos reales y crecientes, en línea con lo dispuesto en el artículo 42 de la Ley General de Telecomunicaciones que dispone la obligación de los operadores y proveedores de adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y los servicios de telecomunicaciones.

Por lo anterior, el uso de DPI para la detección de smishing, cuando se implementa bajo principios de privacidad, transparencia y proporcionalidad, no constituye una vulneración a la privacidad de los usuarios, sino una herramienta legítima y necesaria para su protección en el entorno digital actual, tomando en cuenta el nivel de intrusión mínimo al no involucrar intervención humana ni almacenamiento del contenido. Por lo anterior, se recomienda rechazar esta observación del operador.

Por otra parte, respecto a la observación señalada en el **punto 2 de la sección I**, sobre el requerimiento de mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados en la red, el operador señaló que deberá adquirir una plataforma en específico para cumplir con este requerimiento, lo cual implica una fuerte inversión económica, por lo que, consulta si existe otra medida que no implique un alto costo para cumplir con el objetivo de la propuesta regulatoria.
Al respecto, efectivamente existen configuraciones básicas y de menor costo que buscan minimizar el tráfico de mensajes maliciosos como análisis de tráfico, límite de mensajes por minuto o firewalls de SMS, sin embargo, ninguno de estos permite identificar y localizar dispositivos dañinos conectados a la red o que generan cantidades masivas de tráfico P2P mediante aparatos como SimBoxes. Por lo que, siendo que el objetivo de la propuesta es establecer un marco regulatorio robusto y actualizado a las tecnologías recientes para la prevención y lucha contra el smishing, es que se requiere la implementación de medidas avanzadas que permitan localizar la conexión y uso de estos dispositivos, siendo que la mitigación de prácticas prohibidas, la protección de los usuarios, la seguridad de la red y la preservación de la integridad del servicio son responsabilidades inherentes a la actividad de los operadores. Por lo anterior, se recomienda rechazar esta observación.

Sobre la observación indicada en el **punto 3** de la **sección I** respecto a la valoración por parte de la Sutel del oficio Nº 24-CJIC-2026 emitido por el Centro Judicial de Intervención de las Comunicaciones del Poder Judicial, cabe indicar que, dicho oficio no fue aportado por el operador, de modo que, no es posible realizar un análisis de su contenido y evaluación de fondo sobre esta observación. No obstante, se reitera lo señalado anteriormente en cuanto a que no se está ante una vulneración de la intimidad, confidencialidad o mucho menos ante una escucha o intervención de comunicaciones, siendo que, como ya se indicó, de acuerdo con las mejores prácticas internacionales se cuenta con algoritmos computacionales y el apoyo de la Inteligencia Artificial para identificar una serie de reglas establecidas que permiten filtrar los mensajes maliciosos sin la intervención de personas que pudieran conocer o difundir la información, siendo éstos análisis automatizados en tiempo real. Por lo anterior, se recomienda rechazar esta observación

En cuanto a la observación del **punto 4** de la **sección I** sobre los parámetros que caracterizan un mensaje SMS como malicioso y las reglas para alimentar dichos sistemas de protección, es importante mencionar que, no existe una regla definida sobre como catalogar un mensaje como malicioso, sino que, la correlación del resultado de varios análisis y la probabilidad de riesgo ante estos análisis definen un mensaje como fraudulento.

Es decir, a partir de los resultados de análisis por Inspección Profunda de Paquetes (DPI), análisis de comportamiento como volúmenes o frecuencia de mensajes anormales, verificación de enlaces contra sistemas de reputación, validación y trazabilidad de campañas A2P, detección de campañas de mensajes, es que los sistemas de firewall correlacionan esta información para clasificar un mensaje como potencialmente sospechoso, y basado en umbrales y políticas definidas tanto por el operador como por el proveedor de la solución de firewall SMS es que se decide que un mensaje es malicioso y debe ser bloqueado. Cabe señalar que, existen empresas y sistemas especializados en este tipo de tratamientos que permiten la identificación y bloqueo de mensajes maliciosos.

Asimismo, los proveedores de las soluciones de firewall SMS para detección de mensajes sospechosos cuentan con reglas y modelos ya definidos para la identificación de mensajes maliciosos basados en Inteligencia de Amenazas (Threat Intelligence), que corresponde a información global detallada y ejecutable sobre amenazas de ciberseguridad para ayudar a los equipos de seguridad a detectar, mitigar y prevenir los ciberataques de forma proactiva.

La inteligencia de amenazas, más que solo ser información sobre amenazas, es información correlacionada y analizada para ofrecer a los sistemas de la seguridad un conocimiento profundo sobre posibles amenazas, incluyendo cómo detenerlas[14].

Por lo anterior, no existe un único criterio exacto para definir un mensaje SMS como malicioso, sino que, los sistemas de firewall SMS identifican patrones y probabilidades de riesgo mediante la combinación de múltiples indicadores, permitiendo además adaptarse y

[14] https://www.ibm.com/es-es/think/topics/threat-intelligence

evolucionar frente a nuevas amenazas de smishing. Por lo anterior, se recomienda rechazar esta observación

Sobre las observaciones de los **puntos 5**, **6**, **7**, **8**, **9** y **10** de la **sección I** respecto a la preocupación por parte del operador ante el plazo inicialmente otorgado de 180 días, como se determinó anteriormente, dicho plazo será ampliado considerando que se recibió por parte de otro operador, una propuesta detallada de calendario gradual de implementación con plazos razonables para la puesta en funcionamiento de cada uno de los requerimientos dispuestos en la regulación sometida a consulta pública, y estará dividida en 3 fases, iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas de filtrado en SMS y posteriormente 2 fases adicionales, 12 meses (360 días) para aplicar medidas avanzadas en el tráfico de SMS y 18 meses (540 días) para medidas de voz. Por lo anterior, se recomienda acoger estas observaciones.

Con respecto a la observación del **punto 11** de la **sección I** sobre que la presente propuesta sea tratada como una nueva regulación, ya que el operador considera que la metodología regulatoria contenida en la resolución RCS-294-2023 fue concebida y aprobada con un alcance delimitado a los servicios de voz y al enmascaramiento de llamadas, siendo que la presente regulación no es una simple actualización sino que implica un cambio sustancial del régimen regulatorio aplicable, lo cual requiere un análisis del impacto regulatorio que valore sus efectos.

Al respecto, debe señalarse que; si bien es cierto, la resolución RCS-294-2023 enmarca la regulación para minimizar el impacto de estafas telefónicas mediante el método del enmascaramiento de llamadas, su fundamento al igual que la presente propuesta regulatoria, radica en la necesidad de una cooperación de los operadores y proveedores de servicios de telecomunicaciones en contra de la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en el desarrollo de tecnologías de la información y prevenir los actos dirigidos contra la confidencialidad, integridad, disponibilidad de sistemas informáticos, redes, datos, así como el abuso de tales sistemas, lo cual se deriva de las iniciativas de ajuste a la Ley N° 9048 y la Ley N° 9135 que reformaron al Código Penal, para la incorporación de los delitos informáticos y conexos.

Por otra parte, la Ley N°8642 es conteste con lo desarrollado en la Ley N°7593, siendo que resulta de vital importancia la protección de los derechos de los usuarios finales de los servicios de telecomunicaciones, y aboga por que exista un desarrollo de las telecomunicaciones que contribuya con la seguridad ciudadana, para lo cual los operadores deben adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios, conforme al artículo 42 de la Ley 8642.

Después de la emisión de la resolución RCS-294-2023, y ante la evidencia de que las modalidades de fraude han migrado hacia otros medios tecnológicos (particularmente la mensajería de texto SMS en sus modalidades P2P y A2P), la Dirección General de Mercados mediante oficio número 03422-SUTEL-DGM-2025 del 24 de abril de 2025 realizó una consulta a los operadores y proveedores con numeración asignada, con el fin de

recabar criterios técnicos sobre acciones adicionales que permitan ampliar el alcance de las medidas de bloqueo y mitigación del fraude en redes públicas de telecomunicaciones.

De las respuestas recibidas, se desprenden elementos comunes relevantes: **i)** la factibilidad de reforzar la autenticación del identificador de origen en troncales SIP mediante mecanismos como P-Asserted-Identity y controles de ANI por troncal, con el objetivo de impedir la suplantación de numeración asignada; **ii)** la necesidad de incorporar controles específicos sobre tráfico de mensajería A2P, dada su naturaleza automatizada y su potencial para facilitar campañas masivas de smishing; **iii)** la conveniencia de adoptar medidas basadas en estándares internacionales de autenticación y verificación del origen como el OOBS.

Es por ello, que en el oficio número 02238-SUTEL-DGM-2026 del 06 de marzo de 2026 sometido a consulta pública, se realiza un amplio análisis técnico sobre el smishing y vishing, los SMS A2P y P2P, así como los mecanismos de bloqueo y filtrado específicos para SMS sin desnaturalizar el servicio ni vulnerar el marco de privacidad, y que delimiten finalidades, controles y salvaguardas de tratamiento de datos, con el objetivo de garantizar la seguridad de los usuarios finales y las redes de los operadores.

Lo anterior, de igual forma tiene su asidero normativo en el Reglamento sobre el Régimen de Protección al usuario final, el cual es explícito en señalar en el numeral 106 lo relativo a las prácticas prohibidas por parte de los usuarios, donde se prohíbe a estos: *“alterar o poner en riesgo la operación normal de la red y su seguridad, así como degradar la calidad del servicio; acciones que provoquen interferencias, interrupciones, congestión o daños a la red y a otros usuarios de los servicios de telecomunicaciones; actuar con engaño, fraude, mala fe, dolo en la suscripción o uso del servicio; utilizar los servicios de telecomunicaciones para fines distintos del contratado”*. Por lo que se faculta al operador/proveedor para suspender el servicio de forma temporal y en caso de que no se corrija dicha condición en el plazo de dos meses, proceder con la suspensión definitiva, liquidación contable y la disposición del recurso numérico. De igual forma, el artículo 75 del citado reglamento dispone la suspensión de servicios prepago en caso de determinarse la comisión de prácticas prohibidas.

Adicionalmente, el artículo 5 incisos 7) y 8) del citado Reglamento establece dentro de las obligaciones de los usuarios finales, las siguientes: *"(...) **7.** Evitar el envío de comunicaciones que puedan perjudicar los derechos de los demás usuarios finales y la seguridad de las redes de los operadores/proveedores. **8.** Abstenerse de realizar prácticas prohibidas o de utilizar los servicios de telecomunicaciones para fines distintos del contratado (...)"*. En caso de verificarse dichas conductas, se dispone que los contratos de servicios de telecomunicaciones se extinguirán conforme al numeral 47 inciso 4) del mismo cuerpo normativo. Asimismo, en concordancia con la recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1244, las amenazas por comunicaciones maliciosas y falsificación de identidad ocurren en plataformas convergentes, lo que exige una defensa multidimensional (voz y datos) apoyada en las normas vigentes como lo es la RCS-294-2023.

Es decir, existe un marco normativo de rango superior que en aras de la protección de los derechos de los usuarios de los servicios de telecomunicaciones establece obligaciones para los usuarios y operadores, como en el caso de las prácticas prohibidas, de manera

que la regulación propuesta es complementaria a la previamente emitida con la finalidad de establecer las disposiciones para la gestión del tráfico SMS con el fin de garantizar la seguridad de los usuarios, evitando prácticas como el “smishing” entre otras, ya que, tal y como el operador lo reconoce, actualmente se implementan acciones idénticas a las propuestas para los servicios de voz, por lo tanto, no se está ante una regulación novedosa o sorpresiva para los operadores, en el tanto la propuesta sometida a consulta resulta necesaria para la protección de los usuarios, para la seguridad de las redes y los servicios, además que, los operadores tienen experiencia en la implementación de las medidas planteadas. Por tanto, se recomienda acoger parcialmente los argumentos del Instituto Costarricense de Electricidad (ICE) y emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

En cuanto a la observación del **punto 12** de la **sección I**, respecto a las posibles afectaciones a servicios de autenticación y notificación ante un bloqueo absoluto de la totalidad del tráfico A2P no trazable, el operador solicita que la medida regulatoria permita enfoques graduados y basados en riesgo, evitando afectaciones indiscriminadas a servicios que no presentan evidencia de comportamiento fraudulento. Al respecto, basado en esta y otras observaciones relacionadas a este asunto, como se indicó anteriormente en este documento, gran parte de los mensajes A2P corresponden a mensajes de autenticación con información sensible para el acceso a cuentas personales de los usuarios, de modo que, es indispensable que se garantice la integridad de la información de extremo a extremo y por ende su trazabilidad, ya que, un mensaje sin información de trazabilidad no garantiza que no haya sido interceptado por ciberdelincuentes. Por lo anterior, no es de recibo la propuesta del operador, de modo que, se debe permitir el tránsito únicamente de mensajes A2P con información de trazabilidad, así como analizar la coherencia en las comunicaciones, es decir, verificar en tiempo real que el origen de la comunicación coincida con la ruta por la que ingresa y el operador conectado a dicha ruta, de modo que, deberán bloquear cualquier comunicación que no muestre esta coherencia en la trazabilidad. De igual manera, como se señaló anteriormente, los operadores pueden implementar registros de excepciones para clientes autorizados a enviar mensajes informativos de forma masiva, para evitar afectaciones indiscriminadas a servicios que no presentan evidencia de comportamiento fraudulento. Por lo anterior, se recomienda rechazar esta observación.

En lo que respecta a las observaciones de la **sección II** para la **sección 9.1** de la regulación sometida a consulta pública, sobre el inciso A el operador solicita se aclare *“(…) ¿a qué se refiere con tráfico que intente evadir los controles? ¿tráfico que inicie con 506 (sin el +) o que no cumpla la NAI Internacional con CC? (…)”*. Al respecto, se indica que, esto se refiere a cualquier mecanismo o situación donde un operador local o internacional enmascare recursos numéricos para simular tráfico internacional como local para la terminación de mensajes.

Además, en dicha observación el operador señaló que la aplicación de controles intensivos y homogéneos sobre el tráfico SMS P2P podría resultar innecesario y desproporcionado, sin una correlación directa con el riesgo que se pretende mitigar. Lo señalado por el Instituto Costarricense de Electricidad (ICE) no resulta coherente, ya que, como se ha indicado ampliamente en este documento, la ausencia de mecanismos avanzados y automatizados de análisis de tráfico deja a los usuarios expuestos a un incremento significativo de fraudes

digitales, afectando la seguridad de los usuarios, por lo que, contrario a lo manifestado por el operador, la aplicación de medidas intensivas y avanzadas es proporcional y necesario para mitigar riesgos reales y crecientes relacionados al smishing.

En cuanto a la observación sobre que recomendación de la UIT específica se utilizó para requerir mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados a la red como SimBoxes, es importante aclarar que, no existe una recomendación específica sobre este requerimiento, sino que, comprende el análisis y correlación de varios indicadores de red que permiten identificar dispositivos de envío masivo de mensajes SMS, como comportamiento de movilidad, volumen de tráfico, patrones de envío, simetría de comunicaciones y ubicaciones estáticas de tarjetas SIM, ya que, dispositivos como Simboxes suelen permanecer en ubicaciones fijas, además, dado que los Simboxes concentran grandes cantidades de servicios móviles en un mismo punto, generan volúmenes de tráfico anormales en una sola radiobase, e incluso en una sola celda, por lo que, este comportamiento respecto a incrementos anómalos en el volumen del tráfico por varios servicios que pasan la mayor parte del tiempo conectados a una sola radiobase, permite mediante el análisis de movilidad, patrones de comportamiento y volumen de tráfico detectar equipos como Simboxes que generan tráfico de forma masiva de forma imprevisible para la red. Esto sumado a servicios de localización LBS (Location Based Services) ya integrados en las redes móviles permite estimar la posible ubicación de estos equipos. Cabe señalar que, para el objetivo de esta disposición regulatoria es indispensable identificar y frenar el uso de Simboxes, ya que, de estos envían de forma masiva mensajes con intentos de smishing a usuarios de todo el país, siendo estos equipos los mayormente utilizados para prácticas de smishing y uso de rutas grises.

Es importante mencionar que, en el mercado existen proveedores de soluciones de firewall SMS que ofrecen detección de SimBoxes y detección de rutas grises, basados en los análisis mencionados anteriormente y apoyados con Inteligencia Artificial para correlacionar el resultado de dichos análisis y determinar de forma automática la probabilidad de que un equipo de estos se encuentre conectado en la red, así como su ubicación estimada.

Basado en el principio de neutralidad tecnológica dispuesto en el artículo 3 inciso h) de la Ley N°8642, esta Superintendencia no tiene la potestad de recomendar un proveedor o tecnología específica para localizar SimBoxes, por lo que, queda a discreción del operador los mecanismos que implementará para cumplir con la regulación propuesta. Por lo anterior, se recomienda rechazar esta observación.

Sobre la observación de la **sección II** para el **apartado 9.1** de la propuesta sometida a consulta pública, específicamente sobre el **inciso C subinciso 6)** respecto al uso de Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP) y Análisis Heurístico para la lucha contra el smishing, el operador recomendó: *"(…) valorar si necesita algún complemento dado que a este tipo de función no se ha hace referencia dentro de la solución propuesta por la ITU (…)"*. Al respecto, es importante mencionar que, la UIT no dispone de una recomendación específica para cada aspecto puntual en la propuesta regulatoria, lo que si tiene son marcos técnicos que promueven mecanismos adaptativos para análisis y procesamiento anti-spam. En la propuesta regulatoria se mencionó que, la recomendación ITU-T X.1247 señala la

importancia de utilizar mecanismos adaptativos que se ajusten a los nuevos tipos de spam que surgen constantemente y sus variaciones, por lo que, la solución implementada por parte de los operadores para combatir el smishing debe disponer de dominios de seguridad con capacidades de detección, administración y procesamiento del tráfico de mensajes maliciosos para bloquear su tráfico, de modo que, el uso de Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP) y Análisis Heurístico para detectar patrones de smishing se ajusta con la citada recomendación como un mecanismo de detección adaptativo y ajustable ante nuevas amenazas para la seguridad de la red y los derechos de los usuarios. Por lo anterior, se recomienda rechazar esta observación.

Respecto a la observación de la **sección II** para el **apartado 9.1** de la regulación sometida a consulta pública, específicamente sobre el **inciso C subinciso 14)**, donde el operador solicitó aclarar si el alcance está o no limitado a verificar la profundidad de todos los países para identificar que ninguno cumpla con 11 dígitos, cabe señalar que, este requerimiento se refiere a cualquier mecanismo o situación donde un operador local o internacional enmascare recursos numéricos para simular tráfico internacional como local para la terminación de mensajes. De modo que, se recomienda rechazar esta observación.

En lo relativo a la observación de la **sección II** para el **apartado 9.1** de la regulación sometida a consulta pública, específicamente sobre el **inciso D** respecto al uso de sistemas de reputación de enlaces para bloquear mensajes que contengan enlaces a sitios WEB maliciosos, el operador solicita que se defina sobre quién recae la responsabilidad de determinar que un sitio es malicioso, brindando como ejemplo una campaña de mensajes enviada por un banco y bloqueada por error. Cabe reiterar que, los sistemas de reputación de enlaces funcionan asignando una puntuación basada en factores como la antigüedad del sitio Web, cambios de ubicación históricos, indicios de actividades sospechosas, o detección de malwares al analizar el contenido del sitio Web[15], de modo que, para que un sitio sea considerado como malicioso debe cumplir con varios requisitos que den como resultado una puntuación que se considere de riesgo. Aun así, esta Superintendencia es consciente que ningún sistema de este tipo puede garantizar la nula probabilidad de falsos positivos, de modo que, es importante aclarar que, el bloqueo de mensajes maliciosos no se limita al uso de sistemas de reputación de enlaces, sino que, comprende el análisis y la correlación de la información obtenida mediante cada uno de los requerimientos dispuestos en la regulación propuesta, es decir, la correlación de la información obtenida de sistemas de reputación con listas blancas o de excepción permite disminuir la probabilidad de falsos positivos. Además, como se indicó en la sección 9.3 inciso E. de la propuesta sometida a consulta pública, todos los operadores y proveedores deben establecer registros de las entidades autorizadas para el envío de mensajes SMS A2P, de modo que, los operadores pueden implementar listas de excepción con registros de clientes autorizados para enviar mensajes A2P de forma masiva donde cada operador sabe cuáles clientes están autorizados a remitir grandes volúmenes de mensajes.
Asimismo, sobre el tipo de reporte requerido en este mismo inciso y la solución a la que se debe integrar el operador para su entrega, cabe señalar que, la propuesta señala que los operadores y proveedores deberán reportar a la Sutel los mecanismos implementados

[15] https://docs.trendmicro.com/en-us/documentation/article/trend-micro-web-security-online-help-about-web-reputation

respecto a los sistemas de reputación de enlaces, es decir, informar sobre que mecanismo fue adoptado por el operador, de modo que, no se requiere un tipo de reporte definido o reiterado, solamente un informe que detalle los mecanismos implementados para el cumplimiento de este punto, que podrá ser entregado mediante los canales oficiales de Sutel para recibir documentación. Por lo anterior, se recomienda rechazar esta observación.

Respecto a la observación de la **sección II** para el **apartado 9.2** de la regulación propuesta, es importante indicar que, el operador no es claro sobre los términos relacionados a la CS, PS y RAI ni su relación con redes Wi-Fi, de modo que, esta Superintendencia no se puede referir a dicha observación debido a que no se tiene claridad sobre las consultas planteadas por el operador, de modo que se recomienda rechazar esta observación. Aun así, cabe reiterar que le corresponde a los operadores y proveedores realizar los ajustes necesarios para cumplir los requerimientos propuestos y responsabilizarse por el tráfico que cursa sus redes.

Sobre la observación de la **sección II** para el **apartado 9.3** de la propuesta sometida a consulta pública, específicamente sobre el **inciso A**, el operador solicita que la responsabilidad sea compartida con proveedores de servicio del tráfico A2P internacional. Al respecto, la regulación propuesta claramente establece que dichas medidas aplican para la totalidad de operadores y proveedores de servicios de telecomunicaciones que brindan servicios de mensajería SMS y generen tráfico de tipo A2P, así como, para los operadores y proveedores que reciban mensajes SMS A2P por rutas de interconexión internacional o local.

Asimismo, en esta observación el operador también solicitó que se reconozcan los límites objetivos del control operacional para garantizar la trazabilidad de extremo a extremo en todas las comunicaciones, y distribuir responsabilidades entre agregadores, carriers internacionales, plataformas externas cuyas operaciones y controles no se encuentran bajo el control del operador. Al respecto, es importante mencionar que, agregadores o plataformas internacionales se encuentran fuera del alcance regulatorio de esta Superintendencia, por lo que, como se indicó anteriormente, la regulación propuesta aplica para la totalidad de operadores y proveedores de servicios de telecomunicaciones que brindan servicios de mensajería SMS. Además, como ya se ha hecho ver en este documento, los mensajes A2P son utilizados para el envío de información sensible de autenticación para cuentas de usuario, por lo que, es de vital importancia garantizar su trazabilidad de extremo a extremo con el fin de asegurar su integridad y confidencialidad desde su origen y hasta el usuario final, por lo que, los operadores y proveedores deben revisar los acuerdos pactados con agregadores y plataformas internacionales para ajustarse a los requerimientos dispuestos en la presente actualización regulatoria, de cara a las responsabilidades establecidas. De modo que, se recomienda rechazar esta observación.

Respecto a la observación de la **sección II** para el **apartado 9.4** de la regulación propuesta, es importante reiterar que el operador de servicios de telecomunicaciones es responsable del tráfico que transita por sus redes, tal y como lo dispone el artículo 64 del Reglamento de Acceso a Interconexión de Redes de Telecomunicaciones, cada operador o proveedor

será responsable de implementar los mecanismos relacionados con el manejo fraudulento o uso no autorizado de los servicios en sus respectivas redes, para lo cual, deberá existir una comunicación constante entre las partes, de forma que se pueda prevenir, controlar, detectar y erradicar el uso no autorizado de las redes de telecomunicaciones de forma consistente con lo dispuesto en el artículo 42 de la Ley General de Telecomunicaciones respecto a: *"Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios."* Por lo anterior, se recomienda rechazar esta observación.

En lo relativo a la observación de la **sección II** para el **apartado 9.5** de la regulación propuesta donde el operador cuestiona la funcionalidad de los números señuelos, de la misma forma que se indicó en el inciso B de dicho apartado, la implementación de números cebos o señuelo facilitan la identificación de generadores de spam, ya que, corresponden a rangos numéricos no asignados a usuarios finales y por ende no deberían recibir comunicaciones. El uso de números señuelos en servicios de voz es promovido en la recomendación ITU-T X.1246 para atraer generadores de spam.

Asimismo, la recomendación UIT-T X.1247 promueve el uso de señuelos con números de teléfono no otorgados a usuarios para detectar el tráfico spam en mensajería SMS, de este modo, todos los mensajes que sean distintos de los previstos pueden ser procesados como tráfico sospechoso para analizar su contenido. Además, dicha recomendación señala que los señuelos deben cumplir una etapa de aprendizaje para verificar el tráfico sospechoso y filtrar el tráfico que no es spam antes de generalizar sus características, ya que, un usuario por error puede realizar una comunicación a estos números señuelos, sin que corresponda a un hecho que atente contra la seguridad. Por lo anterior, se recomienda rechazar esta observación.

Por otra parte, en dicha observación el operador manifiesta que no se justifica la imposición de nuevas medidas regulatorias adicionales a la resolución RCS-294-2023, dado que esta ha demostrado resultados relevantes en cuanto al bloqueo de llamadas enmascaradas. Al respecto, si bien es cierto que la implementación de dicha medida ha evidenciado el bloqueo de grandes volúmenes de llamadas enmascaradas, y que a su vez, ha colaborado con la seguridad ciudadana, es importante mencionar que, los ataques de vishing no se limitan exclusivamente al enmascaramiento de llamadas, por el contrario, los delincuentes utilizan todos los medios a su alcance para obtener información sensible de los usuarios, siendo el enmascaramiento de llamadas solo uno de estos, por lo que, la regulación propuesta busca complementar la resolución RCS-294-2023 y cerrar brechas adicionales al enmascaramiento de llamadas. Por lo que, cada uno de los requerimientos señalados en la regulación sometida a consulta pública tiene como objetivo ampliar el alcance de la citada resolución y maximizar la eficiencia en los sistemas de seguridad y prevención para minimizar el impacto de los ciberataques mediante mensajes de texto SMS (Smishing) y llamadas (Vishing).
Además, el hecho de que una normativa haya dado resultados positivos en un área específica no significa que no pueda mejorarse para aumentar su alcance o incorporar otras áreas que igualmente requieren intervención, máxime como se ha indicado considerando

la capacidad y velocidad de adaptación de los defraudadores. Por lo que, se recomienda rechazar esta observación.

Sobre la observación de la **sección II** para el **apartado 9.6** de la regulación sometida a consulta pública, el operador solicita que el plazo original de 180 días naturales otorgado en la citada normativa se pueda ampliar, o prorrogar, en al menos 180 días naturales adicionales debido a los procedimientos de contratación pública que debe cumplir este operador. Al respecto, como se indicó anteriormente en este documento, se recomienda acoger la propuesta para implementar un calendario gradual según la propuesta aportada por otro operador, la cual se desglosa en 3 fases, iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas en cuanto a servicios de mensajería SMS y posteriormente 2 fases adicionales para medidas avanzadas con plazos para puesta en operación de 12 meses (360 días) para completar las mediadas aplicables a los servicios de mensajería SMS y 18 meses (540 días) para la implementación de los requerimientos de seguridad para servicios de voz.

Lo anterior atiende la solicitud del Instituto Costarricense de Electricidad (ICE) respecto a prorrogar en al menos 180 días naturales adicionales al plazo original, al determinar 360 días naturales para la implementación total incluyendo las medidas avanzadas en servicios de mensajería SMS que requerirán la contratación de nuevos servicios por parte de los operadores y 540 días naturales para los requerimientos relacionados a servicios de voz. De modo que, se recomienda acoger esta observación.

Finalmente, respecto a la observación planteada en la **sección III** sobre la responsabilidad de los operadores para generar los criterios técnicos utilizados para el bloqueo de los mensajes sospechosos y la inclusión de un tercer participante que asuma de forma imparcial y rigurosa la ejecución de estas validaciones, cabe señalar que, dicha preocupación respecto a una eventual asignación de responsabilidad a los operadores por errores en la implementación de mecanismos antifraude no resulta consistente con la naturaleza de la prestación de servicios de telecomunicaciones ni con las prácticas en materia de seguridad, ya que, los operadores son responsables de la gestión, operación y seguridad de sus redes, incluyendo la integridad del tráfico que cursa por ellas. En este contexto, la implementación de medidas para la detección y mitigación de prácticas irregulares, como el smishing o el vishing, no constituye una función delegable a un tercero, sino una obligación propia de la prestación de los servicios y seguridad de la red de telecomunicaciones.

Trasladar la generación o definición de criterios técnicos de validación y bloqueo a un tercer participante no solo diluye la responsabilidad del operador, sino que, introduce riesgos adicionales en términos de latencia operativa, dependencia externa y falta de alineación con las características específicas de cada red, además, resulta contrario a las mejores prácticas internacionales que se plantearon en el informe que respalda la regulación sometida a consulta pública. Cada operador posee visibilidad, infraestructura y capacidades técnicas únicas sobre su tráfico, lo que lo posiciona como el actor idóneo para definir e implementar mecanismos de control efectivos.

Cabe señalar que, los sistemas automatizados de detección de fraude que propone esta propuesta regulatoria complementaria están diseñados para operar bajo esquemas de mejora continua, donde los criterios de detección son ajustables dinámicamente para minimizar tanto los falsos negativos como los falsos positivos. Cada sistema formará parte del ambiente técnico y operativo de cada operador, por lo que, no puede ser completamente estático ni predefinido por una entidad externa.

En cuanto al riesgo de afectación a tráfico legítimo, si bien es un posible desafío en cualquier sistema de filtrado, no constituye un argumento para evitar su implementación y dejar a los usuarios al descubierto en cuanto a los intentos de fraude que se incrementan a diario, siendo que, existen mecanismos para mitigar este riesgo como listas blancas, validación de remitentes, monitoreo y ajustes en los umbrales de detección. Esto sumado a sistemas ágiles de atención de reclamaciones de los usuarios permite garantizar un balance adecuado entre seguridad y continuidad de los servicios, sin necesidad de renunciar a la implementación de controles efectivos y modernos que minimicen el impacto de los ciberataques.

Es importante destacar que, la ausencia de medidas antifraude sí genera una afectación directa y comprobada sobre los usuarios, exponiéndolos a riesgos económicos y de seguridad. En este sentido, el costo de la inacción del operador es significativamente mayor que el riesgo controlado de eventuales ajustes en los sistemas de detección.

Por lo anterior, le corresponde a cada operador definir, implementar y ajustar los criterios técnicos que considere más adecuados para cumplir con el objetivo y los requerimientos de la propuesta regulatoria sometida a consulta pública, asumiendo plenamente la responsabilidad sobre su eficacia, de modo que, los operadores son responsables de definir, desarrollar y ajustar los criterios técnicos asociados a la detección de tráfico malicioso. Delegar a un tercero como responsable de estas funciones no resulta necesaria ni conveniente, y podría comprometer la efectividad y agilidad de los mecanismos de protección que busca la normativa y la regulación propuesta, los cuales son requeridos en un entorno de amenazas dinámicas. Por lo anterior, se recomienda rechazar esta observación.
Con base en el análisis anterior, se recomienda acoger parcialmente los argumentos del Instituto Costarricense de Electricidad (ICE) y emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

Además, se recomienda acoger la observación sobre ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente en este documento y presentada por parte de Claro CR Telecomunicaciones S.A. (Claro). Se recomienda rechazar las observaciones restantes planteadas por este operador.

3.5. Posición de Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty):
Mediante el oficio LY-Reg0090-2026 del 24 de abril de 2026 (NI-05533-2026) Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty) por medio del señor Donato Rivas Garro, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
A. Consideraciones Iniciales

(…) mi representada considera que el abordaje de esta problemática debe realizarse integralmente, incorporar a los demás actores claves, y sustentarse en una cooperación entre operadores y proveedores de telecomunicaciones, otros actores privados claves, esta Superintendencia y otras instituciones competentes, en un marco de combate contra la ciberdelincuencia y el fortalecimiento de la seguridad informática.

Tal como se menciona e incluso se subraya en el oficio en cuestión, el artículo 2, inciso f), de la Ley n.° 8642, Ley General de Telecomunicaciones, establece dentro de uno de los objetivos del régimen de telecomunicaciones el apoyo a la seguridad ciudadana. Dicha referencia no debe interpretarse como la imposición de una obligación exclusiva a los operadores de telecomunicaciones, ni mucho menos como fundamento para la aplicación de sanciones ante eventuales incumplimientos, sino como un deber de colaboración en el marco de un esfuerzo articulado y compartido entre los distintos actores públicos y privados.

En este sentido, dicho objetivo debe entenderse como un principio orientador de políticas públicas coordinadas, y no como una transferencia desproporcionada de responsabilidades a un solo sector regulado.

Adicionalmente, más allá de las potestades de esta Superintendencia, resulta contrario a la proporcionalidad y la razonabilidad reiteradamente exigidos por la Sala Constitucional, entre otras, en la resolución Nº 12746 – 2019, del 10 de Julio del 2019 a las 12:11, que el abordaje de esta problemática y las medidas propuestas, se limiten y se circunscriban a la imposición de obligaciones exclusivas a los operadores y proveedores de telecomunicaciones.

Por todo lo anterior, consideramos que el alcance del oficio propuesto constituye una extralimitación en su interpretación o aplicación, siendo contrario a la Ley General de Telecomunicaciones, así como a los principios de legalidad, razonabilidad y seguridad jurídica que rigen la actuación administrativa.

B. Impacto Económico y Ausencia de Mecanismos Compensatorios o Incentivos Económicos.

Liberty es consciente de los fines que persigue esta Superintendencia con esta propuesta, no obstante, considera fundamental que cualquier metodología que se proponga se diseñe bajo un análisis de impacto regulatorio, que, entre otros, contemple los costos del proyecto y su impacto económico.

Resulta difícil de justificar que las medidas propuestas deban ser sufragadas de forma exclusiva por los operadores y proveedores de telecomunicaciones, cuando se trata de un fenómeno complejo y multifactorial que involucra a múltiples actores del ecosistema digital.
Por esto, Liberty estima que tanto el financiamiento como la ejecución de las medidas deberían distribuirse de manera más equilibrada entre todos los actores involucrados.

Alternativamente, consideramos necesario que la imposición de tales obligaciones se acompañe de mecanismos compensatorios o incentivos económicos, que permitan mitigar el impacto financiero que estas cargas puedan generar sobre los operadores y proveedores. La ausencia de este tipo de mecanismos no solo implica una transferencia desproporcionada de costos económicos y operativos hacia un único sector, sino que también puede afectar negativamente la inversión, la innovación y la sostenibilidad de los servicios de telecomunicaciones, en contravención de los objetivos de desarrollo e inversión previstos en la Ley General de Telecomunicaciones.

C. Violación al principio de neutralidad tecnológica.

La regulación propuesta y específicamente la obligación de implementar en nuestras redes sistemas de firewall para mensajería SMS con capacidades adaptativas de identificación, análisis y filtrado, apoyados con Inteligencia Artificial violenta a todas luces el principio de neutralidad tecnológica del inciso h) del artículo 3 de la Ley General de Telecomunicaciones.

La implementación obligatoria de estas medidas a través de una resolución administrativa, con especificaciones concretas sobre el uso de una tecnología, quebranta el principio de reserva de ley que recepta el artículo 39 de la Constitución Política.

D. Limitaciones de la responsabilidad derivada de las obligaciones de terceros en el tráfico internacional

De igual manera, debe de analizarse con especial cautela la responsabilidad que se pretende delegar a los operadores y proveedores de servicios de telecomunicaciones, sobre el tráfico internacional del servicio de mensajería de texto y sus diferentes modalidades. Por ejemplo, en el punto 9, se dispone que los sistemas de firewall a ser implementados, deben de tener la capacidad de: identificar tráfico de tipo P2P o A2P que ingresa a la red del operador por rutas de interconexión internacional, detectar y bloquear la totalidad del tráfico de tipo A2P o P2P con origen internacional, bloquear la totalidad del tráfico A2P que ingrese a sus redes por rutas de interconexión internacional o local, simulando de cualquier manera ser de tipo P2P o aquel en el que se enmascare el número de origen, etc.

Adicionalmente, la aplicación de este tipo de medidas sobre el tráfico internacional podría generar distorsiones en los precios de los servicios de mensajería, al trasladar a los operadores y proveedores costos adicionales derivados del bloqueo, filtrado y gestión de tráfico A2P y P2P internacional.

Asimismo, derivaría en una obligatoriedad indirecta de negociar o renegociar contratos comerciales con proveedores internacionales de servicios de mensajería y llamadas, en condiciones impuestas unilateralmente por la regulación, lo cual podría afectar la libertad contractual, alterar el equilibrio económico de los contratos vigentes y generar asimetrías competitivas en el mercado.
(…)
En consecuencia, estas implementaciones requieren de un estudio detallado y sistemático del ordenamiento jurídico, en relación con el mercado costarricense. De igual manera, cualquier ajuste regulatorio debe observar el principio de mínima intervención, evitando imponer cargas adicionales desproporcionadas a los operadores y proveedores.

E. Derechos de los usuarios finales.

Resulta esencial que las medidas que se adopten no se implementen en detrimento de los derechos de los usuarios finales que actúan de buena fe. Cualquier metodología que implique bloqueos preventivos, restricciones al uso de servicios, filtrado de comunicaciones o limitaciones al tráfico legítimo debe diseñarse con extremo cuidado, garantizando el respeto a los principios de debido proceso, presunción de licitud de las comunicaciones, acceso a los servicios, continuidad, no discriminación y protección de datos personales.

F. Sobre el plazo de implementación.
El plazo de 180 días naturales que se propone otorgar a los proveedores y operadores para la implementación de las configuraciones necesarias a nivel de sus sistemas carece de fundamentación y se encuentra alejado de la realidad, ignorando las distintas fases que requiere un proyecto de este nivel de complejidad y tecnicismo.

La fase previa a la implementación del proyecto, que podría iniciar hasta que se haya emitida la resolución, conllevaría que las empresas del sector realicemos un estudio de viabilidad de las medidas impuestas, búsqueda de proveedores que puedan brindar esas soluciones en específico, solicitud y comparación de cotizaciones bajo un marco de obligatoriedad, así como la búsqueda de una partida y/o asignación de recursos- en caso de existir- para así poder iniciar con la fase de contratación del proveedor o de los proveedores y la ejecución del proyecto. Al incluirse tráfico internacional, sería necesario además la renegociación de las condiciones con los carriers internacionales, que, de igual forma, estaríamos los operadores y proveedores locales supeditados al cumplimiento de un mandato regulatorio, que podría derivar en desventajas competitivas para tratar de contratar en igualdad de condiciones.

Posterior a la fase de contratación del proveedor (es), iniciaría la fase de ejecución, que como es de conocimiento de esta Superintendencia, conllevaría al menos diseños, desarrollo, pruebas, revisión e incorporación de procesos, capacitaciones, entre otros.

Adicionalmente, para nosotros es importante que esta Superintendencia tome en cuenta, que tal y como lo realizan esta entidad, mi representada tiene un proceso presupuestario, que incluye la preparación, autorización ejecución, y rendición de cuentas; y la imposición de estas medidas que tienen un impacto económico dentro de un plazo casi que de inmediato, tiene repercusiones e impacta el presupuesto de mi representada.

Por lo que, consideramos que un plazo de al menos 24 meses, a partir de la publicación de la resolución en el Diario Oficial La Gaceta, sería razonable para una planificación y ejecución efectiva. Entendiéndose además que esto no depende exclusivamente de los operadores y proveedores de telecomunicaciones regulados.

Alternativamente, sugerimos establecer fases diferenciadas e hitos.

G. Observaciones a la Propuesta de Metodología.

Sin detrimento de lo indicado anteriormente que representa sustantivamente la posición de mi representada, de seguido encontraran nuestras observaciones puntuales y recomendaciones a las medidas planteadas:

1. 9.1-C, puntos 10-11. Riesgo de falsos positivos sobre tráfico legítimo. Los umbrales de Rate Limiting y los patrones de detección de campañas pueden bloquear mensajes válidos, tales como OTPs bancarios, alertas de salud, y confirmaciones transaccionales, teniendo un impacto en usuarios finales legítimos, así como en los ingresos de los operadores por los volúmenes de este tipo de mensajería. Para esto, se recomienda la aplicación de umbrales contextuales, y no fijos. Por lo que, sugerimos que se incluya que los umbrales de Rate Limiting y detección de campañas sean configurables según el perfil del remitente. Un remitente previamente registrado (banco, institución pública, marca establecida) debe poder operar con umbrales distintos a uno desconocido.

2. 9.1-C Exigencias técnicas elevadas sobre el firewall SMS. La regulación establece 15 capacidades mínimas: DPI con IA, NLP, análisis heurístico, geolocalización, sistemas de reputación de enlaces en tiempo real, detección de AIT y SimBoxes, entre otras; que representan inversión en costo y un tiempo significativo en plataforma especializada. Por lo que, se debería valorar la necesidad solicitar la totalidad de esas 15 capacidades.
3. 9.1-E. Restricciones estrictas sobre uso de datos DPI. La regulación prohíbe utilizar el contenido inspeccionado para fines distintos a seguridad y exige destrucción posterior. Esto requeriría de una arquitectura de datos específica y auditable. Conviene que la regulación final sea explícita en los mecanismos de auditoría y certificación del cumplimiento de esta restricción.

4. Estandarización del registro A2P. Se debería definir el formato único del registro de entidades emisoras A2P (9.3-E) para todos los operadores, evitando fragmentación e inconsistencias entre operadores.

5. 9.5.A — Servicios de Llamadas de Voz. Se debe aclarar el alcance de lo esperado en el punto (d) — Identificación de llamadas automatizadas con grabaciones de voz o voz sintética (robocalls):

- *¿qué tecnología o estándar se contempla para esta detección?*
- *¿Bloqueos? En EEUU hay toda una infraestructura alrededor de los robocalls incluyendo varias bases de datos a nivel país que se actualizan periódicamente, e.g.; DNO, RMD; donde hay que registrarse para transitar tráfico de EEUU.*

6. 9.5.D — Adopción de Out-of-Band SHAKEN (OOBS). La adopción masiva de OOBS fuera de Estados Unidos y Canadá es prácticamente inexistente. Ningún país de Centroamérica o el Caribe ha implementado STIR/SHAKEN ni OOBS a la fecha, y los carriers intermedios en estas regiones no soportan la infraestructura de certificados digitales (STI-CPS) que el protocolo requiere. Esto representa un problema de cadena: si el Carrier internacional recibe tráfico de carriers que no firman con STIR/SHAKEN, no puede autenticarlo con ningún nivel de "attestation" y Liberty podría rechazarlo. Se debería considerar que imponer OOBS como obligatorio inmediato en un entorno donde el ecosistema regional no lo soporta generaría disrupciones operativas significativas sin un beneficio proporcional.

H. Solicitud de Apertura de Comité Técnico Consultivo sobre Medidas de Seguridad.

Por último, respetuosamente quisiéramos sugerir a esta Superintendencia que valore la creación y dirección de un Comité Técnico Consultivo con los operadores interesados, que tenga como mandato y objeto la revisión integral de esta propuesta; y que proponga recomendaciones al Consejo de esta Superintendencia, como se ha realizado en otros temas, tales como el Comité Técnico de Calidad que está revisando y actualizando los indicadores de distintos servicios, el Comité de Registro Prepago en cuanto a la implementación de un nuevo proceso de activación de servicios prepago y los distintos flujos de funcionamiento de un nuevo Registro Prepago, y el Comité de Portabilidad que aprobó en tiempo record un pliego de condiciones y ya ha iniciado el proceso de selección de la Entidad de Referencia para la Portabilidad Móvil.
(…)"

Las observaciones a la propuesta presentadas por Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty) se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty) se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.5.1. Análisis de las observaciones realizadas por Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty):

En cuanto a lo dispuesto por la empresa Liberty en las consideraciones iniciales, esta Superintendencia considera prudente indicar que la propuesta regulatoria sometida a consulta pública no tiene como finalidad sustituir los modelos actuales de seguridad implementados por los operadores y proveedores de servicios de telecomunicaciones, sino fortalecer progresivamente las capacidades de mitigación de afectación a los usuarios finales y minimizar el impacto de los ciberataques derivados de prácticas como el smishing y vishing, los cuales presentan una evolución constante conforme a los cambios y mejoras tecnológicas.

En este sentido con base a la información proporcionada por los operadores y proveedores de servicios de telecomunicaciones, y desarrollado en el oficio número 02238-SUTEL-DGM-2026 del 06 de marzo del 2026, se evidencia un crecimiento sostenido en los mecanismos de ciberataques asociados al uso indebido de numeración nacional e internacional, así como la utilización de rutas grises, spoofing y esquemas automatizados de mensajería fraudulenta, lo cual justifica técnicamente la necesidad de fortalecer el marco regulatorio vigente.

No obstante, debe aclararse que la regulación propuesta establece capacidades mínimas esperadas y no impone tecnologías específicas, de conformidad con el principio de neutralidad tecnológica contenido en el artículo 3 inciso h) de la Ley N° 8642, por lo que, no lleva razón el operador al indicar que la regulación propuesta violenta este principio.

En cuanto a las observaciones relacionadas con privacidad de las comunicaciones y tratamiento de datos personales, debe reiterarse que las medidas regulatorias propuestas no persiguen el monitoreo generalizado de contenido privado de los usuarios y acceso indiscriminado por parte de un humano, sino la identificación de patrones técnicos

asociados a tráfico malicioso, campañas fraudulentas, suplantación de identidad y distribución de enlaces potencialmente peligrosos, mediante sistemas automatizados sin intervención humana, todo ello en observancia de los principios de proporcionalidad y razonabilidad.

De igual forma, resulta importante señalar que el numeral 3 incisos b) y c) y el artículo 42 de la Ley N°8642, impone a los operadores el deber de proteger los derechos de los usuarios de los servicios de telecomunicaciones, garantizar la privacidad y confidencialidad de las comunicaciones y promover el uso de los servicios en apoyo a la seguridad ciudadana, para lo cual deben adoptar medidas técnicas y administrativas idóneas para garantizar la seguridad de sus redes y servicios, siendo precisamente bajo dicho marco jurídico que se desarrolla la presente propuesta regulatoria.

Respecto de la propuesta relacionada con modelos de registro de campañas A2P y validación previa de remitentes, esta Superintendencia reconoce el valor técnico de esquemas comparables implementados en otras jurisdicciones internacionales, tales como "*The Campaign Registry (TCR*)" en los Estados Unidos; sin embargo, la incorporación de un modelo nacional integral de registro de campañas requiere análisis adicionales sobre interoperabilidad, gobernanza, administración de identificadores, trazabilidad y coordinación entre operadores, por lo que, su eventual implementación deberá analizarse en una etapa posterior de madurez regulatoria. Por lo anterior, se recomienda rechazar esta observación.

Respecto a la observación sobre el plazo inicial de implementación, como se indicó anteriormente en este documento, se recomienda acoger la propuesta aportada por otro operador para optar por un calendario gradual de implementación en 3 fases iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas en cuanto a servicios de mensajería SMS y posteriormente 2 fases adicionales para medidas avanzadas con plazos para puesta en operación de 12 meses (360 días) para completar las mediadas aplicables a los servicios de mensajería SMS y 18 meses (540 días) para la implementación de los requerimientos de seguridad para servicios de voz. De modo que, se recomienda acoger esta observación.

Sobre las observaciones relacionadas con el **apartado 9.1.C puntos 10** y **11** sobre el riesgo de falsos positivos sobre tráfico legítimo, derivados de la implementación de mecanismos automatizados de detección y bloqueo de tráfico SMS, particularmente en relación con tráfico A2P legítimo correspondiente a servicios bancarios, autenticación multifactor (2FA), notificaciones transaccionales y comunicaciones automatizadas válidas, esta Superintendencia considera pertinente aclarar que la propuesta regulatoria sometida a consulta pública no establece como criterio único de bloqueo la unidireccionalidad de las comunicaciones ni la existencia aislada de patrones automatizados, más bien corresponde un análisis integral de los distintos comportamientos para determinar si una comunicación es o no bloqueada.

La metodología regulatoria propuesta contempla un análisis basado en trazabilidad, autenticación, coherencia de rutas, validación de origen, verificación de las rutas de

enlaces, comportamiento histórico, correlación de eventos y patrones asociados a campañas maliciosas, de modo que la ausencia de respuestas por parte del usuario final no constituye por sí sola un elemento suficiente para catalogar el tráfico como fraudulento o malicioso.

Asimismo, debe considerarse que la propuesta regulatoria incorpora la obligación de mantener registros de clientes autorizados para el envío de tráfico A2P, lo cual permite a los operadores diferenciar tráfico legítimo previamente validado frente a comportamientos anómalos o campañas de smishing. Además, es importante destacar que los mecanismos de gestión de errores forman parte inherente de cualquier sistema de detección de fraude o ciberataques y no requieren necesariamente una definición exhaustiva a nivel normativo. Corresponde a los operadores, en el marco de su responsabilidad operativa, mantener un equilibrio adecuado entre seguridad y continuidad del servicio, implementando mecanismos como listas blancas de remitentes verificados, canales de gestión de reclamos para desbloqueos ágiles, o ajustes continuos de umbrales y modelos de detección.

Al igual que se indicó anteriormente respecto a la implementación de un registro de servicios autorizados para el envío de mensajes informativos masivos sin recibir respuesta de los remitentes que además debe ser compartido entre operadores y proveedores interconectados, le corresponderá al operador verificar adecuadamente la identidad de sus clientes y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas o entidades legitimas se encuentren en dicho registro de excepciones, y bloquear todo el tráfico que presente un comportamiento similar y no se encuentre en el citado registro.

Bajo el principio de neutralidad tecnológica, la obligación planteada recae en la capacidad de los operadores de implementar controles efectivos contra el smishing, a través de las herramientas disponibles, cuya implementación, ajuste y optimización corresponde a cada operador en función de su red y su tráfico. Por lo que, se recomienda acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Sin embargo, se aclara que este requerimiento solo es aplicable para mensajes A2P.

Respecto a las observaciones relacionadas con el **apartado 9.1.C** sobre la complejidad técnica y económica asociada a la implementación de firewalls SMS con capacidades avanzadas de análisis, inteligencia artificial, procesamiento de lenguaje natural (NLP), análisis heurístico y detección automatizada en tiempo real, esta Superintendencia considera importante señalar que la regulación sometida a consulta pública establece capacidades funcionales mínimas esperadas y no la adopción obligatoria de una tecnología, proveedor o arquitectura específica.

En este sentido, conforme al principio de neutralidad tecnológica dispuesto en el artículo 3 inciso h), Ley N.°8642, corresponde a cada operador o proveedor seleccionar las soluciones tecnológicas que mejor se ajusten a sus condiciones de infraestructura, capacidad operativa y planificación financiera.

No obstante, esta Superintendencia reconoce que determinadas capacidades avanzadas requieren procesos progresivos de adquisición, integración y adaptación tecnológica, razón por la cual resulta razonable adoptar un esquema escalonado de cumplimiento regulatorio según fases de implementación, priorizando inicialmente capacidades esenciales relacionadas con autenticación, trazabilidad, bloqueo de tráfico enmascarado y validación de rutas.

Asimismo, debe considerarse que las amenazas asociadas al smishing presentan una evolución constante y utilizan mecanismos automatizados cada vez más sofisticados, incluyendo evasión de filtros mediante variaciones ortográficas, enlaces dinámicos, técnicas de spoofing y utilización de plataformas automatizadas, por lo que la adopción progresiva de herramientas avanzadas de análisis resulta técnicamente necesaria para garantizar la efectividad de las medidas regulatorias.

En relación con las observaciones sobre el **apartado 9.1.E** respecto al uso de mecanismos de Inspección Profunda de Paquetes (DPI) y su eventual impacto sobre la privacidad de las comunicaciones y protección de datos personales, esta Superintendencia considera necesario aclarar que la finalidad de las medidas regulatorias propuestas no consiste en realizar monitoreo generalizado o indiscriminado del contenido privado de las comunicaciones de los usuarios. La utilización de mecanismos de DPI contemplada en la propuesta regulatoria se limita exclusivamente a la identificación de amenazas asociadas a campañas de smishing, enlaces maliciosos, malware, spoofing y patrones de fraude que comprometan la seguridad de los usuarios y de las redes públicas de telecomunicaciones. Por lo que, se reitera que de conformidad con las mejores prácticas internacionales, sistemas informáticos e Inteligencia Artificial se conjugan para la aplicación en tiempo real de una serie de reglas que permiten determinar si una comunicación es o no maliciosa, por lo que, no se está ante una vulneración de la privacidad, confidencialidad ni mucho menos ante una intervención de comunicaciones.
Asimismo, las medidas regulatorias deben implementarse bajo criterios de proporcionalidad, minimización de datos y finalidad específica, conforme a los principios contenidos tanto en el artículo 42, Ley N.°8642, como en la Ley N.°8968 "*Protección de la Persona frente al Tratamiento de sus Datos Personales*".

En desarrollo de lo anterior, y en atención a los principios establecidos en la Ley N.º 8968 y su Reglamento, así como la Resolución N.º 28348-2021 de la Sala Constitucional, se precisa que el derecho a la autodeterminación informativa no es absoluto. Como ha resuelto la Sala Constitucional, este derecho puede ser limitado de manera justa, razonable y transparente para salvaguardar bienes constitucionales superiores como la seguridad ciudadana, como es el caso de lo establecido en el artículo 2 inciso f) de la Ley N.º 8642, y la adecuada prestación de los servicios públicos de telecomunicaciones, a partir del artículo 8 incisos b) y e) de la Ley N.º 8968.

En este aspecto, la Inspección Profunda de Paquetes (DPI) propuesta no constituye una vulneración al secreto de las comunicaciones, ya que no implica una intromisión humana en el contenido de los mensajes. Este es un proceso automatizado basado en reglas técnicas, inteligencia artificial y análisis heurístico. Este tipo de tratamiento, además, es

congruente con las medidas de seguridad lógica establecidas por el artículo 10 de la Ley N.º 8968 y el Capítulo IV del Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales N.º 37554-JP, los cuales obligan a los responsables del tratamiento de datos a adoptar mecanismos que garanticen la integridad y seguridad de la información.

En igual sentido, al evacuar la consulta facultativa sobre el proyecto de ley que derivó en la Ley N.º 8968, la Sala Constitucional por medio de la Resolución N.º 05268 - 2011 validó la constitucionalidad de su articulado y reconoció que la protección de datos personales responde a una necesidad imperiosa de equilibrar el derecho a la autodeterminación informativa con otros bienes jurídicos constitucionalmente protegidos, como la seguridad ciudadana y el orden público, los cuales pueden justificar limitaciones razonables y proporcionadas al tratamiento de datos.

Adicionalmente, la Sala Constitucional por medio de la Resolución N.º 02222 - 2024 reconoció la legitimidad de imponer requisitos técnicos de ciberseguridad a los operadores de telecomunicaciones, siempre que estos no resulten arbitrarios ni discriminatorios y persigan fines legítimos como la protección de los usuarios y la seguridad de las redes. En dicho pronunciamiento, si bien el Tribunal se abstuvo de analizar el fondo de los estándares técnicos por considerar que ello excede la naturaleza sumaria del amparo, validó la potestad de la Administración para establecerlos, siempre que se fundamenten en criterios objetivos y razonables. Esto debe tomarse en cuenta para la posición de esta Superintendencia al dictar medidas como el DPI, que se sustentan en estándares internacionales y en los principios de seguridad y proporcionalidad.

En este mismo orden de ideas, la Sala Constitucional por medio de la Resolución N.º 29976 - 2025 ha sido enfática al señalar que el derecho a la intimidad, la autodeterminación informativa y la confidencialidad "*no pueden considerarse derechos absolutos, pues evidentemente hay otros intereses superiores que prevalecen a la consideración individual de las personas*". En dicha sentencia, la Sala también reconoció la legitimidad del tratamiento automatizado de datos personales bajo estrictos principios de confidencialidad y seguridad. Por lo tanto, así como el interés público estadístico justifica el acceso y procesamiento de información crediticia individualizada, el interés público en la seguridad ciudadana y la protección de los usuarios frente al *smishing* y *vishing* justifica la implementación del DPI bajo los principios de proporcionalidad, minimización de datos y confidencialidad que esta Superintendencia dispone. Sobre esta resolución, conviene citar que la Sala Constitucional reconoce lo siguiente:

> *No hay duda de que actualmente el cúmulo de los avances tecnológicos y científicos están alcanzando una nueva dimensión que demarca una nueva cúspide tecnológica, la que hunde sus raíces en los derechos humanos y aquellos de las generaciones futuras, de modo que, evidentemente es necesario el establecimiento de salvaguardias y protecciones que deberán estar asentadas sobre bases jurídicas y éticas. Por ejemplo, la inteligencia artificial genera una gran cantidad de alertas y precauciones por el peligro que significa para las sociedades, pero es justo decirlo también, que permitirá grandes conquistas en otras áreas de la ciencia y de la*

> *técnica en menor tiempo para beneficio del ser humano, por señalar una, la medicina. Pero, es cierto también, que los derechos a la autodeterminación informativa (como lo entendió el legislador), y a la intimidad, no pueden interponer una barrera infranqueable frente a un legítimo interés público, toda vez que en la otra cara de la moneda, están las necesidades de una realidad social y económica del país.*

Por lo anterior, la implementación del DPI se debe realizar bajo un estricto y verificable cumplimiento de los siguientes principios, que responden a lo establecido por la normativa citada y por la jurisprudencia constitucional:

1. **Principio de finalidad.** El análisis de los mensajes se limitará exclusivamente a la identificación de patrones objetivos de *smishing* y *vishing*, no siendo utilizado para ningún otro fin.

2. **Principio de proporcionalidad y principio de minimización.** El sistema se configurará para acceder únicamente a la información estrictamente necesaria para la detección de amenazas. No se realizarán copias permanentes del contenido de los mensajes. Una vez analizados y determinados como legítimos, los datos serán descartados, cumpliendo así con el principio de proporcionalidad y minimizando la retención de datos.

3. **Principio de seguridad.** Los operadores deberán implementar las medidas de seguridad administrativas, físicas y lógicas a las que se refiere el Capítulo IV del Reglamento de la Ley N.º 8968, garantizando que el tratamiento automatizado no derive en accesos no autorizados ni fugas de información. El deber de confidencialidad es extensivo a estos sistemas automatizados.

4. **Principio de transparencia.** Esta Superintendencia velará por que los operadores informen a sus usuarios, en los términos de sus contratos y políticas de privacidad, sobre la implementación de estos sistemas de filtrado de seguridad, en cumplimiento del principio de transparencia.

Por lo tanto, la medida propuesta es constitucional y se concibe como una aplicación directa de los deberes de seguridad y la protección al usuario establecidos en los artículos 42 de la Ley General de Telecomunicaciones, N.º 8642 y 10 de la Ley N.º 8968, en armonía con la jurisprudencia sentada por la Sala Constitucional, la cual ha avalado medidas de control de acceso y seguridad.
En otro orden de ideas, sobre la observación relacionada con la necesidad de estandarizar el registro de tráfico A2P, esta Superintendencia considera que dicha propuesta resulta pertinente, en tanto permite fortalecer la trazabilidad, autenticación y control de los remitentes que utilizan el servicio de mensajería SMS para comunicaciones masivas, transaccionales, comerciales, informativas o de autenticación.

En efecto, la existencia de registros A2P administrados de forma aislada por cada operador podría generar diferencias operativas, asimetrías en los requisitos exigidos a los remitentes,

dificultades de interoperabilidad y posibles vacíos de control frente a remitentes que utilicen múltiples rutas o agregadores para cursar tráfico hacia usuarios finales. Por ello, resulta razonable valorar la conveniencia de establecer parámetros mínimos comunes para el registro de clientes, remitentes, campañas, rutas autorizadas y agregadores que participen en la cadena de envío de mensajes A2P.

No obstante, debe aclararse que la propuesta regulatoria sometida a consulta pública no pretende crear, en esta etapa, un registro nacional centralizado ni sustituir la relación contractual y operativa que mantienen los operadores con sus clientes o agregadores. La finalidad inmediata de la medida consiste en que cada operador cuente con información suficiente, verificable y actualizada que permita identificar al remitente, validar la legitimidad del tráfico, diferenciar el tráfico A2P autorizado del tráfico irregular y aplicar medidas de bloqueo cuando se detecten inconsistencias, suplantación, rutas no autorizadas o patrones asociados a smishing.

Respecto a las observaciones relacionadas con el **apartado 9.5.A** sobre la implementación de capacidades técnicas para la prevención del vishing en servicios de voz, incluyendo procesamiento de CDRs, análisis de señalización, detección de patrones sospechosos y robocalls, esta Superintendencia reconoce que determinadas capacidades requieren inversiones importantes en infraestructura tecnológica y sistemas especializados. No obstante, debe señalarse que la experiencia internacional evidencia que los esquemas modernos de fraude telefónico utilizan mecanismos automatizados, spoofing de numeración, rutas grises y técnicas avanzadas de suplantación de identidad, lo cual exige fortalecer las capacidades de supervisión, autenticación y trazabilidad de las comunicaciones de voz.

Asimismo, la información estadística remitida por los operadores en cumplimiento de la resolución RCS-294-2023 demuestra que las medidas regulatorias previamente adoptadas han permitido identificar y bloquear cantidades significativas de tráfico fraudulento asociado a enmascaramiento de llamadas, lo cual evidencia la necesidad de continuar fortaleciendo los mecanismos regulatorios existentes.

En este sentido, esta Superintendencia considera razonable establecer un cronograma progresivo de implementación, diferenciando aquellas capacidades que pueden implementarse mediante ajustes sobre infraestructura existente de aquellas que requieren plataformas especializadas de análisis avanzado o inteligencia artificial, según el cronograma de 3 fases sugerido por Claro CR Telecomunicaciones S.A. (Claro).
Sobre las observaciones relacionadas con el **apartado 9.5.D** y la adopción del estándar OOBS, esta Superintendencia coincide en que la implementación de mecanismos de autenticación avanzada de llamadas requiere coordinación interoperador, análisis de compatibilidad técnica y definición progresiva de esquemas de gobernanza y certificación. No obstante, debe considerarse que estándares de autenticación como STIR/SHAKEN y OOBS constituyen actualmente referencias internacionales ampliamente utilizadas para combatir esquemas de spoofing y suplantación de identidad en redes de voz.

En consecuencia, la propuesta regulatoria pretende establecer una línea base para la evolución futura de mecanismos de autenticación de llamadas en Costa Rica, sin imponer una implementación inmediata o absoluta que desconozca las limitaciones técnicas actuales de los operadores.

Asimismo, esta Superintendencia se encuentra anuente en participar en espacios técnicos de coordinación entre los operadores y proveedores de servicios de telecomunicaciones que hacen uso de numeración asignada, que permitan analizar aspectos relacionados con interoperabilidad, tratamiento de tráfico internacional, modelos de certificación, validación de identidad y cronogramas de implementación.
En cuanto a la solicitud del **punto H** relacionada con la apertura de un Comité Técnico Consultivo para el análisis e implementación de medidas de seguridad asociadas a smishing y vishing, esta Superintendencia considera que la creación de espacios técnicos de coordinación y retroalimentación con operadores, proveedores, agregadores, cámaras empresariales y autoridades competentes puede resultar de gran utilidad para fortalecer la implementación de las medidas regulatorias propuestas.

No obstante, debe aclararse que la eventual conformación de dichos espacios consultivos no suspende ni condiciona las potestades regulatorias y de supervisión atribuidas legalmente a esta Superintendencia conforme a la Ley General de Telecomunicaciones y la Ley N.°7593.

Por lo que, si bien es favorable analizar la creación futura de mesas técnicas o espacios consultivos permanentes orientados al seguimiento e implementación progresiva de las medidas regulatorias relacionadas con seguridad de redes y prevención de fraude en telecomunicaciones, no es justificación para posponer o retrasar la implementación de las medidas propuestas, dado el riesgo latente en que se encuentran los usuarios de servicios de telecomunicaciones ante el aumento de ataques de tipo vishing y smishing, de modo que, se recomienda rechazar esta solicitud.

Con base en el análisis anterior, se recomienda acoger las observaciones respecto a ampliar el plazo de implementación, según se detalla más adelante.

Además, se recomienda acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor, enfatizando que este requerimiento aplica solo para mensajes A2P.
Se recomienda rechazar las observaciones restantes planteadas por este operador.

3.6. Posición del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT):

Mediante el oficio MICITT-DVT-OF-204-2026 del 24 de abril de 2026 (NI-05536-2026), el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) por medio del señor Hubert Vargas Picado, en su condición de Viceministro de Telecomunicaciones,

presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
1. Mecanismos de seguimiento: *Se sugiere valorar la incorporación de un esquema de periodicidad para la remisión de información por parte de los operadores, que permita monitorear la efectividad de las medidas propuestas. Lo anterior, considerando que en la resolución RCS-294-2023 para servicios de voz se contemplaron reportes cuatrimestrales sobre llamadas bloqueadas, lo cual podría servir como referencia para este caso.*

2. Implementación y capacidades técnicas: *(…) tomando en cuenta que dicho criterio se deriva de los insumos recabados en el proceso de consulta a los operadores, y considerando el plazo definido para la implementación de las medidas (180 días naturales), se sugiere valorar la incorporación para estos casos de un esquema de implementación gradual, a fin de facilitar una adopción efectiva y homogénea de las medidas por parte de los distintos operadores.*

3. Responsabilidades en la cadena de tráfico: *(…) podría ser conveniente precisar el alcance de las obligaciones para los distintos operadores, considerando que, si bien las medidas aplican de manera general, el nivel de control y visibilidad sobre el tráfico no es uniforme entre los agentes.*

En particular, aquellos operadores que no cuentan con interconexión internacional directa reciben el tráfico a través de terceros. Lo anterior, tomando en cuenta que en el servicio de mensajería intervienen múltiples actores (operadores de origen, tránsito y destino, así como agregadores), por lo que una delimitación clara de responsabilidades contribuiría a una aplicación más efectiva y proporcional de las medidas, particularmente en escenarios donde el tráfico es gestionado a través de intermediarios o proveedores internacionales.

4. Impacto en la calidad de servicio: *Considerando que algunas de las medidas propuestas implican el análisis de contenido de los mensajes (por ejemplo, mediante mecanismos como DPI), podría valorarse si existe algún análisis previo sobre el impacto de estas soluciones en la calidad del servicio, particularmente en términos de latencia o entrega oportuna de los mensajes. Lo anterior, tomando en cuenta que este tipo de mecanismos requiere un procesamiento adicional sobre el tráfico, lo cual, en escenarios de alto volumen, puede introducir latencia o generar impactos en el desempeño de la red si no es adecuadamente dimensionado. En este sentido, se sugiere considerar este aspecto dentro del diseño de la medida, a fin de evitar afectaciones en la experiencia del usuario final.*

5. Riesgo de falsos positivos: *En el apartado 9.1, inciso c), punto 10, se establece la detección y bloqueo automático de números o entidades que superen umbrales de tasa y volumen de mensajes no correspondientes a un comportamiento humano (Rate Limiting). En este sentido, si bien este tipo de mecanismos resulta adecuado para la detección de tráfico automatizado potencialmente fraudulento, podría valorarse el riesgo de afectación sobre tráfico legítimo, considerando que servicios como la mensajería de autenticación (OTP) o la mensajería transaccional también presentan patrones de envío automatizado y altos volúmenes en cortos periodos de tiempo. Asimismo, se observa que la propuesta se enfoca principalmente en mecanismos de detección y bloqueo, sin que se detallen de forma específica mecanismos orientados a la gestión de posibles errores de clasificación. Por lo anterior, se sugiere considerar mecanismos complementarios que permitan mitigar posibles falsos positivos, a fin de evitar afectaciones en servicios esenciales para las personas usuarias.*

6. Definición de criterios cuantitativos: *En el apartado 9.1, punto 11, inciso b), se hace referencia a "cantidades considerables" de mensajes, lo cual podría dar lugar a interpretaciones distintas entre operadores. En este sentido, se sugiere valorar la incorporación de criterios más concretos o lineamientos de referencia que permitan una aplicación más uniforme de la medida.*
(…)
consideramos que la propuesta regulatoria es jurídicamente viable y acorde con las competencias establecidas en la LGT para para la SUTEL, estando alineada con los postulados de la seguridad y protección del usuario como fines superiores del Estado.
(…)"

Las observaciones a la propuesta presentadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.6.1. Análisis de las observaciones realizadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT):

Las observaciones planteadas por el Viceministerio de Telecomunicaciones del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) se orientan principalmente al fortalecimiento de la ciberseguridad nacional, la protección de los usuarios finales y la necesidad de establecer mecanismos coordinados para la prevención de fraudes mediante comunicaciones electrónicas, así como minimizar el impacto de los ciberataques mediante mensajes de texto SMS (smishing) y llamadas (vishing), destacando que la propuesta regulatoria es jurídicamente viable y acorde con las competencias establecidas en la LGT para para la SUTEL, estando alineada con los postulados de la seguridad y protección del usuario como fines superiores del Estado.

Esta Superintendencia coincide con la posición planteada por el Viceministerio de Telecomunicaciones del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) en cuanto a la importancia de adoptar medidas regulatorias preventivas que permitan fortalecer la trazabilidad de las comunicaciones, minimizar el uso de rutas irregulares y robustecer las capacidades de detección temprana de esquemas de smishing y vishing.

Asimismo, resulta relevante destacar que las observaciones remitidas por el Viceministerio de Telecomunicaciones del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) guardan coherencia con los objetivos y lineamientos contenidos en la Estrategia Nacional de Ciberseguridad 2023-2027, particularmente en lo relacionado con gestión de riesgos, protección de infraestructura crítica y fortalecimiento de capacidades de respuesta frente a amenazas digitales.

Ahora bien, respecto a la observación del **punto 1**, sobre mecanismos de seguimiento, según se indicó anteriormente, de la misma forma que se requirió en la resolución RCS-294-2023, la regulación que se emita incluirá la obligación de los operadores de remitir reportes cuatrimestrales sobre la cantidad de mensajes SMS y llamadas bloqueadas por ser identificadas como tráfico malicioso, con la finalidad de monitorear la efectividad de las medidas propuestas, de modo que, se recomienda acoger esta solicitud.

Sobre la observación del **punto 2**, como se indicó anteriormente, se recomienda acoger la única propuesta de calendario gradual recibida para la implementación de esta propuesta,

la cual se dividide en 3 fases, iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas de filtrado en SMS y posteriormente 2 fases adicionales, 12 meses (360 días) para aplicar medidas avanzadas en el tráfico de SMS y 18 meses (540 días) para medidas de voz.

Respecto a la observación del **punto 3**, sobre las responsabilidades de los operadores ante acciones de terceros internacionales, es fundamental diferenciar entre la responsabilidad sobre el origen del tráfico y la responsabilidad sobre la gestión de este dentro de la red. Efectivamente, los operadores nacionales no son responsables de las acciones de terceros en redes internacionales, sin embargo, sí son responsables del tráfico que cursan sus redes o aceptan que ingrese para ser entregado a los usuarios dentro de su red. Cada operador tiene la capacidad técnica de aplicar controles, análisis y decisiones para bloquear tráfico malicioso.

La imposición de obligaciones sobre el tratamiento del tráfico dentro de la red del operador, no les traslada responsabilidades por actos de terceros en redes internacionales, sino que, la propuesta regulatoria establece un deber de gestión diligente del tráfico que ingresa a sus redes y es entregado a los usuarios, al amparo de lo dispuesto en el artículo 42 de la Ley N°8642 que dispone que los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. De modo que, se recomienda rechazar esta observación.

En cuanto a la observación del **punto 4**, sobre el posible impacto en la calidad del servicio derivado de la implementación de mecanismos de análisis automatizado de tráfico, es importante señalar que los operadores actualmente se encuentran sujetos a reglamentaciones que establecen indicadores y umbrales de calidad de servicio, incluyendo métricas relacionadas con el tiempo de entrega de mensajes de texto, según lo dispone la resolución RCS-152-2017 *Umbrales de Cumplimiento para los Indicadores Establecidos en el Reglamento de Prestación y Calidad de Servicios*. En este contexto, cualquier implementación tecnológica debe diseñarse y dimensionarse tomando en cuenta el cumplimiento de dichos indicadores, como una condición propia de la prestación de servicios de telecomunicaciones, además, conforme las mejores prácticas internacionales, la aplicación de las reglas para el filtrado de mensajes se realizan en tiempo real, por lo que, no se identifica una afectación en la calidad del servicio de las comunicaciones.
Los sistemas modernos de inspección y análisis de tráfico operan mediante arquitecturas distribuidas, procesamiento en tiempo real y técnicas de optimización que permiten analizar grandes volúmenes de tráfico con impactos mínimos en latencia. Además, el procesamiento requerido para analizar contenido e identificar patrones de smishing representa una fracción en comparación con otras funciones de filtrado previo, como enrutamiento, control de trazabilidad y registro de remitentes autorizados, lo que disminuye el tráfico que debe ser analizado con técnicas avanzadas de inspección de contenido.

Adicionalmente, los mecanismos de detección pueden configurarse de forma selectiva y basada en riesgo, lo que permite priorizar el análisis en segmentos de tráfico más susceptibles a ciberataques mediante mensajes de texto SMS (Smishing) y llamadas

(Vishing), como lo es el tráfico internacional, reduciendo aún más cualquier impacto potencial sobre el desempeño global del servicio.

Los escenarios de alto volumen forman parte de la operación normal de cualquier red de telecomunicaciones, por lo que, la gestión de capacidad, dimensionamiento de infraestructura y escalabilidad son responsabilidades fundamentales de los operadores, siendo que, las mejores prácticas internacionales permiten el establecimiento de mecanismos para el filtrado de tráfico sin afectar la calidad de los servicios.

Es importante reiterar que el principio de neutralidad tecnológica se respeta a cabalidad, ya que, las obligaciones planteadas no radican en adoptar una tecnología específica, sino en implementar mecanismos efectivos de detección y mitigación de smishing y vishing, por lo que, le corresponde a cada operador seleccionar, dimensionar y optimizar las soluciones técnicas que le permitan cumplir con los objetivos de seguridad de la propuesta regulatoria y los indicadores de calidad de servicio establecidos dispuestos en la regulación vigente, de modo que, se recomienda rechazar esta observación, ya que no se evidencian afectaciones en la experiencia del usuario final.

Sobre la observación del **punto 5** respecto a la preocupación de un eventual impacto en el tráfico legítimo, como mensajes de autenticación OTP o transaccionales, es importante señalar que los mecanismos de Rate Limiting no operan de forma aislada ni bajo criterios simples de volumen. Estos sistemas forman parte de esquemas de análisis que considera múltiples variables simultáneamente, como reputación del remitente, historial de comportamiento, relación contractual con el operador, patrones de contenido y comportamiento en cuanto a la remisión de tráfico. Esto permite diferenciar de manera efectiva entre tráfico automatizado legítimo como autenticaciones OTP o mensajería transaccional, y patrones asociados a campañas de smishing, reduciendo significativamente el riesgo de falsos positivos. Además, cabe señalar que, el esfuerzo de evitar prácticas de smishing busca que los usuarios puedan estar tranquilos sobre los mensajes de tipo OTP que reciben.

Adicionalmente, como se ha enfatizado a lo largo de este documento, el tráfico legítimo debe ser trazable, por lo que, los servicios como OTP y mensajería empresarial deben operar bajo esquemas registrados, autenticados y gestionados a través de rutas oficiales o agregadores autorizados, lo que permite a los operadores aplicar tratamientos diferenciados de forma que el tráfico legítimo pueda ser identificado, mientras que el tráfico no identificado o anómalo sea sujeto a controles más estrictos. Como se indicó anteriormente, los operadores pueden implementar un registro de servicios autorizados para el envío de mensajes A2P informativos masivos sin recibir respuesta, por lo que, le corresponderá al operador verificar adecuadamente la identidad de sus clientes y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes, garantizando que solo empresas o entidades legitimas se encuentren en dicho registro de excepciones, y bloquear todo el tráfico que presente un comportamiento similar y no se encuentre en el citado registro.

Respecto a la ausencia de mecanismos de gestión de errores de clasificación, es importante destacar que estos forman parte inherente de cualquier sistema de detección de ciberataques y no requieren necesariamente una definición exhaustiva a nivel normativo. Corresponde a los operadores, en el marco de su responsabilidad operativa, mantener un equilibrio adecuado entre seguridad y continuidad del servicio, implementando mecanismos como listas blancas de remitentes verificados, canales de gestión de reclamos para desbloqueos ágiles, o ajustes continuos de umbrales y modelos de detección.

Cabe señalar que, las medidas de Rate Limiting además de permitir identificar comportamientos no compatibles con un uso humano, pueden ser calibrados y ajustados para minimizar impactos sobre tráfico legítimo, por lo que, omitir este tipo de controles por el riesgo de falsos positivos implicaría dejar sin tratamiento el envío masivo automatizado de mensajes, que es uno de los principales mecanismos de smishing.

Bajo el principio de neutralidad tecnológica, la obligación planteada recae en la capacidad de los operadores de implementar controles efectivos contra el smishing. El Rate Limiting constituye una de varias herramientas disponibles, cuya implementación, ajuste y optimización corresponde a cada operador en función de su red y su tráfico. De modo que, se recomienda rechazar esta observación.

Finalmente, sobre la observación del **punto 6**, respecto a la incorporación de criterios concretos y lineamientos que permitan una aplicación uniforme de la medida, es importante destacar que, la detección de campañas de smishing basada en patrones de volumen y frecuencia de envío es uno de los mecanismos más efectivos y ampliamente utilizados a nivel internacional para identificar comportamientos no compatibles con uso humano. La referencia a *“cantidades considerables”* no busca establecer un umbral rígido, sino definir un criterio funcional que permita a los operadores identificar actividad anómala según el contexto de su propia red.

La fijación de umbrales únicos, estáticos y uniformes para todos los operadores resulta técnicamente inadecuado, ya que, las redes de los operadores difieren en escala, arquitectura, volumen de tráfico y tipo de clientes, por lo que, una cantidad especifica de mensajes puede ser irrelevante en un entorno y crítico en otro.

Por lo anterior, la utilización de un concepto abierto como *“cantidades considerables”* responde a la necesidad de habilitar enfoques dinámicos y adaptativos, donde cada operador pueda definir sus propios umbrales y modelos de detección en función de su volumen de tráfico habitual y el comportamiento histórico de sus clientes.

Desde la perspectiva de efectividad, imponer lineamientos excesivamente prescriptivos o umbrales rígidos podría generar el efecto contrario al deseado, facilitando la evasión por parte de actores maliciosos que ajustan sus patrones para mantenerse por debajo de límites conocidos. En cambio, la flexibilidad en la definición de *“cantidades considerables”* permite a los operadores adaptar sus controles de forma continua frente a amenazas dinámicas.

La consistencia entre operadores, no se logra mediante la imposición de valores idénticos, sino a través de la convergencia en objetivos y resultados en cuanto a detectar y mitigar eficazmente campañas de smishing. Bajo el principio de neutralidad tecnológica, cada operador, en ejercicio de su responsabilidad sobre la red, debe implementar mecanismos idóneos que le permitan cumplir con este objetivo, independientemente de los parámetros específicos utilizados, de modo que, la obligación debe definirse en términos de la capacidad para identificar envíos masivos anómalos en cortos periodos de tiempo y no de parámetros específicos, siendo que, le corresponde a cada operador establecer, ajustar y optimizar sus criterios internos, asegurando su efectividad y minimizando impactos sobre tráfico legítimo, por lo que, se recomienda rechazar esta observación.

Con base en el análisis anterior, se recomienda rechazar las observaciones planteadas por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) en los puntos 3, 4, 5 y 6. En cuanto a las observaciones de los puntos 1 y 2 sobre mecanismos de seguimiento y plazo de implementación respectivamente, las mismas fueron atendidas y acogidas con fundamento en estas observaciones y las planteadas por otros interesados que expresaron su posición ante esta consulta pública, según fue anteriormente analizado en este documento.

3.7. Posición de la Cámara de Infocomunicación y Tecnología (INFOCOM):

Mediante el oficio CIT-0010-2026 del 24 de abril de 2026 (NI-05538-2026) la Cámara de Infocomunicación y Tecnología (INFOCOM) por medio de la señora Ana Lucía Ramírez Calderón, en su condición de Directora Ejecutiva, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
***1.** En primer lugar, consideramos oportuno que de previo a que se emita el informe técnico al Consejo Directivo de la SUTEL, sobre los resultados de la presente consulta, o de previo a que dicho Órgano tome su decisión, se pueda realizar una reunión o espacio a modo de taller, para que los operadores interesados puedan ampliar, técnicamente, aspectos relevantes en cuanto a la idoneidad, o no, de las medidas y su alcance; así como en cuanto a los términos y condiciones de su implementación.*

***2.** Hemos revisado con atención, el Apartado 9 del Oficio N°02238-SUTEL-DGM-2026 (…) Consideramos que la propuesta regulatoria del apartado referido debe de tratarse con especial cautela, considerando que ciertas medidas podrían eventualmente **violentar la privacidad de las comunicaciones de los usuarios** de los operadores de y proveedores de servicios de telecomunicaciones. El derecho fundamental a la privacidad de las comunicaciones se encuentra dispuesto en el Art. 24 de la Constitución Política. Asimismo, se encuentra regulado en el Art. 42 de la Ley General de Telecomunicaciones, y en el Art. 6 del Reglamento sobre Medidas de Protección de la Privacidad de las Comunicaciones. Por lo tanto, se sugiere que se revise la propuesta a la luz de estos principios y derechos constitucionales.*

***3.** Se reconoce la relevancia de atender fenómenos como el smishing y vishing, sin embargo, se considera que la propuesta trasciende el alcance original de la RCS-294-2023, la cual fue concebida específicamente para abordar el **enmascaramiento de llamadas en servicios de voz**. En ese sentido, **la extensión hacia SMS no constituye una simple actualización, sino un cambio sustancial del régimen regulatorio** que debería tratarse como una nueva regulación, con su respectivo análisis de impacto integral.*

***4.** La propuesta introduce **obligaciones de carácter amplio** y en algunos casos absolutas, como el bloqueo de la totalidad del tráfico A2P no trazable, o la validación integral del origen de los mensajes: Este enfoque resulta*

***desproporcionado**, en tanto no distingue adecuadamente entre tráfico legítimo e ilegítimo, pudiendo generar afectaciones a servicios esenciales como autenticaciones, notificaciones bancarias y comunicaciones empresariales.*

*En ese sentido, se considera que la propuesta conlleva una **violación al principio de proporcionalidad y razonabilidad**. No se justifica la proporcionalidad y razonabilidad exigida para el planteamiento de la ejecución de las medidas descritas. No se tiene claridad en la motivación ni el análisis de los medios requeridos para alcanzar los fines propuestos. Aunque la industria comparte el objetivo o fin que buscan estas medidas, se tiene inquietud sobre su viabilidad, costos y eficacia de lo propuesto, siendo que los medios para alcanzar este fin podrían ser desproporcionados; considerando la carga exigida a los operadores y proveedores de servicios de telecomunicaciones. De igual manera, cualquier ajuste regulatorio debe observar el **principio de mínima intervención**, evitando imponer cargas adicionales desproporcionadas a los operadores y proveedores.*

***5.** Debe de analizarse con especial cautela la responsabilidad que se pretende delegar a los operadores y proveedores de servicios de telecomunicaciones, sobre el **tráfico internacional del servicio de mensajería de texto y sus diferentes modalidades:** Por ejemplo, en el punto 9, se dispone que los sistemas de firewall a ser implementados, deben de tener la capacidad de: identificar tráfico de tipo P2P o A2P que ingresa a la red del operador por rutas de interconexión internacional, detectar y bloquear la totalidad del tráfico de tipo A2P o P2P con origen internacional, bloquear la totalidad del tráfico A2P que ingrese a sus redes por rutas de interconexión internacional o local, simulando de cualquier manera ser de tipo P2P o aquel en el que se enmascare el número de origen, etc. La responsabilidad de los operadores y proveedores debe de tener un límite en el territorio nacional, siendo contrario a la seguridad jurídica, poderse achacársele a estos, toda responsabilidad por las obligaciones de terceros en el tráfico internacional. Consideramos que estas implementaciones requieren de un estudio detallado y sistemático del ordenamiento jurídico, en relación con el **mercado costarricense**.*

***6.** La **imposición implícita de soluciones tecnológicas** específicas, tales como firewalls con inteligencia artificial, inspección profunda de paquetes y sistemas avanzados de detección automatizada, pareciera extralimitar las potestades la SUTEL. La **regulación debe ser tecnológicamente neutral**, estableciendo objetivos de cumplimiento, pero permitiendo a los operadores adoptar las soluciones más adecuadas según su arquitectura y condiciones operativas.*

*El **principio de neutralidad tecnológica** se encuentra en el artículo 3, inciso h) de la Ley General de Telecomunicacione nueva regulación s, el cual establece los principios rectores en los cuales se sustenta dicha ley. Consideramos que la regulación propuesta estaría en conflicto con este principio, al disponer la obligatoriedad de mecanismos específicos de prevención, violentado así la discrecionalidad de los operadores y con ello su libertad de comercio. Asimismo, mediante la implementación obligatoria de estas medidas, con especificaciones concretas, a través de una resolución administrativa, y no mediante la promulgación de una ley, se estaría transgrediendo el **principio de reserva de ley,** lo cual hace necesario reconsiderar la propuesta.*

***7.** Otro aspecto relevante es la **asignación de responsabilidades al operador más allá de su ámbito de control efectivo:** En el caso del tráfico A2P internacional, intervienen múltiples actores (agregadores, carriers, plataformas externas), por lo que no resulta razonable exigir al operador local garantizar trazabilidad extremo a extremo en toda la cadena global. De igual forma, la habilitación para inspeccionar el contenido de los mensajes SMS plantea implicaciones importantes en materia de privacidad, confidencialidad y secreto de las comunicaciones. En este punto, es necesario establecer límites claros, salvaguardas específicas y criterios de proporcionalidad que eviten tratamientos indiscriminados de la información de los usuarios.*

***8. Es necesario diferenciar claramente entre SMS P2P y A2P:** El problema descrito por la propuesta se concentra principalmente en el tráfico A2P y en el uso de rutas grises, por lo que extender controles intensivos al SMS P2P podría resultar innecesario y desproporcionado.*

***9.** La **definición de "atributos mínimos de identificación" resulta ambigua** en su redacción actual, lo que podría generar interpretaciones divergentes entre operadores. En este sentido, sería recomendable contar con estándares técnicos uniformes y claramente definidos por la autoridad reguladora.*

10. *En términos operativos, las* ***medidas propuestas implican cargas significativas*** *en inversión, operación y adaptación tecnológica, lo cual debería ser evaluado mediante un* ***análisis de costo-beneficio*** *y considerando mecanismos de implementación gradual.*

11. *Adicionalmente, se considera que la regulación debería contemplar un* ***enfoque progresivo, incluyendo fases piloto y evaluación de resultados antes de su adopción*** *generalizada, especialmente tomando en cuenta la heterogeneidad de capacidades técnicas entre operadores.*

12. *En relación con los* ***servicios de voz****, se considera que* ***no se justifica, en esta etapa, la imposición de nuevas obligaciones adicionales,*** *considerando que la RCS-294-2023 ya ha mostrado resultados relevantes en el bloqueo de llamadas fraudulentas.*

13. Sobre el plazo de implementación de las configuraciones necesarias a nivel de los sistemas: *En nuestro criterio, el plazo de 180 días naturales que se pretende otorgar a los proveedores y operadores para esta implementación, y para proceder con los ajustes técnicos de las medidas regulatorias dispuestas, resulta imposible de cumplir y no es congruente con la realidad práctica, tomando en cuenta la complejidad y el tecnicismo requerido para estas acciones. Por lo tanto, en caso de adoptar la propuesta regulatoria dispuesta en el apartado 9 del oficio número 02238-SUTEL-DGM-2026, se debe de proporcionar un plazo razonable, de por lo menos 24 meses a partir de la publicación, o una ejecución por etapas, que considere el grado de complejidad de cada una de las medidas.*
(…)"

Las observaciones a la propuesta presentadas por la Cámara de Infocomunicación y Tecnología (INFOCOM) se interpusieron dentro del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. Además, las observaciones se realizaron según los solicitado en la convocatoria de consulta pública ya que la misma se presentó de manera electrónica al medio indicado por la Superintendencia. Así las cosas, las observaciones interpuestas por la Cámara de Infocomunicación y Tecnología (INFOCOM) se ajustan en tiempo y forma a lo solicitado por la Sutel, por lo cual, se procederá con el siguiente análisis.

3.7.1. Análisis de las observaciones realizadas por la Cámara de Infocomunicación y Tecnología (INFOCOM):

Respecto a la observación del **punto 1**, como se indicó anteriormente, esta Superintendencia considera que la creación de espacios técnicos de coordinación y retroalimentación con operadores y proveedores puede resultar de gran utilidad para fortalecer la implementación de las medidas regulatorias propuestas, sin embargo, estos espacios no suspenden ni condicionan las potestades regulatorias de supervisión atribuidas legalmente a esta Superintendencia conforme a la Ley General de Telecomunicaciones y la Ley N.°7593, además, ante las tendencias detectadas por esta Superintendencia respecto al crecimiento del tráfico malicioso e intentos de smishing y vishing a los usuarios, se considera urgente aplicar la normativa vigente para proteger a los usuarios y evitar que el mercado de mensajería SMS pierda credibilidad y caiga en desuso como ha pasado en otras latitudes, por lo que, si bien se resalta la importancia de estos espacios, esto no es una condición para postergar la implementación de medidas regulatorias con el fin de minimizar el impacto de ciberataques mediante mensajes de textos SMS y llamadas telefónicas, en pro de la seguridad de los usuarios.

Asimismo, respecto a que en este taller los operadores puedan ampliar, técnicamente, aspectos sobre la idoneidad de las medidas y su alcance; así como los términos y condiciones de su implementación, cabe señalar que, este espacio fue otorgado mediante la presente consulta pública, donde se les brindó a todos los operadores y proveedores involucrados un espacio para que aportaran sus observaciones ante la implementación de las medidas propuestas, y fue atendido por los operadores con mayor mercado de mensajes SMS y llamadas. Inclusive la Dirección General de Mercados mediante oficio número 03422-SUTEL-DGM-2025 del 24 de abril de 2025 realizó una consulta previa a los operadores y proveedores con numeración asignada, con el fin de recabar criterios técnicos sobre acciones adicionales que permitan ampliar el alcance de las medidas de bloqueo y mitigación del fraude en redes públicas de telecomunicaciones, razón por la cual esta Superintendencia ha brindado el espacio suficiente para realizar observaciones y aportes, por lo que, se recomienda rechazar esta observación.

No obstante, esta Superintendencia considera que la creación de espacios técnicos futuros de coordinación y retroalimentación con operadores, proveedores, agregadores, cámaras empresariales y autoridades competentes puede resultar de gran utilidad para fortalecer la implementación de las medidas regulatorias propuestas. En consecuencia, se valora favorablemente analizar la creación futura de mesas técnicas o espacios consultivos permanentes orientados al seguimiento e implementación progresiva de las medidas regulatorias relacionadas con seguridad de redes y prevención de fraude en telecomunicaciones, no obstante debe reconocerse la urgencia de la adopción de regulaciones que mitiguen el riesgo en que se encuentran los usuarios de los servicios de telecomunicaciones ante el crecimiento de ataques de vishing y smishing que se ha documentado en el sector.

Por otra parte, sobre la observación del **punto 2** respecto a la supuesta violación de la privacidad de las comunicaciones de los usuarios, de la misma manera que se ha explicado ampliamente en este informe, esta Superintendencia es responsable respecto al cumplimiento del principio rector sobre privacidad de la información de los usuarios dispuesto en el artículo 3, inciso j) de la Ley N°8642 Ley General de Telecomunicaciones, que obliga a los operadores y proveedores a garantizar la intimidad y confidencialidad de la información de los usuarios de telecomunicaciones, por ello, la propuesta regulatoria no implica la intervención o acceso indiscriminado a las comunicaciones por parte de un humano, sino que, corresponde a procesos automatizados, ejecutados por sistemas informáticos diseñados específicamente para identificar patrones previamente definidos asociados a fraudes, tanto de smishing como de vishing. Lo cual a su vez resulta conforme con la obligación de los operadores y proveedores de adoptar medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios, según lo dispuesto en el artículo 42 de la citada Ley.

Este análisis se limita a elementos estrictamente necesarios para detectar amenazas y los datos no se almacenan de forma permanente, ya que, el análisis se realiza en tiempo real y con fines exclusivos de ciberseguridad, garantizando la destrucción de los datos una vez cumplan su cometido con el sistema de firewall. Además, la propuesta claramente dispone que los datos obtenidos por estos sistemas automatizados solo pueden ser utilizados para

fines relacionados con el fin de minimizar el impacto de ciberataques mediante el smishing y el vishing, protegiendo la privacidad de las comunicaciones.

Asimismo, la recomendación de la Unión Internacional de Telecomunicaciones UIT-T X.1244 define el phishing como *"3.2.10 phishing (usurpación de identidad): Intento de adquirir de manera fraudulenta y delictiva información sensible, como nombres de usuario, contraseñas y datos bancarios, mediante la suplantación de una entidad fiable en las comunicaciones electrónicas."* y permite que estos paquetes sean rechazados según el punto *"10.6.1 Rechazo de paquetes en la entidad de red Es posible imponer alguna política, como ACL (lista de control de acceso) en un encaminador o cualquier entidad de red para descartar paquetes sospechosos de ser spam procedente de una dirección o prefijo IP concretos. El spammer puede enviar sus mensajes desde dentro o desde fuera de la red del ISP. Los ISP que quieren proteger sus redes contra el spam habrán de solucionar ambos problemas con distintos enfoques."*. Por lo que, se recomienda rechazar esta observación.

En cuanto a la observación del **punto 3**, sobre que la presente propuesta regulatoria sea tratada como una nueva regulación, debe señalarse que, si bien es cierto, la metodología regulatoria contenida en la resolución RCS-294-2023 fue concebida y aprobada con un alcance delimitado a los servicios de voz y al enmascaramiento de llamadas, no obstante, su fundamento al igual que la presente propuesta regulatoria, radica en la necesidad de una cooperación de los operadores y proveedores de servicios de telecomunicaciones en contra de la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en el desarrollo de tecnologías de la información y prevenir los actos dirigidos contra la confidencialidad, integridad, disponibilidad de sistemas informáticos, redes, datos, así como el abuso de tales sistemas, lo cual se deriva de las iniciativas de ajuste a la Ley N° 9048 y la Ley N° 9135 que reformaron al Código Penal, para la incorporación de los delitos informáticos y conexos.

Por otra parte, tal y como se señaló anteriormente, el fundamento jurídico de la presente propuesta regulatoria se basa en la Ley N°8642 que es conteste con lo desarrollado en la Ley N°7593, siendo que resulta de vital importancia la protección de los derechos de los usuarios finales de los servicios de telecomunicaciones, y aboga por que exista un desarrollo de las telecomunicaciones que contribuya con la seguridad ciudadana, para lo cual los operadores deben adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios, conforme al artículo 42 de la Ley 8642.

Debe destacarse que, después de la emisión de la resolución RCS-294-2023, y ante la evidencia de que las modalidades de fraude han migrado hacia otros medios tecnológicos (particularmente la mensajería de texto SMS en sus modalidades P2P y A2P), la Dirección General de Mercados mediante oficio número 03422-SUTEL-DGM-2025 del 24 de abril de 2025 realizó una consulta a los operadores y proveedores con numeración asignada, con el fin de recabar criterios técnicos sobre acciones adicionales que permitan ampliar el alcance de las medidas de bloqueo y mitigación del fraude en redes públicas de telecomunicaciones.

De las respuestas recibidas, se desprenden elementos comunes relevantes: **i)** la factibilidad de reforzar la autenticación del identificador de origen en troncales SIP mediante mecanismos como P-Asserted-Identity y controles de ANI por troncal, con el objetivo de

impedir la suplantación de numeración asignada; **ii)** la necesidad de incorporar controles específicos sobre tráfico de mensajería A2P, dada su naturaleza automatizada y su potencial para facilitar campañas masivas de smishing; **iii)** la conveniencia de adoptar medidas basadas en estándares internacionales de autenticación y verificación del origen como OOBS.

Es por ello, que en el oficio número 02238-SUTEL-DGM-2026 del 06 de marzo de 2026 sometido a consulta pública, se realiza un amplio análisis técnico sobre el smishing y vishing, los SMS A2P y P2P, así como los mecanismos de bloqueo y filtrado específicos para SMS sin desnaturalizar el servicio ni vulnerar el marco de privacidad, y que delimitan finalidades, controles y salvaguardas de tratamiento de datos, con el objetivo de garantizar la seguridad de los usuarios finales y las redes de los operadores.

De manera que la regulación propuesta es complementaria a la previamente emitida por esta Superintendencia con la finalidad de establecer las disposiciones para la gestión del tráfico SMS y garantizar la seguridad de los usuarios, evitando prácticas como el “smishing” entre otras, ya que, tal y como el operador lo reconoce, actualmente se implementan acciones idénticas a las propuestas para los servicios de voz, por lo tanto, no se está ante una regulación novedosa o sorpresiva para los operadores, en el tanto la propuesta sometida a consulta resulta necesaria para la protección de los usuarios, para la seguridad de las redes y los servicios, acorde con las disposiciones normativas vigentes, y además que, los operadores tienen experiencia en la implementación de las medidas planteadas, como es el caso de la resolución RCS-294-2023. Por tanto, se recomienda acoger los argumentos de la Cámara de Infocomunicación y Tecnología (INFOCOM) y emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

Respecto a la observación del **punto 4**, sobre que las medidas propuestas resultan desproporcionadas o contrarias al principio de mínima intervención, no se sostiene a la luz de la naturaleza, magnitud y evolución de los casos de smishing, ni del rol que desempeñan los operadores en el ecosistema de mensajería SMS.

Cabe señalar que, un análisis de proporcionalidad debe considerar no solo la carga operativa para los operadores, sino también el riesgo que enfrentan los usuarios y el sistema en su conjunto. Se reitera que, esta Superintendencia ha registrado un incremento marcado en el tráfico malicioso y ha solicitado múltiples acciones a los operadores que resultan consistentes con la regulación propuesta. El smishing se ha consolidado como una de las principales causas de ciberataque, caracterizado por su alta escalabilidad, bajo costo de ejecución y dificultad de trazabilidad. En este contexto, la ausencia de medidas estructurales eficaces genera una afectación directa y masiva sobre los usuarios, lo que justifica la adopción de mecanismos más robustos.

La medida de bloquear la totalidad del tráfico A2P no trazable responde precisamente a este principio de proporcionalidad. No se trata de una restricción arbitraria, sino de garantizar que solo el tráfico que puede ser identificado, validado y auditado debe ser permitido en las redes de los operadores.

El tráfico A2P no trazable constituye el principal canal de explotación para campañas de smishing, debido a la facilidad con la que permite ocultar la identidad del originador. Por lo que permitir su tránsito bajo el argumento de evitar cargas operativas equivale a mantener abierta la principal vía de fraude.

En cuanto a la razonabilidad y proporcionalidad de las medidas, es importante destacar que no se prohíbe el tráfico A2P en su totalidad, sino únicamente aquel que no cumple condiciones mínimas de trazabilidad, además, existen alternativas viables y ampliamente mencionadas en este documento para permitir el tráfico legítimo, como registros de remitentes, validación de identidad de clientes, uso de agregadores autorizados, mecanismos de autenticación y registros de excepción.

Respecto a la preocupación sobre costos y viabilidad, como se indicó anteriormente, estos deben analizarse en el contexto de las responsabilidades inherentes a la obligación de los operadores de adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. La implementación de mecanismos de trazabilidad, control y filtrado forma parte de las capacidades técnicas esperadas en operadores modernos, especialmente ante amenazas que afectan directamente la confianza en los servicios de telecomunicaciones.

El principio de mínima intervención no implica ausencia de regulación, sino la adopción de medidas necesarias y adecuadas para alcanzar un fin legítimo. En este caso, la medida propuesta es idónea y no impone cargas adicionales desproporcionadas a los operadores y proveedores, dado que ataca directamente la principal característica del smishing que corresponde al tráfico no trazable, además, otras medidas menos restrictivas han demostrado ser insuficientes frente a la evolución del smishing, por lo que, la regulación propuesta es necesaria y proporcional al permitir la continuidad del tráfico legítimo bajo condiciones claras y alcanzables.

Adicionalmente, cabe señalar que, la falta de intervención o la adopción de medidas parciales o inadecuadas genera un efecto adverso al trasladar el costo del fraude a los usuarios, mientras se mantienen inalteradas las condiciones que permiten la proliferación del smishing.

Finalmente, es importante destacar que, el principio de neutralidad tecnológica dispuesto en la regulación vigente se respeta a cabalidad, ya que, las obligaciones propuestas se definen en términos de resultados, al garantizar la trazabilidad del tráfico A2P, dejando a los operadores la libertad de implementar las soluciones técnicas que consideren más adecuadas para cumplir con este requisito.

Por lo anterior, se recomienda rechazar lo señalado por la Cámara de Infocomunicación y Tecnología (INFOCOM), ya que, las medidas propuestas no solo cumplen con los principios de proporcionalidad y razonabilidad, sino que, representan una respuesta necesaria y técnicamente justificada frente a una amenaza latente en perjuicio de los derechos de los usuarios. El bloqueo del tráfico A2P no trazable no constituye una carga desproporcionada,

sino un esquema mínimo de seguridad que permite proteger eficazmente a los usuarios y fortalecer la integridad de los servicios de mensajería SMS.

Sobre la observación del **punto 5**, respecto a que la responsabilidad de los operadores debe limitarse estrictamente al territorio nacional, excluyendo el tratamiento del tráfico internacional entrante, cabe señalar que, no resulta consistente con la realidad técnica de las redes de telecomunicaciones ni con los principios básicos de gestión de riesgos en infraestructuras críticas.

Se reitera que no es lo mismo la responsabilidad sobre el origen del tráfico, que la responsabilidad sobre la gestión de este dentro de la red. Los operadores nacionales no son responsables de las acciones de terceros en redes internacionales, sin embargo, sí son responsables del tráfico que cursa sus redes o aceptan que ingrese para ser entregado a los usuarios dentro de su red.

Cabe aclarar que el punto de control y responsabilidad para un operador no es el origen geográfico del mensaje, sino el punto de ingreso a la red nacional. En ese punto, el operador tiene la capacidad técnica de aplicar controles, análisis y decisiones para bloquear tráfico malicioso. Permitir el tránsito de tráfico malicioso bajo el argumento de que su origen es internacional, implica renunciar a ese control por parte del operador y trasladar el riesgo directamente a los usuarios, además, el tráfico internacional es precisamente una de las principales vías de smishing, debido a la facilidad de ocultar o falsear el origen, uso de rutas grises y la ausencia de mecanismos de autenticación y trazabilidad. Por lo tanto, excluir este tráfico de medidas de control es inconsistente con el objetivo de la regulación propuesta y debilita estructuralmente cualquier estrategia para minimizar el impacto de ciberataques.

En cuanto al argumento de seguridad jurídica, este no se ve afectado por la imposición de obligaciones sobre el tratamiento del tráfico dentro de la red del operador, ya que, no se está trasladando la responsabilidad a los operadores por actos de terceros, sino que, se establece un deber de gestión diligente del tráfico que ingresa a sus redes y es entregado a los usuarios.

Sobre el requerimiento de estudios adicionales del ordenamiento jurídico, es importante mencionar que, la regulación propuesta tiene asidero en la normativa vigente sobre protección de los derechos de los usuarios y seguridad de la red de telecomunicaciones y se respalda en las mejores prácticas internacionales, y a lo largo de este documento se ha complementado el fundamento de las medidas propuestas, de modo que, un análisis normativo no puede utilizarse como condición para postergar la adopción de medidas frente a un problema cuya materialidad y urgencia son evidentes. La evolución de los ciberataques ha superado ampliamente los esquemas tradicionales de control territorial, requiriendo enfoques basados en gestión de riesgo y control en puntos de interconexión internacional.

Por lo anterior, se recomienda rechazar los alegatos en cuestión, dado que la responsabilidad de los operadores no se extiende al comportamiento de terceros en redes internacionales, sino que, abarca de manera clara la gestión del tráfico que ingresa a sus

redes. La implementación de medidas para identificar y bloquear mensajes SMS maliciosos en puntos de interconexión internacional no solo es jurídicamente viable, sino técnicamente necesaria para garantizar la protección efectiva de los usuarios y la integridad del servicio.

Respecto a la observación del **punto 6** sobre que las medidas impuestas atentan contra el principio de neutralidad tecnológica, de la misma forma que se ha indicado a lo largo de este documento, las medidas requeridas en la propuesta regulatoria no atentan contra dicho principio, ya que, no se promueve la adopción de una tecnología específica, sino que, se establecen capacidades mínimas de seguridad que deben cumplir las redes de los operadores para garantizar la seguridad de los usuarios, las cuales, pueden implementarse de diversas formas según la arquitectura de cada operador.

En todo momento se ha hecho énfasis en que Sutel no tiene la potestad para imponer un modelo especifico de Inteligencia Artificial para el cumplimiento de la propuesta regulatoria, sino que, los operadores cuentan con la discreción de escoger las tecnologías que mejor se ajusten a su infraestructura y presupuesto, con base en los requerimientos de seguridad mínimos planteados. Por lo anterior, se recomienda rechazar esta observación.

En cuanto a la observación del **punto 7** sobre la responsabilidad de los operadores para garantizar la trazabilidad de extremo a extremo en toda la cadena global, de la misma forma que se atendió en el punto 5 anterior, se reitera que, los operadores nacionales no son responsables de las acciones de terceros en redes internacionales, sin embargo, sí son completamente responsables del tráfico que cursa sus redes o aceptan que ingrese para ser entregado a los usuarios dentro de su red, ya que, en el punto de interconexión el operador tiene la capacidad técnica de aplicar controles, análisis y decisiones para bloquear tráfico no trazable y garantizar el ingreso de únicamente el tráfico trazable de extremo a extremo.

Asimismo, sobre la preocupación planteada en este mismo punto respecto a la privacidad, confidencialidad y secreto de las comunicaciones de los usuarios por mecanismos de inspección de contenido, tal y como se ha explicado a lo largo de este documento, la regulación propuesta es responsable en cuanto a preservar el principio rector sobre privacidad de la información de los usuarios dispuesto en el artículo 3, inciso j) y numeral 42 de la Ley N°8642 Ley General de Telecomunicaciones, por lo que, debe reiterarse que, la propuesta de realizar análisis como Inspección Profunda de Paquetes (DPI) en los mensajes SMS, no atenta contra dicho principio, ya que, las medidas propuestas no implican la intervención de un humano para el acceso indiscriminado o la lectura del contenido de los mensajes, sino que corresponde a un proceso automatizado, ejecutado por sistemas informáticos diseñados específicamente para identificar patrones definidos asociados a fraudes, como enlaces maliciosos, estructuras y firmas digitales conocidas típicas de smishing, cuyo análisis se limita a elementos estrictamente necesarios para detectar amenazas en enlaces maliciosos o patrones sintácticos, además, la regulación contempla el no almacenamiento permanente de los datos, realizando un análisis en tiempo real con fines exclusivos de ciberseguridad, y garantizando la destrucción de los datos una vez cumplan su cometido con el sistema de firewall. Asimismo, los operadores tienen

prohibido acceder a estos datos para fines distintos al objetivo de esta regulación. Por lo anterior, se recomienda rechazar esta observación.

Respecto a la observación del **punto 8**, sobre que extender los controles de tráfico a la mensajería SMS P2P podría resultar innecesario y desproporcionado, afirmando que el problema del smishing se concentra exclusivamente en el tráfico A2P y en el uso de rutas grises, debe resaltarse que, si bien históricamente una parte relevante del smishing se ha originado en canales A2P, no significa que el tráfico P2P no sea usado como mecanismo de evasión de sistemas antifraude, más bien se ha documentado a nivel nacional una gran incidencia de tráfico de smishing a través de servicios de tipo P2P, de modo que, por medio de tráfico P2P también se pueden generar ciberataques. Los atacantes han adaptado sus estrategias para aprovechar precisamente aquellos segmentos de la red donde los controles son más débiles, como el uso de SimBoxes para envío de mensajes desde líneas móviles aparentemente legítimas o distribución por segmentos de campañas de mensajes para evitar umbrales de detección tradicionales. Tal y como se ha desarrollado a lo largo del documento, los defraudadores demuestran una gran capacidad de adaptabilidad y la búsqueda constante de alternativas para lograr su cometido, por lo que, las acciones deben ser integrales y no puntuales.

Por lo que, limitar las medidas de control únicamente al tráfico A2P genera un efecto de desplazamiento del fraude hacia el canal P2P, debilitando significativamente la efectividad de cualquier estrategia de mitigación contra el impacto de los ciberataques, como la que propone esta propuesta regulatoria.

Es importante mencionar que, la implementación de medidas sobre tráfico P2P no implica necesariamente la aplicación de controles indiscriminados, sino la incorporación de capacidades proporcionales y basadas en el riesgo que enfrentan, como detección de patrones anómalos de envío, identificación de comportamientos no compatibles con uso humano asociados a la automatización, análisis de contenido en busca de indicadores de fraude como enlaces maliciosos y su correlación con listas de reputación.

Desde la perspectiva de proporcionalidad, excluir el tráfico P2P de cualquier tipo de control deja por fuera del análisis un canal que está siendo activamente explotado, de modo que, el beneficio para un operador en cuanto a evitar controles en el tráfico P2P es inferior al riesgo de permitir la expansión del fraude por esa vía.

Es importante destacar que, la implementación de estas medidas regulatorias contra el smishing debe concebirse como un sistema integral de seguridad, donde todos los elementos relevantes son considerados para la toma de decisiones y no limitar el alcance de las medidas a un solo tipo de tráfico como lo es A2P, ya que, esto reduce su efectividad y además, introduce incentivos para la evasión y migración hacia P2P.

Por lo anterior, se recomienda rechazar esta observación, ya que, si bien el tráfico A2P es relevante para los casos de smishing, no es el único elemento ni necesariamente el predominante en todos los escenarios relacionados a este tipo de ciberataques. La inclusión de controles proporcionales sobre tráfico P2P es necesaria para garantizar la efectividad

de las medidas que minimicen el impacto de este tipo de prácticas irregulares, evitando la migración del problema hacia canales menos controlados y asegurando una protección integral de los usuarios.

En cuanto a la observación del **punto 9** respecto a que la definición de "atributos mínimos de identificación" resulta ambigua, cabe señalar que, la regulación propuesta establece como una obligación de los operadores *"(…) bloquear todo mensaje A2P que no cumpla con los atributos mínimos de identificación que permitan identificar su origen o presenten sospechas de modificaciones que afecten la integridad del mensaje(…)"*, es decir, que los mensajes muestren por la menos la información mínima que permita al operador identificar inequívocamente el origen del mensaje y la integridad del contenido. Con base en el principio de neutralidad tecnológica, y considerando los múltiples escenarios en cuanto a la infraestructura técnica de cada operador, no es correcto establecer estándares uniformes por las diferentes tecnologías que los operadores tienen disposición de implementar, por lo que, se recomienda rechazar la observación.

Sobre la observación del **punto 10**, como se ha indicado anteriormente, los costos asociados a la implementación de mecanismos de seguridad deben considerarse parte integral de la operación de servicios de telecomunicaciones. La protección contra ciberataques como el smishing y el vishing es un componente esencial de la calidad y confiabilidad del servicio y seguridad de la red de telecomunicaciones. En consecuencia, corresponde a los operadores asumir estos costos como parte de sus obligaciones inherentes.

Por lo anterior, no resulta procedente someter la implementación de medidas antifraude a un análisis de costo-beneficio. Bajo el principio de neutralidad tecnológica, corresponde a cada operador definir e implementar las soluciones que le permitan cumplir con la obligación de mitigar el fraude, asumiendo los costos asociados como parte de su responsabilidad operativa y de su compromiso con la protección de los usuarios. Por lo anterior, se recomienda rechazar esta observación.

Por lo anterior, no se considera de recibo la observación planteada en cuanto a supeditar la implementación de las medidas propuestas a la realización de un análisis específico de costo-beneficio. La presente iniciativa regulatoria responde a un enfoque de regulación basada en evidencia, sustentado en hechos objetivos y verificables que demuestran la existencia de una problemática actual y creciente asociada a los ataques de smishing y vishing. La propuesta surge de una necesidad debidamente documentada y de un riesgo cierto e identificado que actualmente enfrentan los usuarios de las redes de telecomunicaciones.

Bajo un juicio de razonabilidad y proporcionalidad, esta Superintendencia considera que los beneficios derivados de la adopción de medidas preventivas contra el fraude, en términos de protección de los usuarios, seguridad de las redes y apoyo a la seguridad ciudadana, superan los costos asociados a su implementación. En consecuencia, retrasar o condicionar la adopción de estas medidas implicaría mantener expuestos a los usuarios

frente a una amenaza actual y acreditada, por lo que no resulta procedente acoger la observación formulada y se recomienda su rechazo.

Sobre las observaciones de los **puntos 11** y **13**, sobre el plazo de implementación, en línea con las observaciones anteriores, se recomienda acoger la única propuesta de calendario gradual recibida para la implementación de esta propuesta regulatoria, la cual se dividide en 3 fases, iniciando con una primera fase de 6 meses (180 días) para implementar medidas básicas de filtrado en SMS y posteriormente 2 fases adicionales, 12 meses (360 días) para aplicar medidas avanzadas en el tráfico de SMS y 18 meses (540 días) para medidas de voz.

Respecto a la observación del **punto 12**, como se indicó anteriormente, el hecho de que una disposición regulatoria haya dado resultados positivos en un área específica no significa que no pueda mejorarse para complementar su alcance o incorporar otras áreas que igualmente requieren intervención. La regulación propuesta busca complementar y robustecer la resolución RCS-294-2023 para cerrar brechas de ciberataques que se realizan fuera del enmascaramiento de llamadas, por lo que, se recomienda rechazar la observación.

Por lo anterior, se recomienda acoger la observación respecto a ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por otro operador.

Además, se recomienda acoger la propuesta de emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

Se recomienda rechazar las observaciones restantes realizadas la Cámara de Infocomunicación y Tecnología (INFOCOM).

3.8. Posición de Millicom Cable Costa Rica, S.A. (Tigo):

Mediante el oficio CAFF-54-2026 del 28 de abril de 2026 (NI-05678-2026) Millicom Cable Costa Rica, S.A. (Tigo) por medio de la señora Roxana María Sánchez Eguizabal, en su condición de apoderada generalísima, presentó su posición con respecto a la consulta pública en cuestión, en los siguientes términos:

"(…)
***PRIMERO:** Del análisis del documento sometido a consulta se identifica una ambigüedad en la delimitación del sujeto obligado, al utilizarse indistintamente expresiones como "todos los operadores" y "los proveedores del servicio de Mensajería SMS".*

Al respecto, consideramos fundamental que la regulación circunscriba expresamente las obligaciones propuestas a aquellos operadores que efectivamente prestan el servicio de SMS y que cuentan con trazabilidad end-to-end sobre dicho servicio, particularmente los operadores móviles.

En determinados escenarios tecnológicos, como SMS sobre IMS, SMSoIP o VoWiFi, el tráfico de mensajes puede ser transportado sobre redes IP fijas cifradas, en las cuales el operador de acceso no presta servicios ni

mensajería SMS, no tiene control sobre la capa de aplicación ni dispone de visibilidad o trazabilidad integral del servicio.

En estos casos, imponer obligaciones de identificación, inspección o bloqueo de tráfico SMS a operadores que únicamente proveen conectividad IP podría resultar técnicamente inviable y ajeno a su rol funcional dentro de la cadena de prestación del servicio. Solicitamos respetuosamente que la versión final de la propuesta: 1) precise de forma expresa el alcance subjetivo de las obligaciones en materia de SMS, y; 2) excluya aquellos supuestos en los que el operador no presta el servicio ni cuenta con trazabilidad técnica sobre el mismo.

***SEGUNDO:** La propuesta contempla mecanismos de inspección y análisis del tráfico SMS con fines de detección de fraude. Al respecto, estimamos necesario advertir que, en entornos IP modernos el tráfico suele encontrarse cifrado de extremo a extremo, además, la implementación de DPI profundo podría requerir capacidades técnicas desproporcionadas y podría generar **riesgos asociados a la privacidad y confidencialidad de las comunicaciones**, que deben evaluarse cuidadosamente bajo criterios de necesidad y proporcionalidad.*

Consideramos pertinente que la regulación reconozca explícitamente estas limitaciones técnicas y evite interpretaciones que conduzcan a la imposición automática de DPI en redes donde ello no resulte técnica ni jurídicamente razonable.

***TERCERO:** En relación con las obligaciones propuestas para la mitigación de fraude en servicios de voz (incluyendo firewalls avanzados y mecanismos como OOB SHAKEN), observamos que el documento aplica obligaciones homogéneas a operadores con modelos de red profundamente distintos y presupone niveles de control sobre señalización, interconexión internacional y arquitectura de red que no todos los operadores poseen.*

*Existen operadores que no gestionan directamente interconexiones internacionales, dependen de terceros para tránsito de tráfico, o utilizan arquitecturas heredadas que no permiten la implementación inmediata de ciertos mecanismos avanzados. Asimismo, la implementación de estas soluciones conlleva **inversiones significativas**, que difícilmente se justifican desde un caso de negocio, al tratarse de medidas orientadas exclusivamente a obligaciones regulatorias.*

*Por lo anterior, consideramos necesario que la regulación diferencie obligaciones según el **tipo de operador y su rol en la cadena de valor** y adopte un enfoque **proporcional y basado en capacidades técnicas reales**.*

***CUARTO:** Finalmente, manifestamos nuestra preocupación respecto al plazo de 180 días naturales propuesto para la implementación integral de las medidas. Dicho plazo debe contemplar un análisis técnico detallado, el procesos de adquisición, la integración con redes existentes, pruebas, ajustes y puesta en producción.*

Para soluciones complejas de seguridad de red y señalización, este plazo resulta altamente exigente, especialmente para operadores que requieren adecuaciones estructurales relevantes.

Solicitamos respetuosamente considerar los esquemas de implementación por etapas, plazos diferenciados según complejidad técnica, o mecanismos transitorios que permitan una adopción ordenada y efectiva.
(…)"

Las observaciones a la propuesta presentadas por Millicom Cable Costa Rica, S.A. (Tigo) se interpusieron fuera del plazo brindado por Sutel el cual era de 10 días hábiles después de publicada dicha convocatoria en el diario oficial La Gaceta. De modo que, las observaciones se presentaron de forma extemporánea y varias de las mismas ya fueron analizadas anteriormente en este documento

3.8.1. Análisis de las observaciones realizadas por Millicom Cable Costa Rica, S.A. (Tigo):

Tal y como consta en el Diario Oficial La Gaceta N° 65 del 10 de abril del año 2026, se sometió a consulta pública a todos los interesados, la propuesta regulatoria desarrollada en el oficio número 02238-SUTEL-DGM-2026 del 6 de marzo del 2026 según lo dispuesto en el Acuerdo 029-014-2026 adoptado por el Consejo de la Sutel en la sesión ordinaria N°014-2026 celebrada el 12 de marzo del 2026, en acatamiento de lo establecido en el numeral 361 de la Ley General de la Administración Pública. Siendo que las observaciones sobre dicha propuesta de regulación se debían interponer dentro de los **diez (10) días hábiles siguientes** a la publicación en La Gaceta, en las instalaciones de la Superintendencia de Telecomunicaciones en Guachipelín Escazú, Oficentro Multipark, edificio Tapantí, 4to piso, en horario de 8:00 am a 4:00 pm, vía fax 2215-68821 o al correo electrónico gestiondocumental@sutel.go.cr.

Ahora bien la publicación de la propuesta se realizó el 10 de abril de 2026 y el plazo para presentar oposiciones se contabiliza a partir del día hábil siguiente, es decir, 13 de abril de 2026, lo anterior conforme expresamente lo indicó la publicación y en aplicación del artículo 38 de la Ley de notificaciones judiciales[16], el cual dispone que todo plazo empieza a correr a partir del día siguiente hábil de la notificación a todas las partes, por lo tanto, el plazo para presentar las oposiciones **vencía el 24 de abril de 2026**, fecha en que terminaba la contabilización de los 10 días hábiles plazo de ley para presentar las posiciones u oposiciones correspondientes.

No obstante, para el caso que nos ocupa, se tiene que **Millicom Cable Costa Rica, S.A. (Tigo)** presentó sus oposiciones a la propuesta regulatoria de referencia el 28 de abril de 2026 según se logra apreciar en el NI-05678-2026, ergo, se recomienda su rechazo y no proceder con su análisis de fondo, por haber sido presentadas de manera extemporánea. No obstante, dicho operador se puede referenciar a las respuestas brindadas en el presente documento sobre los mismos argumentos expuestos.

Por las consideraciones expuestas, se recomienda rechazar la totalidad de las oposiciones de **Millicom Cable Costa Rica, S.A. (Tigo)** y no conocer el fondo de estas, por haberse presentado de manera extemporánea.

4. CONCLUSIONES DEL ANÁLISIS DE LAS POSICIONES RECIBIDAS ANTE LA CONSULTA PÚBLICA REALIZADA POR ESTE ENTE REGULADOR.

De la revisión y análisis de las posiciones presentadas ante esta consulta pública, y habiendo evacuado las observaciones planteadas, se determina lo siguiente:

4.1. Respecto a las observaciones planteadas por **CallMyWay NY S.A. (Call My Way)** se recomienda:

[16] El cual resulta de aplicación supletoria de conformidad con el artículo 9 inciso 1) de la Ley General de Administración Pública.

4.1.1. Acoger la observación sobre incluir y reforzar el fundamento jurídico que motiva la aplicación de las medidas dispuestas en la regulación sometida a consulta pública y habilita a los operadores a tomar acciones al respecto.

4.1.2. Acoger parcialmente las consultas sobre la validación del Título Global y la verificación en tiempo real del origen del mensaje, con el fin de homologar y brindar mayor claridad sobre la definición de trazabilidad.

4.1.3. Acoger la observación de requerir a todos los operadores y proveedores de mensajería SMS la inclusión del comprobante de entrega y recepción de mensaje SMS, así como cualquier configuración necesaria para el éxito de la presente propuesta regulatoria y su coordinación entre operadores.

4.1.4. Acoger parcialmente la observación sobre indicar la frecuencia de remisión de reportes, por lo que, en congruencia con la resolución RCS-294-2023, se solicitará a los operadores y proveedores de telefonía aportar un informe de forma cuatrimestral, con la cantidad de llamadas identificadas como vishing y sus respectivos bloqueos, y de igual manera, los operadores y proveedores de mensajería SMS deben presentar un informe de forma cuatrimestral sobre la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus respectivos bloqueos.

4.1.5. Ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por **Claro CR Telecomunicaciones S.A. (Claro).**

4.2. Se recomienda rechazar las observaciones restantes presentadas por **CallMyWay NY S.A. (Call My Way)**

4.3. Respecto a las observaciones planteadas por **Mitto AG** se recomienda rechazar en su totalidad al exceder el alcance de los análisis y requerimientos dispuestos en la propuesta de regulación sometida a consulta pública.

4.4. Sobre las observaciones presentadas por **Claro CR Telecomunicaciones S.A. (Claro)** se recomienda:

4.4.1. Acoger parcialmente la propuesta sobre robustecer lo requerido en la sección 9.3 inciso E. de la regulación sometida a consulta pública, respecto a la obligación de que los operadores y proveedores implementen registros de las entidades desde las cuales se envía tráfico de SMS A2P, adicionando que, los operadores y proveedores de mensajería SMS A2P deben verificar adecuadamente la identidad de sus clientes de mensajería A2P y la finalidad en cuanto al uso que pretende hacer el cliente con el envío masivo de mensajes, garantizando que solo empresas legitimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no incluidos en este registro. Esto aplica de igual forma para las rutas de

interconexión, de modo que, solo se enviará a otros operadores el tráfico A2P de remitentes autorizados y previamente verificados. Los operadores y proveedores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios. Estos registros se deben compartir entre operadores y proveedores interconectados.

4.4.2. Acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Este requerimiento aplica solo para mensajes A2P.

4.4.3. Acoger de forma complementaria la propuesta del operador sobre permitir a los operadores el registro y validación de plantillas para mensajes A2P.

4.4.4. Acoger el excluir el tráfico multimedia IP de las obligaciones contenidas en esta propuesta regulatoria.

4.4.5. Acoger la solicitud sobre indicar el límite de tiempo para el resguardo de los registros de llamadas (CDR), para lo cual aplica lo dispuesto en el artículo 52 del RPUF, el cual establece un plazo mínimo de cuatro (4) años para conservar los registros detallados de las comunicaciones (llamadas y SMS) que cursen los usuarios finales dentro o fuera de sus redes.

4.4.6. Acoger la propuesta de dividir la implementación de la presente propuesta regulatoria en 3 fases de la siguiente manera, cuyos plazos corren a partir la puesta en vigor:

- **Fase 1 de 180 días (6 meses):** priorizar la implementación de medidas básicas de bloqueo en cuanto a servicios de mensajería SMS, como restricciones por enmascaramiento, reglas para tráfico no trazable, registro de entidades autorizadas para envío de mensajes A2P, validación de rutas e identificación de remitentes y centros de atención al usuario final para reporte de SPAM.

- **Fase 2 de 360 días (12 meses):** implementación de medidas avanzadas con capacidades de Inteligencia Artificial para detección y bloqueo en tiempo real de mensajes SMS maliciosos, con Inspección Profunda de Paquetes (DPI), Procesamiento de Lenguaje Natural (NLP), Análisis Heurístico, sistemas de reputación de enlaces, e intercambio de información entre operadores. Esta fase incluye la implementación de la totalidad de requerimientos establecidos en la normativa para mensajes SMS tanto A2P como P2P.

- **Fase 3 de 540 días (18 meses):** implementación de la totalidad de los requerimientos de seguridad dispuestos en el apartado 9.5 de la

propuesta regulatoria para incorporar sistemas de firewall antispam en los servicios de voz, implementación de señuelos y adopción del estándar Out-of- Band SHAKEN (OOBS).

El detalle completo respecto a este calendario de implantación se muestra en una sección posterior de este informe.

4.4.7. Incorporar en la fase 2 del cronograma el intercambio de información entre operadores y proveedores.

4.5. Se recomienda rechazar las observaciones restantes presentadas por **Claro CR Telecomunicaciones S.A. (Claro).**

4.6. Respecto a las observaciones planteadas por el **Instituto Costarricense de Electricidad (ICE)** se recomienda:

4.6.1. Acoger la solicitud de ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por **Claro CR Telecomunicaciones S.A. (Claro).**

4.6.2. Acoger parcialmente la solicitud de emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

4.7. Se recomienda rechazar las observaciones restantes presentadas por el **Instituto Costarricense de Electricidad (ICE).**

4.8. Sobre las observaciones presentadas por **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty)** se recomienda:

4.8.1. Acoger la solicitud de ampliación del plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por **Claro CR Telecomunicaciones S.A. (Claro).**

4.8.2. Acoger la propuesta del operador sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor, enfatizando que este requerimiento aplica tanto para mensajes A2P como P2P.

4.9. Se recomienda rechazar las observaciones restantes presentadas por **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty).**

4.10. En cuanto a las observaciones presentadas por el **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)** se recomienda acoger:

4.10.1. Incorporar mecanismos de seguimiento, de modo que, de la misma forma que se requirió en la resolución RCS-294-2023, se solicitará a los operadores y proveedores reportes cuatrimestrales relacionados a la cantidad de mensajes SMS y llamadas bloqueadas por ser identificadas como tráfico malicioso.

4.10.2. Ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por **Claro CR Telecomunicaciones S.A. (Claro).**

4.11. Se recomienda rechazar las observaciones restantes presentadas por **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)**.

4.12. Respecto a las observaciones planteadas por la **Cámara de Infocomunicación y Tecnología (INFOCOM)** se recomienda acoger:

4.12.1. Ampliar el plazo de implementación, conforme la propuesta gradual de 3 fases analizada anteriormente y presentada por **Claro CR Telecomunicaciones S.A. (Claro).**

4.12.2. Emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

4.13. Se recomienda rechazar las observaciones restantes presentadas por la **Cámara de Infocomunicación y Tecnología (INFOCOM)**.

4.14. Sobre las observaciones presentadas por **Millicom Cable Costa Rica, S.A. (Tigo)** se recomienda rechazar en su totalidad por haber sido presentadas de forma extemporánea.

4.15. Con base en lo anterior, implica modificar parcialmente la propuesta regulatoria sometida a consulta pública denominada "*ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)*" bajo los siguientes términos:

a) Cambiar la anterior denominación y definir la resolución que se emita como ***"MEDIDAS REGULATORIAS PARA MINIMIZAR EL IMPACTO DE CIBERATAQUES POR SMISHING (SMS) Y VISHING (VOZ) EN LAS REDES DE TELECOMUNICACIONES".***

b) Agregar un nuevo inciso en la **sección 9.1** que se lea: *"**F.** Los operadores y proveedores de mensajería SMS deben brindar comprobante de entrega y recepción de mensaje SMS para la evaluación de tasas de éxito de entrega de mensajes, además de, cualquier configuración necesaria entre operadores y*

proveedores para garantizar el cumplimiento de las obligaciones dispuestas en la presente normativa.".

c) Agregar un nuevo inciso en la **sección 9.1** que se lea: *"**G.** Los operadores y proveedores de mensajería SMS deben presentar un informe de forma cuatrimestral con la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus respectivos bloqueos, diferenciando entre mensajes P2P y A2P"*.

d) Agregar un nuevo inciso en la **sección 9.1** que se lea: *"**H.** Los operadores y proveedores de mensajería SMS deben conservar los registros detallados de las comunicaciones que cursen los usuarios finales dentro o fuera de sus redes durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del Reglamento sobre el Régimen de Protección al Usuario Final (RPUF)"*.

e) Agregar un nuevo inciso en la **sección 9.1** que se lea: *"**I.** Los operadores y proveedores deben disponer de Centros de Atención al Usuario Final para que sus clientes puedan reportar al operador que les brinda el servicio de mensajería SMS y con el cual mantienen una relación comercial, los casos donde exista sospecha de smishing"*.

f) Modificar parcialmente el **inciso C** de la **sección 9.5** para que se lea: *"**C.** Los operadores y proveedores deben disponer Centros de Atención al Usuario Final para que sus clientes puedan reportar al operador que les brinda el servicio de telefonía y con el cual mantienen una relación comercial, los casos donde exista sospecha de vishing."*.

g) Agregar un nuevo inciso en la **sección 9.5** que se lea: *"**F.** Los operadores y proveedores de telefonía deben presentar un informe de forma cuatrimestral, con la cantidad de llamadas identificadas como maliciosas (vishing) y sus respectivos bloqueos"*.

h) Agregar un nuevo inciso en la **sección 9.5** que se lea: *"**G.** Los operadores y proveedores de telefonía deben conservar los registros detallados de las comunicaciones que cursen los usuarios finales dentro o fuera de sus redes durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF)"*.

i) Modificar parcialmente el **inciso E** de la **sección 9.3** para que se lea: *"**E.** Los operadores y proveedores deben establecer registros de los clientes autorizados a enviar tráfico de SMS A2P y/o clientes autorizados a enviar grandes cantidades de mensajes informativos A2P, sin recibir respuesta del usuario receptor. Estos registros serán actualizados con el ingreso o retiro de un nuevo cliente emisor de mensajes SMS A2P o de campañas de envío masivo de mensajes A2P, donde se indique el nombre del cliente y el segmento de numeración que hace uso. Además, esta Superintendencia podrá consultar a los operadores y proveedores dichos registros. Los operadores y proveedores de mensajería SMS A2P deben verificar*

adecuadamente la identidad de sus clientes y la finalidad en cuanto al uso que pretende hacer el cliente con el envío masivo de mensajes A2P, garantizando que solo usuarios legítimos se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no incluidos en este registro, así mismo para generadores de campañas de envío masivo de mensajes no autorizados. Esto aplica de igual forma para las rutas de interconexión, de modo que, solo se enviará a otros operadores el tráfico A2P de remitentes autorizados y previamente verificados. Los operadores y proveedores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios. Estos registros se deben compartir entre operadores y proveedores interconectados.".

j) Modificar en su totalidad el **inciso A** de la **sección 9.6** para que se lea: *"**A.** Los proveedores y operadores con numeración asignada por esta Superintendencia, deben proceder con la implementación de las medidas dispuestas en esta normativa, de forma gradual y progresiva dividida en 3 fases, cuyo plazo corre a partir de la publicación de la presente metodología regulatoria en el diario Oficial La Gaceta. Cada una de estas 3 fases se detalla a continuación:*

1) Fase 1. Plazo de 180 días (6 meses): implementación de medidas de seguridad básicas en servicios de mensajería SMS.

*Del apartado **9.1 SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P**, las siguientes medidas deben ser implementadas dentro del plazo de 180 días:*

a) *Inciso A sobre asegurar la trazabilidad del tráfico de mensajes SMS desde el origen y hasta el destino, bloqueando todo tráfico no trazable o que intente evadir filtros de seguridad.*

b) *Inciso B sobre bloquear el tráfico de mensajes SMS que no especifique atributos de identificación que permitan conocer el origen de la comunicación.*

c) *Inciso C subinciso 1, sobre diferenciar el tráfico de tipo P2P del A2P.*

d) *Inciso C subinciso 2, sobre bloquear tráfico A2P o P2P con origen internacional, cuyo número de origen haya sido enmascarado con un número local.*

e) *Inciso C subinciso 4, sobre verificación en tiempo real del origen del mensaje.*

f) *Inciso C subinciso 10, sobre detección y bloqueo automático de servicios que superen umbrales de tasa y volumen de mensajes no correspondientes a un comportamiento humano.*

g) *Inciso C subinciso 13, sobre análisis de simetría en las comunicaciones para identificar el tráfico que nunca recibe respuesta.*

h) *Inciso C subinciso 14, sobre el bloqueo del tráfico de mensajes SMS internacional que de cualquier manera simule ser de tipo local.*

i) *Inciso D sobre el bloqueo del tráfico de mensajes SMS internacional que de cualquier manera simule ser de tipo local.*

j) *Inciso F propuesto anteriormente, sobre que los operadores faciliten cualquier configuración necesaria entre operadores y proveedores para garantizar el cumplimiento de las obligaciones dispuestas en la presente regulación.*

k) *Inciso G propuesto anteriormente, sobre presentar un informe de forma cuatrimestral con la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus respectivos bloqueos, diferenciando entre mensajes P2P y A2P.*

l) *Inciso H propuesto anteriormente, sobre conservar los registros detallados de las comunicaciones durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del RPUF.*

m) *Inciso I propuesto anteriormente, sobre disponer de centros de atención al usuario final para el reporte de casos de smishing.*

*Con respecto al apartado **9.3 SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P**, la totalidad de las medidas dispuestas en este apartado deben ser implementadas dentro del plazo de 180 días, las cuales corresponde a los incisos A, B, C, D y E de esta sección.*

*Del apartado **9.5. SERVICIOS DE LLAMADAS DE VOZ**, las siguientes medidas deben ser implementadas dentro del plazo de 180 días:*

a) *Inciso C sobre disponer de centros de atención al usuario final para el reporte de casos de vishing.*

2) *Fase 2. Plazo de 360 días (12 meses): implementación de medidas de seguridad avanzadas en servicios de mensajería SMS.*

*Del apartado **9.1 SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P**, las siguientes medidas deben ser implementadas dentro del plazo de 360 días:*

a) *Inciso C subinciso 3 sobre incorporar capacidades con Inteligencia Artificial para analizar el contenido completo de los mensajes SMS mediante Inspección Profunda de Paquetes (DPI).*

b) *Inciso C subinciso 5 sobre incorporar mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados en la red que envían tráfico masivo.*

c) *Inciso C subinciso 6 sobre incorporar Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP) y Análisis Heurístico.*

d) *Inciso C subinciso 7 sobre contar con capacidad de identificar enlaces maliciosos en el contenido de los mensajes SMS P2P y A2P.*

e) *Inciso C subinciso 8 sobre contar uso de sistemas de reputación de enlaces.*

f) *Inciso C subinciso 9 sobre contar con capacidad de analizar mensajes en formato binario y cualquier otro formato técnico de codificación aplicable a los servicios de mensajería móvil.*

g) *Inciso C subinciso 11 (incluido los apartados a, b, c y d de este subinciso) sobre contar con capacidad de identificar campañas de smishing.*

h) *Inciso C subinciso 12 sobre contar con capacidad de detectar ráfagas de spam (Spam Burst) y campañas de smishing rápidas.*

i) *Inciso C subinciso 15 sobre contar con capacidad de detectar Tráfico Inflado Artificialmente (AIT).*

j) *Inciso D sobre uso de sistemas de reputación de enlaces.*

k) *Inciso E sobre las condiciones para analizar el contenido de los mensajes mediante Inspección Profunda de Paquetes (DPI).*

3) ***Fase 3. Plazo de 540 días (18 meses): implementación de medidas de seguridad avanzadas en servicios de voz.***
Esta fase comprende la implementación de las medidas dispuestas en el apartado 9.5. SERVICIOS DE LLAMADAS DE VOZ, las cuales deben estar en funcionamiento dentro del plazo de 540 días:

a) *Inciso A y sus subincisos a), b), c), d) y e) sobre incorporar sistemas de firewall antispam en los servicios de voz con capacidades de procesamiento masivo de registros de llamadas, procesamiento de información de señalización, detección de patrones de comportamiento sospechoso, identificación de llamadas automatizadas con grabaciones o voz sintética*

b) *Inciso B sobre destinar un rango de números telefónicos para la implementación de señuelos.*

c) *Inciso D sobre adoptar e implementar el estándar Out-of- Band SHAKEN (OOBS).*

d) *Inciso E sobre mantener el cumplimiento de los lineamientos establecidos en la resolución RCS-294-2023.*

e) *Inciso F propuesto anteriormente, sobre presentar un informe de forma cuatrimestral con la cantidad de llamadas de voz identificadas como maliciosas (vishing) y sus respectivos bloqueos.*

f) *Inciso G propuesto anteriormente, sobre conservar los registros detallados de llamadas por un plazo mínimo de 4 años, conforme el artículo 52 del RPUF.".*

k) Agregar un nuevo apartado con la definición de trazabilidad que se lea:

*"**SOBRE LA TRAZABILIDAD DE LAS COMUNICACIONES.***

La trazabilidad de las comunicaciones debe entenderse como la capacidad del operador de identificar, autenticar, correlacionar y registrar de forma confiable el origen, la ruta de transmisión y el destino de cada comunicación, en cumplimiento con el Plan Nacional de Numeración y los esquemas autorizados de interconexión.

En mensajería SMS, un mensaje se considerará trazable cuando su origen pueda ser inequívocamente determinado y validado, ya sea como tráfico P2P asociado a un usuario final legítimo, correctamente autenticado en la red, o como tráfico A2P proveniente de un agregador, proveedor o entidad previamente registrado, validado y autorizado por el operador.

La trazabilidad implica, como mínimo, la verificación de la consistencia de la numeración de origen, la integridad de los parámetros de señalización, la validación de la ruta de entrada como puntos de interconexión, agregadores o proveedores internacionales, así como la correlación con registros de comunicaciones y perfiles de tráfico conocidos. Asimismo, el destino de la comunicación deberá corresponder a una numeración válida y coherente con el plan de numeración vigente.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o filtrar aquellos mensajes SMS cuya trazabilidad no pueda ser garantizada, incluyendo, entre otros, casos de manipulación o suplantación de identidad, incongruencias en la señalización, rutas de origen no autorizadas, ausencia de registro o validación del emisor A2P, o imposibilidad de asociar el tráfico a un usuario o entidad legítima. Estas medidas podrán implementarse mediante mecanismos técnicos tales como

firewalls SMS, sistemas de reputación, análisis de patrones de tráfico y validaciones en tiempo real de señalización y numeración.

En el caso de los servicios de llamadas, se entenderá por trazabilidad la capacidad del operador de identificar y validar de forma confiable el origen, la ruta de señalización y el destino de cada comunicación, en concordancia con el Plan Nacional de Numeración y los acuerdos de interconexión vigentes. Una llamada se considerará trazable cuando el identificador de origen pueda ser verificado como perteneciente a un usuario legítimo o a una entidad autorizada, y cuando la ruta de entrada y los parámetros de señalización sean consistentes y no presenten indicios de manipulación o suplantación.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o etiquetar aquellas llamadas cuya trazabilidad no pueda ser garantizada, incluyendo casos de vishing, rutas internacionales no autorizadas o inconsistencias en la señalización, mediante el uso de mecanismos técnicos como validación de identidad de origen, análisis de patrones de tráfico y controles en puntos de interconexión.”.

5. RECOMENDACIONES

5.1. Dar por recibido y acoger el presente informe que analiza las recomendaciones y posiciones recibidas en la consulta pública, rendido por la Dirección General de Calidad y la Dirección General de Mercados mediante el oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 referente al “*INFORME DE ATENCIÓN DE LAS POSICIONES DE LA CONSULTA PÚBLICA SOBRE LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS MEDIANTE MENSAJES DE TEXTO SMS (SMISHING) Y LLAMADAS (VISHING)*”.

5.1.1. Acoger la observación planteada por **CallMyWay NY S.A. (Call My Way)** respecto a incluir y reforzar el fundamento jurídico que motiva la aplicación de las medidas dispuestas en la regulación sometida a consulta pública y habilita a los operadores a tomar acciones al respecto.

5.1.2. Acoger parcialmente las consultas sobre la validación del Título Global y la verificación en tiempo real del origen del mensaje, con el fin de homologar y brindar mayor claridad sobre la definición de trazabilidad.

5.1.3. Acoger la observación planteada por **CallMyWay NY S.A. (Call My Way)** respecto a requerir a todos los operadores y proveedores de mensajería SMS la inclusión del comprobante de entrega y recepción de mensaje SMS, así como cualquier configuración necesaria para el éxito de la presente propuesta regulatoria y su coordinación entre operadores.

5.1.4. Acoger parcialmente la observación planteada por **CallMyWay NY S.A. (Call My Way)** respecto a solicitar a los operadores y proveedores que cuenten con

numeración asignada aportar un informe de forma cuatrimestral, con la cantidad de llamadas identificadas como vishing y sus respectivos bloqueos, y sobre la cantidad de mensajes SMS identificados como maliciosos y sus respectivos bloqueos (smishing).

5.1.5. Acoger la observación planteada por **CallMyWay NY S.A. (Call My Way)** respecto a ampliar el plazo según las fases de implementación gradual.

5.1.6. Rechazar las observaciones restantes presentadas por **CallMyWay NY S.A.**

5.1.7. Rechazar en su totalidad las observaciones presentadas por **Mitto AG** al exceder el alcance de los análisis y requerimientos dispuestos en la regulación sometida a consulta pública.

5.1.8. Acoger parcialmente la observación planteada por **Claro CR Telecomunicaciones S.A. (Claro)** respecto a robustecer lo requerido en la sección 9.3 inciso E. de la regulación sometida a consulta pública, respecto a la obligación de que los operadores y proveedores implementen registros de las entidades desde las cuales se envía tráfico de SMS A2P, adicionando que, los operadores y proveedores de mensajería SMS A2P deben verificar adecuadamente la identidad de sus clientes de mensajería A2P y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes A2P, garantizando que solo empresas legitimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no incluidos en este registro. Esto aplica de igual forma para las rutas de interconexión, de modo que, solo se enviará a otros operadores el tráfico A2P de remitentes autorizados y previamente verificados. Los operadores y proveedores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios. Estos registros se deben compartir entre operadores y proveedores interconectados.

5.1.9. Acoger la propuesta de **Claro CR Telecomunicaciones S.A. (Claro)** sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Este requerimiento aplica para mensajes A2P.

5.1.10. Acoger la observación planteada por **Claro CR Telecomunicaciones S.A. (Claro)** respecto a excluir el tráfico multimedia IP de las obligaciones contenidas en esta propuesta regulatoria.

5.1.11. Acoger de forma complementaria la propuesta de **Claro CR Telecomunicaciones S.A. (Claro)** sobre permitir a los operadores el registro y validación de plantillas para mensajes A2P.

5.1.12. Acoger la solicitud de **Claro CR Telecomunicaciones S.A. (Claro)** sobre indicar el límite de tiempo para el resguardo de los registros de llamadas (CDR), para lo cual aplica lo dispuesto en el artículo 52 del RPUF, el cual establece un plazo mínimo de cuatro (4) años para conservar los registros detallados de las comunicaciones (llamadas y SMS) que cursen los usuarios finales dentro o fuera de sus redes.

5.1.13. Acoger dividir la implementación gradual de la totalidad de requerimientos dispuestos en la regulación sometida a consulta pública en 3 fases.

5.1.14. Acoger la observación planteada por **Claro CR Telecomunicaciones S.A. (Claro)** respecto a incorporar en la fase 2 del cronograma el intercambio de información entre operadores y proveedores.

5.1.15. Rechazar las observaciones restantes presentadas por **Claro CR Telecomunicaciones S.A. (Claro)**

5.1.16. Acoger la observación planteada por el **Instituto Costarricense de Electricidad (ICE)** respecto a ampliar el plazo de implementación.

5.1.17. Acoger parcialmente la solicitud planteada por el **Instituto Costarricense de Electricidad (ICE)** respecto de emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

5.1.18. Rechazar las observaciones restantes presentadas por el **Instituto Costarricense de Electricidad (ICE)**.

5.1.19. Acoger la observación planteada por **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty)** respecto a ampliar el plazo de implementación.

5.1.20. Acoger la propuesta de **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty)** sobre la implementación de un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos A2P sin recibir respuesta del usuario receptor.

5.1.21. Rechazar las observaciones restantes presentadas por **Liberty Telecomunicaciones de Costa Rica LY, S.A. (Liberty).**

5.1.22. Acoger la observación planteada por el **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)** respecto a incorporar mecanismos de seguimiento, de modo que, de la misma forma que se requirió en la resolución RCS-294-2023, se solicitará a los operadores y proveedores reportes cuatrimestrales relacionados a la cantidad de mensajes SMS y llamadas bloqueadas por ser identificadas como tráfico malicioso.

5.1.23. Acoger la observación planteada por el **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT)** respecto a ampliar el plazo de implementación de las presentes disposiciones regulatorias.

5.1.24. Rechazar las observaciones restantes presentadas por el **Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).**

5.1.25. Acoger la observación planteada por la **Cámara de Infocomunicación y Tecnología (INFOCOM)** respecto a ampliar el plazo de implementación.

5.1.26. Acoger la observación planteada por la **Cámara de Infocomunicación y Tecnología (INFOCOM)** respecto a emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023.

5.1.27. Rechazar las observaciones restantes presentadas por la **Cámara de Infocomunicación y Tecnología (INFOCOM).**

5.1.28. Rechazar en su totalidad las observaciones presentadas por **Millicom Cable Costa Rica, S.A. (Tigo)** por haber sido presentadas de forma extemporánea.

5.1.29. Modificar parcialmente la propuesta regulatoria "*ANÁLISIS DEL ALCANCE DE LA RCS-294-2023 "METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DE ENMASCARAMIENTO DE LLAMADAS" PARA IMPLEMENTARSE EN EL SERVICIO DE MENSAJERÍA DE TEXTO Y SUS DIFERENTES MODALIDADES (SMS)*" bajo los siguientes términos:

a) Cambiar la anterior denominación y definir la resolución que se emita como ***"MEDIDAS REGULATORIAS PARA MINIMIZAR EL IMPACTO DE CIBERATAQUES POR SMISHING (SMS) Y VISHING (VOZ) EN LAS REDES DE TELECOMUNICACIONES"***.

b) Agregar un nuevo inciso en la sección 9.1 que se lea: *"F. Los operadores y proveedores de mensajería SMS deben brindar comprobante de entrega y recepción de mensaje SMS para la evaluación de tasas de éxito de entrega de mensajes, además de, cualquier configuración necesaria entre operadores y proveedores para garantizar el cumplimiento de las obligaciones dispuestas en la presente normativa."*.

c) Agregar un nuevo inciso en la sección 9.1 que se lea: *"G. Los operadores y proveedores de mensajería SMS deben presentar un informe de forma cuatrimestral con la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus respectivos bloqueos, diferenciando entre mensajes P2P y A2P."*.

d) Agregar un nuevo inciso en la sección 9.1 que se lea: *"H. Los operadores y proveedores de mensajería SMS deben conservar los registros detallados de las comunicaciones que cursen los usuarios finales dentro o fuera de sus redes durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF)".*

e) Agregar un nuevo inciso en la **sección 9.1** que se lea: *"**I.** Los operadores y proveedores deben disponer de Centros de Atención al Usuario Final para que sus clientes puedan reportar al operador que les brinda el servicio de mensajería SMS y con el cual mantienen una relación comercial, los casos donde exista sospecha de smishing"*.

f) Modificar parcialmente el **inciso C** de la **sección 9.5** para que se lea: *"**C.** Los operadores y proveedores deben disponer Centros de Atención al Usuario Final para que sus clientes puedan reportar al operador que les brinda el servicio de telefonía y con el cual mantienen una relación comercial, los casos donde exista sospecha de vishing."*.

g) Agregar un nuevo inciso en la sección 9.5 que se lea: *"F. Los operadores y proveedores de telefonía deben presentar un informe de forma cuatrimestral, con la cantidad de llamadas identificadas como maliciosas (vishing) y sus respectivos bloqueos"*.

h) Agregar un nuevo inciso en la sección 9.5 que se lea: *"G. Los operadores y proveedores de telefonía deben conservar los registros detallados de las comunicaciones que cursen los usuarios finales dentro o fuera de sus redes durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del Reglamento Sobre el Régimen de Protección al Usuario Final (RPUF)"*.

i) Modificar parcialmente el inciso E de la sección 9.3 para que se lea: *"E. Los operadores y proveedores deben establecer registros de los clientes autorizados a enviar tráfico de SMS A2P y/o clientes autorizados a enviar grandes cantidades de mensajes A2P informativos, sin recibir respuesta del usuario receptor. Estos registros serán actualizados con el ingreso o retiro de un nuevo cliente emisor de mensajes SMS A2P o de campañas de envío masivo de mensajes A2P, donde se indique el nombre del cliente y el segmento de numeración que hace uso. Además, esta Superintendencia podrá consultar a los operadores y proveedores dichos registros. Los operadores y proveedores de mensajería SMS A2P deben verificar adecuadamente la identidad de sus clientes y la finalidad en cuanto al uso que pretende hacer el cliente con el volumen de mensajes A2P, garantizando que solo usuarios legitimos se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no incluidos en este registro, así mismo para generadores de campañas de envío*

masivo de mensajes no autorizados. Esto aplica de igual forma para las rutas de interconexión, de modo que, solo se enviará a otros operadores el tráfico A2P de remitentes autorizados y previamente verificados. Los operadores y proveedores pueden incluir métodos de reputación a discreción para garantizar que las empresas y el contenido de los mensajes son legítimos y no atentan contra la seguridad de otros usuarios. Estos registros se deben compartir entre operadores y proveedores interconectados.".

j) Modificar en su totalidad el inciso A de la sección 9.6 para que se lea: *"Los proveedores y operadores con numeración asignada por esta Superintendencia, deben proceder con la implementación de las medidas dispuestos en esta normativa, mediante una implementación gradual y progresiva dividida en 3 fases, cuyo plazo corre a partir de la publicación de la presente metodología regulatoria en el diario Oficial La Gaceta. Cada una de estas 3 fases se detalla a continuación:*

1) Fase 1. Plazo de 180 días (6 meses): implementación de medidas de seguridad básicas en servicios de mensajería SMS.

*Del apartado **9.1 SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P**, las siguientes medidas deben ser implementadas dentro del plazo de 180 días:*

a) *Inciso A sobre asegurar la trazabilidad del tráfico de mensajes SMS desde el origen y hasta el destino, bloqueando todo tráfico no trazable o que intente evadir filtros de seguridad.*

b) *Inciso B sobre bloquear el tráfico de mensajes SMS que no especifique atributos de identificación que permitan conocer el origen de la comunicación.*

c) *Inciso C subinciso 1, sobre diferenciar el tráfico de tipo P2P del A2P.*

d) *Inciso C subinciso 2, sobre bloquear tráfico A2P o P2P con origen internacional, cuyo número de origen haya sido enmascarado con un número local.*

e) *Inciso C subinciso 4, sobre verificación en tiempo real del origen del mensaje.*

f) *Inciso C subinciso 10, sobre detección y bloqueo automático de servicios que superen umbrales de tasa y volumen de mensajes no correspondientes a un comportamiento humano.*

g) *Inciso C subinciso 13, sobre análisis de simetría en las comunicaciones para identificar el tráfico que nunca recibe respuesta.*

h) *Inciso C subinciso 14, sobre el bloqueo del tráfico de mensajes SMS internacional que de cualquier manera simule ser de tipo local.*

i) *Inciso D sobre el bloqueo del tráfico de mensajes SMS internacional que de cualquier manera simule ser de tipo local.*

j) *Inciso F propuesto anteriormente, sobre que los operadores faciliten cualquier configuración necesaria entre operadores y proveedores para garantizar el cumplimiento de las obligaciones dispuestas en la presente normativa.*

k) *Inciso G propuesto anteriormente, sobre presentar un informe de forma cuatrimestral con la cantidad de mensajes SMS identificados como maliciosos (smishing) y sus respectivos bloqueos, diferenciando entre mensajes P2P y A2P.*

l) *Inciso H propuesto anteriormente, sobre conservar los registros detallados de las comunicaciones durante un plazo mínimo de cuatro (4) años, de conformidad con el artículo 52 del RPUF.*

m) *Inciso I propuesto anteriormente, sobre disponer de centros de atención al usuario final para el reporte de casos de smishing.*

*Con respecto al apartado **9.3 SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P**, la totalidad de las medidas dispuestas en este apartado deben ser implementadas dentro del plazo de 180 días, las cuales corresponde a los incisos A, B, C, D y E de esta sección.*

*Del apartado **9.5. SERVICIOS DE LLAMADAS DE VOZ**, las siguientes medidas deben ser implementadas dentro del plazo de 180 días:*

a) *Inciso C sobre disponer de centros de atención al usuario final para el reporte de casos de vishing.*

2) Fase 2. Plazo de 360 días (12 meses): implementación de medidas de seguridad avanzadas en servicios de mensajería SMS.

*Del apartado **9.1 SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P**, las siguientes medidas deben ser implementadas dentro del plazo de 360 días:*

a) *Inciso C subinciso 3 sobre incorporar capacidades con Inteligencia Artificial para analizar el contenido completo de los mensajes SMS mediante Inspección Profunda de Paquetes (DPI).*

b) *Inciso C subinciso 5 sobre incorporar mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados en la red que envían tráfico masivo.*

c) *Inciso C subinciso 6 sobre incorporar Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP) y Análisis Heurístico.*

d) *Inciso C subinciso 7 sobre contar con capacidad de identificar enlaces maliciosos en el contenido de los mensajes SMS P2P y A2P.*

e) *Inciso C subinciso 8 sobre contar uso de sistemas de reputación de enlaces.*

f) *Inciso C subinciso 9 sobre contar con capacidad de analizar mensajes en formato binario y cualquier otro formato técnico de codificación aplicable a los servicios de mensajería móvil.*

g) *Inciso C subinciso 11 (incluido los apartados a, b, c y d de este subinciso) sobre contar con capacidad de identificar campañas de smishing.*

h) *Inciso C subinciso 12 sobre contar con capacidad de detectar ráfagas de spam (Spam Burst) y campañas de smishing rápidas.*

i) *Inciso C subinciso 15 sobre contar con capacidad de detectar Tráfico Inflado Artificialmente (AIT).*

j) *Inciso D sobre uso de sistemas de reputación de enlaces.*

k) *Inciso E sobre las condiciones para analizar el contenido de los mensajes mediante Inspección Profunda de Paquetes (DPI).*

3) Fase 3. Plazo de 540 días (18 meses): implementación de medidas de seguridad avanzadas en servicios de voz.
Esta fase comprende la implementación de las medidas dispuestas en el apartado 9.5. SERVICIOS DE LLAMADAS DE VOZ, las cuales deben estar en funcionamiento dentro del plazo de 540 días:

a) *Inciso A y sus subincisos a), b), c), d) y e) sobre incorporar sistemas de firewall antispam en los servicios de voz con capacidades de procesamiento masivo de registros de llamadas, procesamiento de información de señalización, detección de patrones de comportamiento sospechoso, identificación de llamadas automatizadas con grabaciones o voz sintética*

b) *Inciso B sobre destinar un rango de números telefónicos para la implementación de señuelos.*

c) *Inciso D sobre adoptar e implementar el estándar Out-of- Band SHAKEN (OOBS).*

d) *Inciso E sobre mantener el cumplimiento de los lineamientos establecidos en la resolución RCS-294-2023.*

e) *Inciso F propuesto anteriormente, sobre presentar un informe de forma cuatrimestral con la cantidad de llamadas de voz identificadas como maliciosas (vishing) y sus respectivos bloqueos.*

f) *Inciso G propuesto anteriormente, sobre conservar los registros detallados de llamadas por un plazo mínimo de 4 años, conforme el artículo 52 del RPUF.".*

k) Agregar un nuevo apartado con la definición de trazabilidad que se lea:

*"**SOBRE LA TRAZABILIDAD DE LAS COMUNICACIONES.***

La trazabilidad de las comunicaciones debe entenderse como la capacidad del operador de identificar, autenticar, correlacionar y registrar de forma confiable el origen, la ruta de transmisión y el destino de cada comunicación, en cumplimiento con el Plan Nacional de Numeración y los esquemas autorizados de interconexión.

En mensajería SMS, un mensaje se considerará trazable cuando su origen pueda ser inequívocamente determinado y validado, ya sea como tráfico P2P asociado a un usuario final legítimo, correctamente autenticado en la red, o como tráfico A2P proveniente de un agregador, proveedor o entidad previamente registrado, validado y autorizado por el operador.

La trazabilidad implica, como mínimo, la verificación de la consistencia de la numeración de origen, la integridad de los parámetros de señalización, la validación de la ruta de entrada como puntos de interconexión, agregadores o proveedores internacionales, así como la correlación con registros de comunicaciones y perfiles de tráfico conocidos. Asimismo, el destino de la comunicación deberá corresponder a una numeración válida y coherente con el plan de numeración vigente.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o filtrar aquellos mensajes SMS cuya trazabilidad no pueda ser garantizada, incluyendo, entre otros, casos de manipulación o suplantación de identidad, incongruencias en la señalización, rutas de origen no autorizadas, ausencia de registro o validación del emisor A2P, o imposibilidad de asociar el tráfico a

un usuario o entidad legítima. Estas medidas podrán implementarse mediante mecanismos técnicos tales como firewalls SMS, sistemas de reputación, análisis de patrones de tráfico y validaciones en tiempo real de señalización y numeración.

En el caso de los servicios de llamadas, se entenderá por trazabilidad la capacidad del operador de identificar y validar de forma confiable el origen, la ruta de señalización y el destino de cada comunicación, en concordancia con el Plan Nacional de Numeración y los acuerdos de interconexión vigentes. Una llamada se considerará trazable cuando el identificador de origen pueda ser verificado como perteneciente a un usuario legítimo o a una entidad autorizada, y cuando la ruta de entrada y los parámetros de señalización sean consistentes y no presenten indicios de manipulación o suplantación.

En consecuencia, los operadores estarán facultados para bloquear, rechazar o etiquetar aquellas llamadas cuya trazabilidad no pueda ser garantizada, incluyendo casos de vishing, rutas internacionales no autorizadas o inconsistencias en la señalización, mediante el uso de mecanismos técnicos como validación de identidad de origen, análisis de patrones de tráfico y controles en puntos de interconexión.”.

5.1.30. Solicitar a la Secretaría del Consejo de esta Superintendencia gestionar la publicación en el Diario oficial La Gaceta el texto íntegro de la resolución que se adjunta.

5.1.31. Requerir a la Unidad de Comunicación que, una vez publicada la resolución denominada **“*MEDIDAS REGULATORIAS PARA MINIMIZAR EL IMPACTO DE CIBERATAQUES POR SMISHING (SMS) Y VISHING (VOZ) EN LAS REDES DE TELECOMUNICACIONES*”** en el diario oficial La Gaceta debe proceder con la publicación correspondiente en el sitio WEB de esta Superintendencia, señalando que dicha resolución de carácter general se encuentra vigente.

6. FIRMEZA DEL ACUERDO

Por disposición del artículo 56 de la Ley N° 6227, los acuerdos que alcance el Consejo de la Sutel deberán estar contenidos en el acta de la sesión en la que se adopten y ésta a su vez será aprobada en la sesión ordinaria siguiente.

Excepcionalmente, el Consejo de la Sutel podrá disponer la firmeza del acuerdo sin necesidad de aprobación posterior, para lo cual requerirá de la votación de dos terceras partes de la totalidad de sus miembros.

La declaratoria en firme de un acto sin aprobación posterior, supone la supresión de la posibilidad de imponer el recurso de revisión previsto en el artículo 55 de la misma Ley N°6227.

San José, 12 de junio 2026
05772-SUTEL-DGM-2026

Bajo este entendido, se sugiere la conveniencia de conocer el presente informe y declarar en firme su disposición, así por tratarse de un procedimiento administrativo sujeto a plazos reducidos y debido a la importancia e impacto que representa para la seguridad de las redes de telecomunicaciones y la protección de los derechos de los usuarios.

Atentamente,
SUPERINTENDENCIA DE TELECOMUNICACIONES

DERYHAN MUÑOZ BARQUERO (FIRMA)
PERSONA FISICA, CPF-06-0328-0822.
Fecha declarada: 12/06/2026 01:08:48 p. m.

Deryhan Muñoz Barquero
Directora General
Dirección General de Mercados

GLENN FALLAS FALLAS (FIRMA)
Firmado digitalmente por GLENN FALLAS FALLAS (FIRMA)

Glenn Fallas Fallas
Director General
Dirección General de Calidad

JUAN GABRIEL GARCIA RODRIGUEZ (FIRMA)
Firmado digitalmente por JUAN GABRIEL GARCIA RODRIGUEZ (FIRMA)
Fecha: 2026.06.12 14:22:24 -06'00'

Juan Gabriel García Rodríguez
Jefe Dirección General de Mercados

NATALIA RAMIREZ ALFARO (FIRMA)
Firmado digitalmente por NATALIA RAMIREZ ALFARO (FIRMA)
Fecha: 2026.06.12 12:15:54 -06'00'

Natalia Ramírez Alfaro
Dirección General de Calidad

JOSUE CARBALLO HERNANDEZ (FIRMA)
PERSONA FISICA, CPF-01-1162-0699.
Fecha declarada: 12/06/2026 01:13:24 p. m.

Josué Carballo Hernández
Dirección General de Mercados

JOSE ALFONSO SANCHEZ SAENZ (FIRMA)
Firmado digitalmente por JOSE ALFONSO SANCHEZ SAENZ (FIRMA)
Fecha: 2026.06.12 12:13:40 -06'00'

José Sánchez Sáenz
Dirección General de Calidad

CARMEN CASCANTE ARIAS (FIRMA)
Firmado digitalmente por CARMEN CASCANTE ARIAS (FIRMA)
Fecha: 2026.06.12 12:10:09 -06'00'

Carmen Cascante Arias
Dirección General de Calidad

JASS/CCA/JCH
Adjunto: RESOLUCIÓN DE IMPLEMENTACIÓN DE MEDIDAS REGULATORIAS PARA MINIMIZAR EL IMPACTO DE CIBERATAQUES POR SMISHING (SMS) Y VISHING (VOZ) EN LAS REDES DE TELECOMUNICACIONES.
Exp: GCO-DGM-IET-00518-2026.