El suscrito, Secretario del Consejo de la Superintendencia de Telecomunicaciones, en ejercicio de las competencias que le atribuye el inciso b) del artículo 50 de la Ley General de la Administración Pública, Ley 6227, y el artículo 35 del Reglamento Interno de Organización y Funciones de la Autoridad Reguladora de los Servicios Públicos y su Órgano Desconcentrado, me permito comunicar que en sesión ordinaria 035-2026, celebrada el 18 de junio de 2026, mediante acuerdo 021-035-2026 de las 11:45 horas, el Consejo de la Superintendencia de Telecomunicaciones aprobó por unanimidad, la siguiente resolución: ----------

RCS-151-2026

"MEDIDAS REGULATORIAS CON EL FIN DE MINIMIZAR EL IMPACTO DE CIBERATAQUES MEDIANTE MENSAJES DE TEXTO SMS (SMISHING) Y LLAMADAS (VISHING) EN LAS REDES DE TELECOMUNICACIONES"

EXPEDIENTE: GCO-DGM-IET-00518-2026

RESULTANDO

1. Que, el 30 de noviembre de 2023, el Consejo de la Superintendencia de Telecomunicaciones (SUTEL) dictó la resolución RCS-294-2023 adoptada mediante el acuerdo 024-072-2023 alcanzado en sesión ordinaria 072-2023 en la que se estableció 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*" (Folios 167 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

2. Que, 24 de enero de 2024 se publicó la resolución RCS-294-2023, en el alcance número 11 del Diario Oficial La Gaceta número 13 (NI-00840-2024) (Folios 221 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

3. Que, mediante oficio 263-392-2024 del 07 de mayo del 2024 (NI-05978-2025), el Instituto Costarricense de Electricidad (en adelante el ICE) presentó el primer informe cuatrimestral establecidas en la RCS-294-2023 (Folios 265 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

4. Que, mediante oficio número 04721-SUTEL-DGM-2024 de 06 de junio de 2024, la DGM solicitó a los operadores y proveedores de servicios de telecomunicaciones con numeración asignada por esta Superintendencia, la remisión del cumplimiento de lo dispuesto en la resolución administrativa RCS-294-2023 (Folios 288 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

5. Que, mediante oficio RI-0878-2024 de fecha del 30 de agosto de 2024 (NI-11593-2024) la empresa Claro CR Telecomunicaciones S.A. (en adelante CLARO) remitió el reporte de bloqueos de llamadas en las rutas internacionales de numeración fija (Folios 300 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

6. Que, mediante oficio CAFF-193-2024 de fecha del 03 de setiembre de 2024 (NI-11772-2024) la empresa Millicom Cable Costa Rica, S.A. (en adelante TIGO) remitió el reporte de bloqueos de llamadas en las rutas internacionales de la numeración fija (Folios 303 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

7. Que, mediante oficio 263-713-2024 del 06 de setiembre del 2024 (NI-11898-2024), el ICE remitió el informe cuatrimestral establecido en la resolución

RCS-294-2023 (Folios 308 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

8. Que por medio del oficio 9182-516-2024 del 09 de agosto del 2024 (NI-13935-2024) el ICE consulta sobre la aplicación de la resolución RCS-294-2023 a los SMS A2P nacional e internacional, en razón a los siguientes términos: *"(…) 1. ¿La resolución 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" es aplicable a los SMS A2P nacional e internacional? (…) 2. ¿Existe una fecha prevista para el inicio del proceso de revisión regulatoria de la resolución RCS-294-2023 donde, conforme a lo establecido por el Consejo de la SUTEL, se revise su efectividad y se reciba retroalimentación de los interesados? (...)"* (Folios 311 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

9. Que mediante oficio número 09814-SUTEL-DGM-2024, la DGM atendió la consulta planteada por el ICE mediante el oficio 9182-516-2024 del 09 de agosto del 2024 (NI-13935-2024) indicando lo siguiente: *"(…) la resolución administrativa RCS-294-2023 "Metodología regulatoria para la implementación de medidas con el fin de minimizar el impacto de estafas telefónica mediante el método de enmascaramiento de llamadas", la cual es objeto de consulta. (…) sí dicha resolución es aplicable a los SMS A2P nacional e internacional, se debe indicar que conforme a la información que consta en el expediente administrativo GCO-DGM-IET-01223-2022, esta norma regulatoria tiene un enfoque de dirigido exclusivamente a las llamadas telefónicas y su enmascaramiento ("spoofing"). (...). Excluyendo por tanto la interacción de la mensajería de texto (SMS) en cualquiera de sus modalidades P2P (person -to -person, por sus siglas en inglés, es el intercambio de mensajes entre individuos, típico mensaje de*

texto entre usuarios de teléfonos móviles) o A2P (aplication-to-person, el cual corresponde al intercambio de mensajes entre aplicaciones o sistemas automatizados a personas). En este contexto, la regulación RCS-294-223 no sería aplicable a los SMS A2P(...)". Con relación a la actualización de la metodología regulatoria se encuentra la Administración en el proceso de recopilación de los datos a efectos de realizar el análisis correspondiente. (Folios 316 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

10. Que mediante oficio 9182-662-2024 del 13 de diciembre del 2024 (NI-16342-2024) el ICE, indicó lo siguiente: *"(…) como en la mejor disposición para colaborar con la SUTEL en dicho proceso de consulta pública a fin de valorar la procedencia de que se incorporen dentro de dichas disposiciones lo relativo a regulación de los mensajes SMS A2P nacional e internacional, conforme a lo manifestado por el ICE en el oficio 9182-516-2024 antes citado (…)".* (Folios 320 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

11. Que mediante oficio número 11272-SUTEL-DGM-2024 de 20 de diciembre del 2024 la DGM, remitió un recordatorio a los operadores y proveedores de servicios de telecomunicaciones con numeración asignada para uso comercial hacia el usuario final a razón que remitan lo dispuesto en la RCS-294-2023, en la parte dispositiva del POR TANTO correspondiente al numeral 6. (Folios 323 y sgts del expediente GCO-DGM-IET-01223-2022).

12. Que, Mediante oficio 00212-INTP-2024 de fecha del 31 de diciembre del 2024 (NI-16816-2024) la empresa interphone, S.A. (en adelante INTERPHONE) atiende la solicitud del oficio número 11272-SUTEL-DGM-2024, indicando *"(…) nuestro equipo realiza la entrega de los servicios mediante la metodología de P -Asserted-Identity garantizando que las llamadas realizadas únicamente*

puedes ser generadas con el numero IP asignado". (Folios 327 y sgts del expediente GCO-DGM-IET-01223-2022). ----------

13. Que, mediante correo electrónico del 31 de diciembre del 2024 (NI-00004-2025) la Cooperativa de Electrificación Rural de Guanacaste, R.L. (en adelante COOPEGUANACASTE), atendió la solicitud del oficio número 11272-SUTEL-DGM-2024, en el cual dispone lo siguiente *"(…) ya que nuestro proveedor de interconexión para telefonía nacional e internacional es la empresa R&H, en teoría ellos realizan el bloqueo del enmascaramiento de llamadas, por este motivo saber si debemos presentar este reporte (…)"* (Folio 330 del expediente GCO-DGM-IET-01223-2022). ----------

14. Que por medio del oficio GCI SP de fecha del 31 de diciembre del 2024 (NI-00013-2025) la empresa GCI Service Provider S.A. presentó el reporte de bloqueo de llamadas indicando que no tiene numeración pública asignada en interconexiones directas internacionales (Folio 331 al 332 del expediente GCO-DGM-IET-01223-2022). (NI-15284-2025). ----------

15. Que mediante oficio 0001-METROCOM-DGG-2025 de fecha del 02 de enero del 2025, (NI-0023-2025) la empresa Comunicaciones Metropolitanas Metrocom S.A. indicó un reporte de cero llamadas bloqueadas (Folios 334 al 335 del expediente GCO-DGM-IET-01223-2022). ----------

16. Que, mediante oficio sin número con fecha del 31 de diciembre del 2024, la empresa Ring Centrales de Costa Rica, S.A. (NI-00080-2025), reportó un total de 6 llamadas bloqueadas para el año 2024 (Folios 336 AL 661 del expediente GCO-DGM-IET-01223-2022). ----------

17. Que, mediante oficio LY-Reg0005-2025 de fecha del 08 de enero 2025 (NI-00196-2025), la empresa LIBERTY remitió las llamadas bloqueadas al año

2024 que corresponden a un total de 48.522 (NI-00196-2025) (Folios 662 al 663 del expediente GCO-DGM-IET-01223-2022). ----------

18. Que mediante oficio CAFF-8-2025 del 09 de enero del 2025 (NI-00222-2025, la empresa TIGO, indicó que el sistema realizo el bloqueo de seiscientas ochenta mil novecientas treinta y siete llamadas (680.937) (Folios 664-670 del expediente GCO-DGM-IET-01223-2022). ----------

19. Que por medio del oficio 263-55-2025 de fecha del 17 de enero del 2025 (NI-00653-2025), el ICE indicó la cantidad de llamadas bloqueadas correspondiendo a un total de 1.786.231 llamadas bloqueadas para el año 2024 (Folios 671 al 673 del expediente GCO-DGM-IET-01223-2022). ------

20. Que mediante oficio RI-0010-2025 de fecha del 20 de enero del 2025 (NI-00722-2025) la empresa CLARO indicó que las llamadas bloqueadas en setiembre 24 corresponde a 326.539, octubre 24 a 231.537, noviembre a 267.700 y diciembre 24 a 178.779. (Folios 674 al 677 del expediente GCO-DGM-IET-01223-2022). ----------

21. Que mediante oficio 00574-SUTEL-DGM-2025 del 22 de enero de 2025, la DGM, atendió el oficio 9186-662-2024 (NI-16342-2024) del 17 de diciembre del 2024, y señaló: *"En esta línea, se remitió el oficio 11272-SUTEL-DGM-2024, "Recordatorio al cumplimiento de las disposiciones establecidas en las resoluciones administrativas RCS-222-2022 y RCS-294-2023", con fecha 20 de diciembre de 2024, a todos los operadores y proveedores con numeración asignada por esta Superintendencia. En dicho oficio se solicita la información requerida para el proceso de análisis, cuyo objetivo es determinar los ajustes regulatorios necesarios para optimizar la resolución y reducir las distintas formas de estafa a través de servicios de telecomunicaciones. Una vez completadas estas gestiones, se procederá a realizar una invitación a los operadores y*

proveedores con numeración asignada por esta Superintendencia. Esta convocatoria incluirá los hallazgos y demás consideraciones relevantes que puedan incorporarse en una actualización regulatoria relacionada con el tema de su consulta. Este proceso se llevará a cabo durante el primer semestre de 2025." (Folio 678 al 680 del expediente GCO-DGM-IET-01223-2022). ----------

22. Que mediante oficio 9182-130-2025 del 28 de marzo del 2025 (NI-04177-2025) el ICE respondió al oficio 00574-SUTEL-DGM-2025 y señaló en lo que interesa lo siguiente: *"Quedamos atentos a su respuesta, así como en la mejor disposición para colaborar con la SUTEL en dicho proceso de consulta pública a fin de valorar la procedencia de que se incorporen dentro de dichas disposiciones lo relativo a regulación de los mensajes SMS A2P nacional e internacional, conforme a lo manifestado por el ICE en el oficio 9182-516- 2024 antes citado"*. (Folios 683 al 686 del expediente GCO-DGM-IET-01223-2022). ----------

23. Que, mediante oficio LY-Reg0091-2025 del 09 de abril 2025 (NI-04670-2025) la empresa LIBERTY remitió el reporte de llamadas bloqueadas para el I Trimestre 2025. (Folios 687 al 688 del expediente GCO-DGM-IET-01223-2022). ----------

24. Que mediante oficio 03422-SUTEL-DGM-2025 del 24 de abril del 2025 la DGM en relación a lo dispuesto en el POR TANTO 6 de la RCS-294-2023, realizó una consulta e informó a los operadores y proveedores de servicios de telecomunicaciones con numeración lo siguiente: *"(...) con el fin de proceder con el análisis y revisión de la citada resolución, considera oportuno realizar una consulta informal a los operadores y proveedores de servicios de telecomunicaciones con numeración asignada, con el fin de conocer el criterio respecto otras acciones que permitan*

ampliar el alcance de la medida al bloqueo de otros tipos de comunicación con el fin de minimizar el impacto de estafas a través de los servicios de telecomunicaciones (…)". (Folios 689 al 698 del expediente GCO-DGM-IET-01223-2022). ----------

25. Que mediante correo electrónico del 28 de abril del 2025 (NI-05270-2025) la empresa DIDWW CR, S.A. indicó que inició recientemente operaciones y en consecuencia no puede referirse a la solicitud del oficio 03422-SUTEL-DGM-2025. (Folio 705 del expediente GCO-DGM-IET-01223-2022). -------

26. Que mediante oficio 64_CMW_25 del 28 de abril del 2025 (NI-05325-2025) la empresa Callmyway NY, S.A. (en adelante CMW) indicó que las medidas de la resolución RCS-294-2023 son adecuadas y no tienen inconvenientes para la operación y solicitó que se elimine el reporte cuatrimestral de la cantidad de llamadas que se bloquean. (Folios 706 al 707 del expediente GCO-DGM-IET-01223-2022). ----------

27. Que mediante oficio RNG-034-2025 del 25 de abril (NI-05590-2025) la empresa Ring Centrales de Costa Rica S.A. solicitó que se implemente la siguiente solución técnica: *"• Adoptar un estándar internacional como STIR/SHAKEN, el cual ha sido implementado exitosamente en otras jurisdicciones y permite verificar la autenticidad del número de origen sin bloquear de manera indiscriminada las comunicaciones. • En su defecto, establecer una lista de opt-out, en la cual los usuarios que deseen restringir el uso de su número desde terceros proveedores puedan hacerlo de forma explícita. • Como última instancia, implementar una lista de consentimiento (opt-in), donde los usuarios autoricen expresamente el uso de su número desde un proveedor distinto al asignado originalmente"*. (Folio 708 al 709) del expediente GCO-DGM-IET-01223-2022. ----------

28. Que mediante oficio 70_CMW_25 de fecha del 05 de mayo del 2025 (NI-05680-2025) la empresa CMW remitió el reporte de llamadas bloqueadas al 30 de abril con un total de 1.031.971 llamadas (Folio 710 al 711 del expediente GCO-DGM-IET-01223-2022). ----------

29. Que, mediante oficio CAFF-79-2025 de fecha del 07 de mayo del 2025 (NI-05834-2025) la empresa TIGO indicó lo siguiente en atención al oficio 03244-SUTEL-2025, *"(...) fuera del límite de minutos. También se implementaron expresiones regulares al número ANI para evitar que numeraciones mal formadas puedan efectuar llamadas. Adicionalmente las troncales SIP que tenemos con nuestros distintos clientes, solo permiten que ingresen llamadas de los ANI configurados para dicha troncal. Fuera de esto, las mejoras en la posible seguridad de la telefonía dependen también de los mecanismos que se implementen del lado del suscriptor final, como: parcheo de las centrales telefónicas (...)"* (Folios 712 al 714 del expediente GCO-DGM-IET-01223-2022).----------

30. Que mediante oficio 00218-INTP-2025 del 04 de mayo del 2025 (NI-05901-2025) la empresa INTERPHONE indicó que utiliza el sistema P-Asserted-Identy garantizando que las llamadas solo puedan realizarse por un número IP asignado. (Folio 715 al 716 del expediente GCO-DGM-IET-01223-2022).

31. Que mediante correo electrónico del 09 de mayo del 2025 (NI-05969-2025) la empresa R&H International Telecom Services, S.A. (en adelante R&H) presentó la cantidad de llamadas bloqueadas (Folio 717 del expediente GCO-DGM-IET-01223-2022). ----------

32. Que mediante oficio CG-GT-01-090525 del 09 de mayo del 2025 (NI-05981-2025) la empresa COOPEGUANACASTE, indicó que la conexión

internacional se hace por medio de la empresa R&H. (Folios 718 al 720 del expediente GCO-DGM-IET-01223-2022). ----------

33. Que mediante oficio RI-0180-2025 del 08 de mayo del 2025 (NI-05993-2025) la empresa CLARO, presentó el reporte de llamadas bloqueadas al primer cuatrimestre; correspondiendo al mes de enero un total de 143.156; febrero un total de 139.300, marzo un total de 133.298 y abril un total de 129.600. (Folio 721 al 723 del expediente GCO-DGM-IET-01223-2022). ---

34. Que mediante nota sin número de fecha del 13 de mayo del 2025 (NI-06191-2025) la empresa Telecable, S.A. atendió la nota 03422-SUTEL-DGM-2025 y señaló: *"(...) aplicabilidad técnica de la citada resolución dentro de nuestra infraestructura de red. Telecable S.A. no opera rutas de interconexión internacional directa, por lo que los mecanismos de bloqueo estipulados en el inciso II de la Resolución de referencia, no resultan técnicamente aplicables en nuestro entorno operativo y regulatorio. En este sentido, las llamadas internacionales que ingresan a nuestra red lo hacen únicamente en calidad de tránsito, a través de operadores nacionales que sí poseen interconexión internacional directa, específicamente CallMyWay, CLARO, ICE, LIBERTY y TIGO. En consecuencia, el control inicial sobre el tráfico internacional debería recaer en dichos proveedores, quienes desempeñan un papel clave en la detección y prevención temprana de llamadas no autorizadas, que podrían propagarse hacia el resto de la Red Pública Telefónica Conmutada (PSTN), incluida aquella gestionada por Telecable"*. (Folios 724 al 730 del expediente GCO-DGM-IET-01223-2022). ----------

35. Que mediante oficio 263-362-2025 del 13 de mayo del 2025 (NI-06239-2025), el ICE atendió la nota 03422-SUTEL-DGM-2025 e indicó lo siguiente: *"(...) De conformidad con la información enviada por las áreas competentes de la Gerencia de Telecomunicaciones, hacemos de su conocimiento que el ICE no Visualiza otras*

acciones adicionales que minimicen el impacto de las estafas telefónicas mediante el método del enmascaramiento de llamada". (Folio 731 al 732 del expediente GCO-DGM-IET-01223-2022). ----------

36. Que mediante oficio 263-374-2025 del 19 de mayo del 2025 (NI-06550-2025) el ICE, remitió el reporte cuatrimestral del año 2025 del bloqueo de llamadas indicando un total de 2.509.817. (Folio 733 al 735) del expediente GCO-DGM-IET-01223-2022. ----------

37. Que mediante oficio RI-0232-2025 del 04 de junio de 2025 (NI-07453-2025) la empresa CLARO respondió el oficio 03422-SUTEL-DGM-2025 e indicó que los sistemas de la empresa CLARO, realiza el bloqueo efectivo y para una evaluación más precisa requiere un mayor contexto para la valoración de la pretensión de la norma regulatoria. (Folios 736 al 738 del expediente GCO-DGM-IET-01223-2022). ----------

38. Que mediante oficio LY-Reg0191-2025 del 05 de agosto de 2025 (NI-10443-2025), la empresa LIBERTY, presentó el reporte del II cuatrimestre del 2025 referente al bloqueo de llamadas. (Folios 739 al 740 del expediente GCO-DGM-IET-01223-2022). ----------

39. Que, por medio de correo electrónico del 22 de agosto del 2025 la empresa DIDWW CR S.A. indicó que no ha identificado irregularidades de tráfico para el bloqueo de llamadas. (Folio 741 del expediente GCO-DGM-IET-01223-2022). ----------

40. Que, durante el año 2025, la Dirección General de Calidad solicitó al operador LIBERTY en 15 ocasiones la suspensión de más de 30 servicios con numeraciones asignadas a este operador, por prácticas prohibidas

efectuadas mediante mensajes de texto SMS. (Visible en el expediente administrativo FOR-SUTEL-DGC-CA-CGL-00019-2025). ----------

41. Que mediante el acuerdo 023-049-2025 de la sesión ordinaria 049-2025 del Consejo de SUTEL, celebrada el 04 de setiembre del 2025, se requirió a LIBERTY: *"(…) Solicitar a Liberty Telecomunicaciones de Costa Rica LY, S.A., que informe a esta Superintendencia, a través de la Dirección General de Calidad, el cumplimiento de la puesta en operación e implementación efectiva de la solución tecnológica de firewall adaptativo para el filtrado y bloqueo de mensajes SMS maliciosos, incluyendo la remisión de un informe técnico que detalle los avances, resultados obtenidos, y cualquier ajuste realizado posterior a su entrada en funcionamiento, así como la evidencia documental correspondiente que permita verificar la eficacia de dicha solución. (…)"*. (Folios 68 al 77 del expediente L0155-STT-MOT-SA-01320-2025). ----------

42. Que mediante oficio 263-685-2025 del 08 de setiembre del 2025 (NI-12036-2025), el ICE remitió el reporte del bloqueo del II cuatrimestre para un total 3,409,336. (Folios 742 al 744 del expediente GCO-DGM-IET-01223-2022).

43. Que mediante oficio 263-46-2026 del 27 de enero del 2026 (NI-01077-2026), el ICE remitió el reporte del bloqueo de llamadas para el III cuatrimestre para un total de 1.558.350. (Folios 746 al 748 del expediente GCO-DGM-IET-01223-2022). ----------

44. Que mediante oficio número 02238-SUTEL-DGM-2026 con fecha del 06 de marzo de 2026, las Direcciones General de Calidad y General de Mercados 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). ----------

45. Que mediante oficio 02650-SUTEL-SCS-2026 del 18 de marzo del 2026, el Secretario del Consejo de la SUTEL, comunicó el Acuerdo 029-014-2026 de la sesión ordinaria 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). ----------

46. Que, en fecha del 10 de abril de 2026 , se publicó en el diario oficial La Gaceta 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). ----------

47. 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). ----------

48. 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).

49. 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). ----------

50. 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).

51. Que mediante oficio número 7110-399-2026 del 24 de abril de 2026 (NI-05531-2026), el 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). ----------

52. 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). ----------

53. 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). ----------

54. 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). ----------

55. 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). ----------

56. Que por medio del oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 las Direcciones General de Calidad y de Mercados rindieron al Consejo de la SUTEL el "*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)". ----------

57. Que se han realizado las diligencias administrativas necesarias para el dictado de la presente resolución. ----------

CONSIDERANDOS

SOBRE LA PROBLEMÁTICA PLANTEADA ----------

I. SOBRE EL SMISHING (PHISHING MEDIANTE MENSAJES SMS) ----------

1. Que de acuerdo con el desarrollador de soluciones de ciberseguridad **Kaspersky**[1], el *phishing*[2] mediante mensajes de texto SMS (*Short Message Services*), también conocido como ***smishing***, es un ataque de ciberseguridad de suplantación de identidad (*phishing*) a través de mensajes de texto SMS, donde los atacantes engañan a las víctimas para que compartan información confidencial. ----------

2. Que, en materia de protección de los derechos de los usuarios finales de los servicios de telecomunicaciones disponibles al público, a la SUTEL le corresponde garantizar y proteger los derechos de los usuarios y velar por el cumplimiento de los deberes y obligaciones de los operadores y proveedores de telecomunicaciones, asegurando eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, mayor y mejor información, más y mejores alternativas de la prestación de los servicios (artículos 60 y 73 de la LARSP). ----------

[1] https://latam.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it

[2] El **phishing** es un tipo de ciberataque de ingeniería social donde se suplanta la identidad de una entidad o persona para engañar a usuarios mediante diferentes medios de comunicación, con el fin de obtener datos confidenciales, descarguen malwares o se expongan a la ciberdelincuencia. https://www.ibm.com/es-es/think/topics/phishing

3. Que, en el caso de *malwares*, el enlace al que accede la víctima descarga un software malicioso que se instala en el terminal de la víctima, disfrazándose de una aplicación legítima para obtener información sensible y compartirla con los delincuentes. Por otro lado, el enlace también puede llevar a la víctima a un sitio web fraudulento personalizado y diseñado para imitar a sitios legítimos reconocidos, lo que facilita el robo de información. -

4. Que, al respecto, el medio de comunicación Delfino.CR publicó en fecha 15 de octubre de 2025, la nota ***"Los fraudes bancarios aumentan un 65% a nivel mundial en el último año"***[3] donde expuso que, durante el año 2025 los ataques por *smishing* aumentaron 10 veces a nivel global, con un mayor crecimiento en Latinoamérica de hasta 14 veces. ----------

5. Que, el 10 de diciembre de 2025 la Revista Summa publicó la noticia ***"Costa Rica: Ataques con mensajes falsos aumentan 132%"***, donde informó que, en la última edición del Panorama de Amenazas de Kaspersky, se reveló que, en Costa Rica, en el año 2025 se registraron 7,9 millones de intentos de phishing que fueron bloqueados por la empresa de ciberseguridad en la región, lo que representa un promedio de 21.000 detecciones al día. De acuerdo con dicha noticia, este aumento se debe al uso de Inteligencia Artificial por parte de los delincuentes para perfeccionar y automatizar ataques masivos. Además, herramientas digitales que originalmente fueron desarrolladas para optimizar procesos corporativos están siendo utilizadas por los delincuentes para automatizar el envío masivo y personalizado de mensajes fraudulentos, lo que permite a los estafadores alcanzar miles de

[3] https://delfino.cr/2025/10/los-fraudes-bancarios-aumentan-un-65-a-nivel-mundial-en-el-ultimo-ano

víctimas en pocos minutos, con un alto grado de sofisticación y dificultad de rastreo. ----------

6. Que, este aumento en estafas por *smishing* ha llevado a crear campañas de concientización para informar al público general sobre esta amenaza como por ejemplo la nota publicada por el periódico La Republica el 19 de setiembre de 2025, denominada ***"Cuidado con el smishing: 3 recomendaciones para no caer en mensajes de texto falsos"***[4]. Además, otras entidades como la Asociación Bancaria Costarricense[5], Banco de Costa Rica (BCR)[6], Banco Nacional[7], Caja Costarricense de Seguro Social (CCSS)[8], Correos de Costa Rica[9], Instituto Costarricense de Electricidad (ICE)[10], Instituto Mixto de Ayuda Social (IMAS)[11], entre otras, han realizado publicaciones para advertir a sus usuarios sobre intentos de estafa mediante mensajes de texto SMS, donde se suplanta la identidad de estas instituciones. ----------

7. Que, durante el año 2025, la Dirección General de Calidad solicitó al operador **Liberty Telecomunicaciones de Costa Rica LY, S.A.** en 15 ocasiones la suspensión de más de 30 servicios con numeraciones asignadas a este operador, por prácticas prohibidas efectuadas mediante mensajes de texto SMS. ----------

8. Que, lo anterior motivó el acuerdo 023-049-2025 de la sesión ordinaria 049-2025 del Consejo de SUTEL, celebrada el 4 de setiembre del 2025, donde se requirió a este operador *"(…) Solicitar a Liberty Telecomunicaciones de Costa Rica*

---

[4] https://revistasumma.com/costa-rica-ataques-con-mensajes-falsos-aumentan-132/
[5] https://www.abc.fi.cr/prensa/notas-de-prensa-y-comunicados/alerta-de-estafas-por-sms-y-whatsapp-recomendaciones-para-proteger-sus-datos/
[6] https://elguardian.cr/bcr-lanza-campana-alerta-timo-para-proteger-a-clientes-de-fraudes-en-epoca-navidena/
[7] https://www.bncr.fi.cr/blog/smishing-como-protegerse-estafas-sms?srsltid=AfmBOop4UshbLJboErd8fMicOWV9l7-zZAVAY0oYKcwjiiRAl2FLvefd
[8] https://www.youtube.com/watch?v=DYeE8Jd-H38
[9] https://correos.go.cr/correos-de-costa-rica-advierte-sobre-mensajes-fraudulentos-relacionados-con-la-entrega-de-paquetes/
[10] https://www.telediario.cr/nacional/ice-mensajes-falsos-pretenden-estafar-a-usuarios-foto
[11] https://www.telediario.cr/nacional/imas-alerta-de-estafas-cuales-son-los-mensajes-falsos

LY, S.A., que informe a esta Superintendencia, a través de la Dirección General de Calidad, el cumplimiento de la puesta en operación e implementación efectiva de la solución tecnológica de firewall adaptativo para el filtrado y bloqueo de mensajes SMS maliciosos, incluyendo la remisión de un informe técnico que detalle los avances, resultados obtenidos, y cualquier ajuste realizado posterior a su entrada en funcionamiento, así como la evidencia documental correspondiente que permita verificar la eficacia de dicha solución. (…)". -----

9. Que, en cumplimiento con lo anterior, **Liberty Telecomunicaciones de Costa Rica LY, S.A.** mediante el oficio LY-Reg0245-2025 del 26 de setiembre de 2025 (NI-12955-2025) informó sobre la implementación de mejoras tecnológicas en su infraestructura, apoyadas con Inteligencia Artificial, para la detección, prevención y bloqueo de mensajes SMS fraudulentos, las cuales se encuentran en operación desde octubre de 2025 y han contribuido en la disminución de intentos de *smishing* desde numeraciones asignadas a este operador. ----------

10. Que, no obstante, medios de comunicación como El Financiero, cuestionan los vacíos legales de la normativa vigente que facilitan a los delincuentes cometer crímenes mediante *smishing*, según la nota publicada el 26 de setiembre de 2025, denominada ***"Fraude por SMS: el vacío legal que facilita la estafa de millones en Costa Rica"***[12], de modo que, es indispensable que la SUTEL como ente regulador de las telecomunicaciones tome medidas para reducir el tráfico de mensajes SMS maliciosos que atentan contra la seguridad de los usuarios. ----------

[12] https://www.elfinancierocr.com/tecnologia/fraude-por-sms-el-vacio-legal-que-facilita-la/DS72V6UTBREWDH66DKER4XTXCM/story/

II. SOBRE EL *VISHING* (*PHISHING* MEDIANTE SERVICIOS DE VOZ) ---------

11. Que la empresa Cloudflare, líder en conectividad en la nube, define el *vishing*[13] como un tipo de ataque tipo *phishing* que tiene lugar a través de una llamada telefónica para engañar a usuarios con el fin de que compartan información confidencial o descarguen un *malware*, haciéndoles creer que la llamada proviene de una entidad de confianza, como la autoridad tributaria, su empleador, una compañía de la que hagan uso o una persona que conozcan. ----------

12. Que el *vishing* es una forma de ingeniería social, donde los atacantes pueden fingir ser un amigo en una emergencia y pedir a la víctima que les envíe dinero, o hacerse pasar por un miembro del departamento de TI de un empleador para conseguir el nombre de usuario y la contraseña de acceso a la red de la empresa. ----------

13. Que los atacantes de *vishing* suelen utilizar tácticas como elementos sorpresa para la víctima (llamadas inusuales), inducir sensación de urgencia o miedo, petición de información parcial o aprovechar acontecimientos actuales (por ejemplo, la pandemia de COVID-19). --------

14. Que de acuerdo con la noticia publicada el 27 de noviembre de 2025 por el medio Delfino.CR, denominada ***"Engaño telefónico expone datos en una reconocida universidad"***[14], la prestigiosa universidad de Harvard en Estados Unidos, el 18 de noviembre de 2025 sufrió un ataque de *vishing* que tuvo como consecuencia la filtración de datos personales de estudiantes, exalumnos y donantes, utilizando como vía de ataque una

[13] https://www.cloudflare.com/es-es/learning/email-security/what-is-vishing/
[14] https://delfino.cr/2025/11/engano-telefonico-expone-datos-en-una-reconocida-universidad

llamada telefónica, donde los cibercriminales engañaron a un funcionario del departamento de Relaciones con Exalumnos y Desarrollo Institucional (Alumni Affairs and Development) para que entregara voluntariamente sus credenciales de acceso, con las que pudieron ingresar al sistema. Según informa dicha noticia, los ciberdelincuentes realizan una investigación de la organización objetivo y recaban información de la persona que intentarán convertir en la puerta de acceso para que el engaño sea dirigido y a la medida, aumentando las probabilidades de éxito. ----------

15. Que el medio de comunicación NCR Noticias Costa Rica publicó en fecha 3 de julio de 2024 la nota "*¡Lo pueden EXTORSIONAR! Así funciona el vishing; nueva ESTAFA telefónica en la que utilizan IA*", donde informó sobre el uso de aplicaciones de inteligencia artificial que replican cualquier voz para cometer estafas de tipo *vishing*, destacando el aumento en la sofisticación en los sistemas de fraude y la necesidad urgente de implementar tecnologías de reconocimiento de voz basadas en inteligencia artificial para detectar y prevenir anomalías. ----------

16. Que otro mecanismo que utilizan los ciberdelincuentes para cometer ataques de *vishing* es el enmascaramiento de llamadas, el cual consiste en ocultar el número telefónico real de llamante, mostrando en su lugar otro número telefónico para simular una llamada de una institución o empresa. Este tipo de ataque es abordado en la resolución RCS-294-2023 *"METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DEL ENMASCARAMIENTO DE LLAMADAS"*, donde se requirió a todos los operadores de telefonía con numeración asignada por esta

Superintendencia, aplicar el bloqueo generalizado de llamadas internacionales entrantes cuyo número de origen sea enmascarado con prefijos nacionales o similares. ----------

III. MENSAJES SMS P2P Y A2P

17. Que los mensajes SMS *P2P* (Persona a Persona) corresponden al intercambio básico de mensajes de texto SMS entre dos personas a través de la red móvil. Se caracterizan por ser conversaciones privadas entre usuarios sin fines comerciales, es decir, comunicación de dos humanos mediante mensajes de texto, además, utilizan el formato de numeración establecido en el Plan Nacional de Numeración. Estos mensajes son enviados desde el terminal móvil de un usuario y enrutados directamente al usuario destino, garantizando la privacidad de la información. ----------

18. Que, por otra parte, los mensajes SMS *A2P* (Aplicación a Persona) son mensajes generados por un software empresarial o aplicación, hacia un usuario móvil. Los mensajes *A2P* permiten a las empresas automatizar el envío de grandes volúmenes de mensajes con fines informativos y transaccionales. Estos mensajes pueden ser de marketing, alertas de emergencia, recordatorios de citas, mensajes automatizados mediante *chatbots* y autenticación de dos factores (2FA) con contraseñas de un solo uso (OTP). Además, suelen ser enviados desde números telefónicos que no están incluidos en el Plan Nacional de Numeración, o son de tipo alfanumérico. ----------

19. Que de modo que, una empresa utiliza un software o aplicación para automatizar el proceso de escritura y envío de los mensajes, esto permite enviar mensajes a un gran número de personas de forma rápida y eficiente.

A diferencia del tráfico de mensajes *P2P* que ha venido disminuyendo con los años, el uso de mensajes *A2P* ha aumentado debido a la posibilidad de maximizar el alcance de usuarios en menos tiempo y la facilidad de integración con aplicaciones de tipo OTT (*Over The Top*)[15]. ----------

20. Que los mensajes A2P pueden ser de tipo doméstico, donde una empresa local envía los mensajes a usuarios dentro del mismo país, o de tipo internacional cuando los mensajes A2P son generados por un software o aplicación ubicada en un país distinto al de los usuarios receptores. Los mensajes A2P internacionales suelen ser más costosos debido a las tarifas de interconexión entre operadores de diferentes países y los precios de entrega de mensajes fuera de las fronteras territoriales. ----------

21. Que, ciberdelincuentes se aprovechan de los mensajes A2P para cometer ataques de *smishing* o de "*SMS pumping*", también llamado inundación de SMS, el cual es un tipo de fraude donde los atacantes envían un gran volumen de mensajes SMS no solicitados al número de teléfono de una víctima para saturarlo, o utilizan números de tarifa premium para inundar una empresa con mensajes que le harán acumular cargos sustanciales, de los que la empresa será responsable, este último también conocido como tráfico inflado artificialmente (AIT). ----------

22. Que, para llegar a usuarios en otro país, los remitentes de mensajería A2P internacional, contratan un agregador de SMS, que corresponde a una empresa con acuerdos con varios operadores móviles para la entrega de mensajes SMS en diferentes países. Para la distribución de los mensajes A2P, se utilizan rutas conocidas como *"rutas blancas"*, que corresponden a

[15] Aplicaciones y plataformas que distribuyen contenido multimedia (video, audio, voz) directamente a los usuarios a través de internet, sin la necesidad de proveedores de servicios de telecomunicaciones.

canales de mensajería autorizados y oficiales para tráfico de mensajes SMS, según acuerdos pactados entre agregadores, operadores y proveedores a nivel internacional. ----------

23. Que, no obstante, también existen las llamadas *"rutas grises"*, que corresponden a canales no oficiales ni autorizados, usualmente utilizados por proveedores que no están directamente conectados a la red del operador mediante un acuerdo formal y donde no es posible garantizar la trazabilidad de los mensajes de extremo a extremo. El uso de estas rutas es motivado por las bajas tarifas que aplican a cada mensaje A2P enviado, sin embargo, esto es debido a que carecen de fiabilidad en la entrega exitosa de los mensajes e incumplen normas de seguridad y protección de datos, de modo que, el uso de rutas grises sacrifica la confiabilidad e integridad de los mensajes A2P a cambio de un bajo coste en la entrega del mensaje. Esto pone en riesgo la seguridad de los usuarios considerando que los mensajes de autenticación de dos factores (2FA) con contraseñas de un solo uso (OTP) transitan en las redes como tráfico A2P. En la siguiente imagen se muestra la arquitectura de estas rutas: ----------

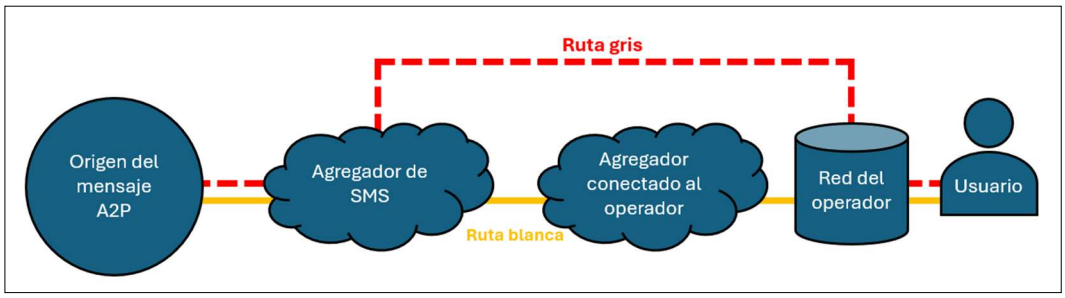

Imagen 1. Arquitectura de tráfico de mensajes SMS A2P.

24. Que, además, se ha detectado que operadores nacionales[16] utilizan rutas de interconexión local con otros operadores para enviar tráfico SMS internacional, enmascarando el número internacional con un número local. Por otra parte, los operadores deben disponer de firewalls con capacidad de identificar el tipo de tráfico recibido y bloquear todo el tráfico internacional que intente ingresar por rutas de interconexión local, enmascarando el número de origen, garantizando que los remitentes utilicen rutas blancas oficiales. ----------

25. Que de acuerdo con el desarrollador de plataformas de comunicación en la nube Infobip[17], existen tres tipos de rutas grises: ----------

- Telecom a Telecom: un operador aprovecha los acuerdos de interconexión con otro operador para enviar tráfico A2P enmascarado como P2P y así monetizar el tráfico A2P, haciendo creer al otro operador que recibe tráfico P2P que cuenta con una tarifa más baja o nula. ----------
- Agregadores A2P: uso de otros agregadores A2P con tarifas mucho más bajas a las establecidas con un operador en un acuerdo formal.
- SimBoxes: son dispositivos que utilizan una gran cantidad de tarjetas SIM de servicios tipo P2P con el objetivo de finalizar el tráfico A2P. Mediante un software recibe el tráfico A2P y lo reenvía por los servicios P2P de cada tarjeta SIM, aprovechando las tarifas más económicas de los servicios P2P o planes ilimitados. ----------

[16] Entiéndase operador local como un operador o proveedor que brinda servicios dentro del territorio nacional y está sujeto a la regulación establecida por esta Superintendencia.
[17] https://www.infobip.com/glossary/what-is-an-sms-gray-route

26. Que, los operadores locales pueden identificar el tráfico de mensajes A2P internacionales por la ruta de ingreso internacional en sus redes y el protocolo utilizado, el cual suele ser SMPP (*Short Message Peer-to-Peer*) o APIs (*Application Programming Interface*) basadas en el protocolo HTTP (*Hypertext Transfer Protocol*). Además, el volumen de mensajes A2P remitidos por una aplicación es mucho mayor que el P2P, dado que, en el tiempo que le toma a un usuario escribir un mensaje, una aplicación pudo haber enviado miles de mensajes a usuarios distintos, y con este comportamiento identificar el tráfico A2P. ----------

27. Que la validación del Título Global, en adelante GT (Global Title) y el análisis de sus patrones permite identificar comunicaciones sospechosas en la red. Los GT son direcciones únicas que identifican la red de origen y destino, además de la ubicación específica de un terminal en dichas redes, ya que, incluyen información de origen y destino sobre código de país, identificador de red, identificador de aplicación o servicio y tipo de enrutamiento[18]. -------

28. Que el Foro de Ecosistema Móvil, en adelante MEF (Mobile Ecosystem Forum) recomienda el uso de registros de identificación de remitentes autorizados para enviar tráfico A2P por las rutas definidas, donde se bloquee el tráfico de los remitentes no registrados[19], destacando los casos de éxito en Reino Unido, Irlanda y España con la implementación de un registro de remitentes de mensajes A2P autorizados. ----------

29. Que el estándar ETSI TR 103 421 *"Network Gateway Cyber Defence"*, el cual se amplía más adelante, señala la importancia de la validación de rutas legitimas por parte de los operadores, cooperando entre ellos con la

[18] https://www.infobip.com/glossary/global-title
[19] https://mobileecosystemforum.com/sms-senderid-protection-registry/

aplicación de especificaciones y la firma de acuerdos de servicio que exigen que el tráfico cumpla con los requisitos mínimos pactados, enfatizando la defensa y seguridad en los puntos de interconexión, de modo que, el tráfico malicioso debe ser interceptado antes de entrar en el núcleo de la red del operador. Dicho estándar, también menciona la importancia de mecanismos para inspeccionar el contenido de los mensajes con el fin de identificar amenazas, lo cual se logra con técnicas como Inspección Profunda de Paquetes (DPI) [20], además, afirma que los firewalls en las redes de los operadores deben poder identificar amenazas y prevenir la conexión de dispositivos que ataquen las redes de telecomunicaciones. ----------

30. Que editoriales como ScienceDirect, recomiendan el uso de herramientas basadas en Machine Learning (aprendizaje automático con Inteligencia Artificial) para combatir el smishing[21]. ----------

31. Que, según la recomendación ITU-T X.1245 de la Unión Internacional de Telecomunicaciones que se amplía más adelante, otro mecanismo para la lucha contra el smishing es el uso de sistemas de reputación de la fuente del mensaje para bloquear tráfico malicioso, así como, el uso de conexiones fiables y seguras entre los dominios de seguridad antispam de los operadores. ----------

32. Que basado en lo anterior, los operadores pueden aplicar las siguientes medidas para contrarrestar el tráfico de SMS A2P maliciosos: ----------

- Establecer registros de entidades desde las cuales se recibe tráfico de SMS A2P. ----------

[20] Técnica avanzada de seguridad de red que examina desde el encabezado del paquete hasta la carga útil (payload) de los datos en tiempo real para identificar malware y filtrar contenido. Analiza archivos y paquetes para buscar firmas específicas de virus, spam o palabras clave con el objetivo de identifica tráfico malicioso y bloquear amenazas.
[21] https://www.sciencedirect.com/science/article/pii/S1877050925009834

- Validación de rutas legitimas, de manera que los operadores garanticen que las rutas mediante las cuales transita el tráfico A2P es a través de un proveedor autorizado que cuenta con acuerdos de interconexión con el operador local y los mensajes recibidos especifican correctamente los atributos de identificación del remitente, según dichos acuerdos. ----------
- Sistemas de firewall de SMS apoyados con Inteligencia Artificial con capacidad de realizar Inspección Profunda de Paquetes (DPI) en busca de enlaces maliciosos o reconociendo patrones y comportamientos repetitivos en los mensajes, ya que un mismo mensaje es enviado a múltiples usuarios. Además, estos sistemas deben ser capaces de revisar y analizar SMS binarios y de otros formatos técnicos de codificación aplicables que puedan utilizarse para instalar malware u otras amenazas a los dispositivos de los usuarios finales. ----------
- Uso de sistemas de reputación de enlaces para bloquear mensajes que contengan enlaces a sitios maliciosos o de dudosa procedencia.
- Uso de herramientas automatizadas para la detección de mensajes de smishing donde se suplanta la identidad de una entidad o persona, e identificación de tráfico inflado artificialmente (AIT) originado por generadores de SMS o SimBoxes. ----------

33. Que, por lo anterior, es necesario que los operadores implementen en sus redes herramientas automatizadas de filtrado que identifiquen el contenido malicioso en los mensajes de texto, como sistemas de firewalls con capacidad de identificar y procesar el tráfico A2P, para que la totalidad de

este sea bloqueado cuando proviene de rutas grises o corresponde a tráfico malicioso, de modo que, se garantice el tráfico A2P únicamente por las rutas autorizadas entre agregadores, operadores y proveedores, según los acuerdos de interconexión establecidos, así como, implementar los elementos de seguridad necesarios para proteger la información y privacidad de los usuarios finales ante los ataques que se dan mediante los mensajes A2P. ----------

IV. SOBRE LA COMPETENCIA DE SUTEL. ----------

1. Que, mediante la Ley No. 7593: "*Ley de la Autoridad Reguladora de los Servicios Públicos*" (en adelante Aresep), a partir del capítulo XI y específicamente el artículo 59, se desarrolla lo referente a la Superintendencia de Telecomunicaciones (SUTEL). Bajo esa línea, el legislador dispuso que le corresponde a la SUTEL: regular, aplicar, vigilar y controlar, el ordenamiento jurídico de las telecomunicaciones, siendo un órgano de desconcentración máxima adscrito a la Aresep, el cual es independiente de todo operador y está supeditado a la normativa que aplica al sector de telecomunicaciones, al Plan Nacional de Desarrollo de las Telecomunicaciones y a las políticas del sector.

2. Que, además, se le otorgó una serie de obligaciones a la Superintendencia, las cuales fueron desarrolladas en el artículo 60 de la *ibid*, que -entre otras- podemos citar: aplicación del ordenamiento jurídico de las telecomunicaciones, garantizar y proteger los derechos de los usuarios de las telecomunicaciones, velar por el cumplimiento de los deberes y derechos de los operadores de servicios de telecomunicaciones, asegurar el cumplimiento de las obligaciones de acceso e interconexión que se impongan a los operadores de redes de telecomunicaciones, controlar y comprobar el uso

eficiente del recurso número, conocer y sancionar las infracciones administrativas en que incurran los operadores y proveedores de servicios de telecomunicaciones. ----------

3. Que, mediante la Ley 8642: Ley General de Telecomunicaciones, se determina la necesidad de garantizar el derecho de los habitantes a obtener servicios de telecomunicaciones, asegurar la aplicación de los principios de universalidad y solidaridad de servicio de telecomunicaciones, proteger los derechos de los usuarios de los servicios de telecomunicaciones, asegurando la eficiencia, igualdad, continuidad, calidad, mayor y mejor cobertura, más y mejores alternativas, garantizar la privacidad y confidencialidad en las comunicaciones, entre muchos otros. ----------

4. Que es claro que la SUTEL ostenta la competencia, no solo para conocer las reclamaciones cuando los derechos de los usuarios del servicio de telecomunicaciones se encuentren vulnerados, sino, garantizar tales derechos a los usuarios velando por el cumplimiento de la normativa técnica y legal aplicable a los operadores y proveedores de telecomunicaciones. ----------

5. Que, el Plan Nacional de Numeración establece las disposiciones para la asignación de numeración a los servicios de telecomunicaciones, con el fin de asegurar en forma objetiva, proporcional, oportuna, transparente, eficiente y no discriminatoria, el acceso a los recursos numéricos asociados con la operación de redes y la prestación de servicios de telecomunicaciones. Esto permite una adecuada selección, identificación e interoperabilidad de los servicios, facilita la interconexión de las redes, y garantiza el efectivo ejercicio de los derechos de los usuarios finales, conforme con lo establecido en la Ley General de Telecomunicaciones, Ley 8642 y sus reformas. ----------

6. Que, según las competencias que ha otorgado el legislador a esta Superintendencia, éstas giran en torno a la protección de los derechos a los usuarios finales en su interacción con los operadores o proveedores de los servicios de telecomunicaciones, la calidad del servicio, promoción y competencia del sector de las telecomunicaciones, la interconexión de redes, interoperabilidad de los servicios y control del recurso numérico, entre otras. Por ende, en apego al artículo 2 inciso f) de la Ley 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 ciudadana, 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. ----------

V. NORMATIVA APLICABLE.

1. Que, un mundo en constante crecimiento tecnológico y la globalización constante produce un crecimiento de herramientas que, bajo diferentes estructuras tecnológicas, son utilizadas para fines ilícitos. Esto pone en peligro a la ciudadanía en tanto surgen delitos en contra de su esfera económica, personal y confidencial por el uso indebido de sus datos personales para ser utilizadas en suplantaciones de identidad y por ende en la consecución de delitos. ----------

2. Que las Naciones Unidas, mediante el Manual sobre los delitos relacionados con la identidad, destaca que a consecuencia de la digitalización y globalización de los servicios basados en redes; *"han promovido el aumento del uso de información relacionada con la identidad. La mayoría de las empresas, así como las*

transacciones federales, dependen del tratamiento de datos electrónicos mediante sistemas automatizados. El acceso a la información relacionada con la identidad permite a los delincuentes intervenir en muchos ámbitos de la vida social. Por otra parte, esa información, además de procesarse, generalmente se almacena en bases de datos, que son por ese motivo un blanco potencial para los delincuentes."[22] Además, en cuanto a las nuevas metodologías para obtener información ante la digitalización, el mismo documento agrega que: "*Resulta extremadamente difícil describir el hurto de identidad definiendo los métodos utilizados para cometer el delito. Varios métodos diferentes corresponden al concepto de "hurto de identidad", que abarcan desde el clásico hurto de correspondencia hasta sofisticadas operaciones de peska (phishing)."*[23]. ----------

3. Que, a través de la Ley 8969 Ley de Protección de la Persona frente al tratamiento de sus datos personales del 07 de julio del 2011 y su reglamento (Decreto 37554-JP) se ha realizado un esfuerzo en aras de regular y resguardar las bases de datos que contengan información de cualquier persona, regulando el derecho de la autodeterminación y tratamiento de los datos en relación con su vida, actividad privada, personalidad, entre otros. --

4. Que a partir de los años 2012 y 2013; mediante la Ley 9048 y Ley 9135 respectivamente, se introduce una importante reforma al Código Penal, la cual incorpora los delitos informáticos y conexos, así como la tipificación ante la violación de las comunicaciones, datos personales, suplantación de identidad, entre otros. Aunado a esto, a partir del 03 de julio del 2017, Costa Rica se adhiere al Convenio de Europa sobre Ciberdelincuencia (Budapest 2011) mismo que reconoce la necesidad de aplicar, con carácter prioritario,

[22] Manual sobre los delitos relacionados con la identidad de la oficina de las Naciones Unidas contra la Droga y el Delito; 2013. Página 14. *Consecuencias de la digitalización.*
[23] ibid. Nuevos métodos derivados de la digitalización para obtener información. Página 18

una política penal común destinada a proteger a la sociedad frente a la ciberdelincuencia. Reconociéndose, -además-, la necesidad de una cooperación con el sector privado 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. ----------

5. Que el dictamen C-041-96 del 11 de marzo de 1996, la Procuraduría General de la República indicó: *"El operador jurídico puede concluir en la existencia de una derogación tácita o implícita cuando el análisis comparativo de la ley anterior y de la posterior revela una antinomia normativa, que torne incompatibles las normas e impida una armonización del régimen jurídico establecido, o bien cuando en virtud de la aprobación de la nueva ley se produzca una dualidad de la regulación de determinados aspectos, aun cuando no exista una verdadera oposición entre la norma primigenia y la segunda (…)".* --

6. Que, parte de los compromisos adquiridos en el citado convenio con Europa, son la implementación de las medidas legislativas y de otro tipo, que sean necesarias para tipificar el delito de actos como: el acceso ilícito a un sistema informático, interceptación ilícita de datos informáticos, abuso de dispositivos, incluidos programas informáticos que permitan la comisión de ilícitos, y acceder a contraseñas códigos de acceso, sistemas o datos informáticos similares. ----------

7. Que el tema de la ciberdelincuencia y seguridad informática atañe a un tema de las telecomunicaciones, y encaja en la problemática hoy plateada por las autoridades judiciales. La misma Procuraduría General de la República, mediante la opinión jurídica PGR-OJ-184-2021 del 24 de noviembre del 2021

denotó: *"El tema de la ciberdelincuencia y la seguridad informática va paralelo a todo lo que atañe a las telecomunicaciones; en tal sentido, nuestro país se sumó también a estos esfuerzos internacionales y aprobó, mediante ley N° 9452 de 26 de mayo de 2017, la Convención de Europa sobre Ciberdelincuencia, como estrategia para lograr el mejoramiento de las técnicas de investigación e incrementar la cooperación internacional entre los Estados, para combatir la amenaza de los ciberdelitos. Costa Rica tiene probablemente la mejor legislación sobre delitos informáticos en América Latina, y ha dado un paso fundamental mediante la aprobación del único instrumento internacional existente que facilita la recolección de evidencia electrónica, la investigación contra el ciber-lavado de dinero, protección integral de la niñez y otros crímenes serios, donde se dé la utilización torcida de las telecomunicaciones. Como ejemplo crítico, sólo en Europa los efectos de la ciberdelincuencia pueden llegar a los 5.000 millones de euros cada año en pérdidas para los* países". ----------

8. Que, la Constitución Política en su numeral 46 establece entre otras cosas lo siguiente: *"Los consumidores y usuarios tienen derecho a la protección de su salud, ambiente, seguridad e intereses económicos; a recibir información adecuada y veraz; a la libertad de elección, y a un trato equitativo. El Estado apoyará los organismos que ellos constituyan para la defensa de sus derechos. La ley regulará esas materias*". ----------

9. Que, el artículo 42 de la Ley General de Telecomunicaciones 8642 regula la privacidad de las comunicaciones y de datos personales y establece que: *"Los operadores y proveedores deberán adoptar las medidas técnicas y administrativas idóneas para garantizar la seguridad de las redes y sus servicios. En caso de que el operador conozca un riesgo identificable en la seguridad de la red, deberá informar a la Sutel y a los usuarios finales sobre dicho riesgo"*. ----------

10. Que se puede afirmar que, la Ley 8642 es conteste con lo desarrollado en la

Ley 7593, siendo que resulta de vital importancia la protección de los derechos de los usuarios finales, pero además, esta Ley aboga por que exista un desarrollo de las telecomunicaciones que contribuya con la seguridad ciudadana, siendo el fraude mediante llamadas enmascaradas una problemática social que requiere de una atención preferente, desde un panorama integral, lo cual justifica que el legislador decidiera incorporarlo en un área como las telecomunicaciones. Bajo esa línea, es de rescatar que el régimen de protección a la intimidad y los derechos del usuario de las telecomunicaciones, desarrollado desde el capítulo II de la Ley General de Telecomunicaciones, a través del artículo 42, determina una obligación a los operadores de garantizar el secreto de la comunicación, el derecho a la intimidad y la protección de los datos de los abonados y usuarios finales, aplicando sistemas y medidas técnicas y administrativas necesarias para garantizar las redes y sus servicios. Al mismo tiempo, el artículo 45 de la Ley 8642 dispone los derechos de los usuarios finales de servicios de telecomunicaciones; al respecto, e importante indicar que este artículo es *numerus apertus* según lo establecido en el inciso 29) que señala que se incluye como derechos los demás establecidos en el ordenamiento jurídico.

11. Que el artículo 106 del Reglamento sobre el Régimen de Protección al Usuario Final dispone como prácticas prohibidas por parte de los usuarios finales, en lo que interesa, las siguientes: ----------

*"**Artículo 106. Prácticas prohibidas por parte de los usuarios finales**. ----------*

Se prohíbe a los usuarios finales realizar cualquiera de las siguientes prácticas prohibidas, según lo dispuesto en el presente Reglamento. ----------

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." ---

12. Que el artículo 5 incisos 7) y 8) del *Reglamento sobre el Régimen de Protección al Usuario Final* 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 (…)".* ----------

13. Que, en la misma línea el artículo 11 inciso 29) del citado reglamento, establece como parte de los deberes de los operadores/proveedores de servicios: *"**29)** Abstenerse de incurrir en prácticas prohibidas".* ----------

14. Que el numeral 47 inciso 4) del Reglamento sobre el Régimen de Protección al Usuario Final dispone que los contratos de servicios de telecomunicaciones se extinguirán cuando se compruebe la comisión de prácticas prohibidas. ----------

15. Que el artículo 75 del reglamento de cita establece lo siguiente "***Artículo 75. Suspensión del servicio prepago móvil*** *(…) La suspensión del servicio prepago móvil aplicará, además, en aquellos casos que el usuario no se encuentre debidamente registrado*

en la plataforma del Registro Prepago o incurra en prácticas prohibidas".

16. Que, en aras de procurar la protección de los derechos de los usuarios, la SUTEL tiene la competencia para establecer mecanismos que busquen el control de fraudes, tal y como dispone el artículo 107 del *Reglamento sobre el Régimen de Protección al Usuario Final* dispone como prácticas prohibidas por parte de los operadores/proveedores, en lo que interesa, las siguientes:

*"**Artículo 107. Prácticas prohibidas por parte de los operadores/proveedores.** -- Se prohíbe a los operadores/proveedores realizar cualquiera de las siguientes prácticas prohibidas, que atente contra los derechos de los usuarios finales, según lo dispuesto en el presente Reglamento. ----------*

(…) ----------

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. ----------

(…) ----------

4. Acciones que, en relación con la prestación del servicio de telecomunicaciones, sean catalogadas como dañinas para la salud de las personas o que supongan un riesgo para la seguridad, privacidad o el ambiente. ----------

5. Subscripción o activación irregular, automática, engañosa o sin contar con la autorización o consentimiento expreso del titular del servicio. ----------

(…) El incumplimiento de las citas prácticas, se considera una violación a los derechos de los usuarios finales". ----------

17. Que el Plan Nacional de Numeración, Decreto Ejecutivo 40943-MICITT establece las disposiciones para la asignación de numeración de los servicios de telecomunicaciones, con el fin de asegurar en forma objetiva, proporcional, oportuna, transparente, eficiente y no discriminatoria, el acceso a los recursos numéricos asociados con la operación de redes y la prestación de servicios de telecomunicaciones en nuestro país. Asimismo, sí bien dicha normativa no establece diferenciaciones respecto a la mensajería de texto SMS en sus modalidades P2P y A2P, es necesario, ante la evidencia en el aumento de actividades ilícitas que se han realizan, establecer disposiciones regulatorias específicas para éstas. ----------

18. Que el artículo 64 del Reglamento de Acceso e Interconexión de Redes de Telecomunicaciones establece que los operadores o proveedores de servicios de telecomunicaciones deberán utilizar los métodos de prevención, detección, control y monitoreo, así como sistemas que permitan la detección inmediata de fraudes o usos no autorizados de la red, de acuerdo con las mejores prácticas internacionales para asegurar que no se haga uso incorrecto de sus respectivas redes de telecomunicaciones. ----------

19. Que mediante el Decreto Ejecutivo 35205-MINAE, se determinó vía reglamentaria, las medidas de protección de la privacidad de las comunicaciones, con el fin –entre otros- de garantizar el secreto de las comunicaciones, el derecho a la intimidad y protección de los datos de carácter personal de los abonados y usuarios. Así mismo, la sección III de ese cuerpo normativo dispone lo relativo a la identificación de llamadas, y en donde para el particular se resalta lo establecido en el artículo 20: *"(…) Filtrado en destino de llamadas sin identificación. Cuando los proveedores que presten el servicio de*

identificación de la línea de origen y ésta se presente con anterioridad a que se establezca la llamada, deberán ofrecer a cualquier abonado que recibe la llamada, la posibilidad mediante un procedimiento sencillo, de rechazar las llamadas procedentes de usuarios o abonados que hayan impedido la visualización de la identificación de la línea de origen.". --

20. Que el Plan Nacional de Desarrollo de las Telecomunicaciones 2022-2027; en aras de impulsar el desarrollo del sector de la Ciencia, Innovación, Tecnología, Telecomunicaciones y Gobernanza Digital, establece como una de sus estrategias y su vinculación con otras políticas públicas, estrategias y planes; la Ciberseguridad en Costa Rica; destacando lo siguiente: *"3.3.3.3. Estrategia Nacional de Ciberseguridad Costa Rica… La estrategia en materia de ciberseguridad data de 2017 y procura la búsqueda de acciones conducentes al aseguramiento de datos y la protección en línea en diferentes aspectos, considera la persona como prioridad, el respeto a los derechos humanos y la privacidad, la coordinación con múltiples partes interesadas y la cooperación internacional (MICITT, 2017a). …Como parte del marco de acción, se consideran otros instrumentos de planificación, entre los que destacamos el papel del PNDT como impulsor también, a la par de esta Estrategia, de una seguridad cibernética en diferentes sectores. … Por lo tanto, lo delineado en la Estrategia a nivel detallado, se considera como un punto de partida para el PNDT en materia de seguridad cibernética y los retos que esto representa para las diferentes poblaciones, desde las infraestructuras críticas, los servicios en línea, servicios financieros, las MIPYMES, las poblaciones en condición de vulnerabilidad, entre otros, para las que se debe considerar transversalmente el tema en los ejes de la planificación sectorial con visión al 2027." --------*

VI. SOBRE EL ANÁLISIS DE LAS OPOSICIONES PRESENTADAS EN CONSULTA A LA PROPUESTA DE LA REGULATORIA

1. Que por medio del oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026, las Direcciones Generales de Calidad y Mercados presentaron al Consejo de la SUTEL el "*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)*" ----------
2. Que sobre el análisis de oposiciones realizado por las Direcciones General de Calidad y de Mercados se acoge en su totalidad por el Consejo de la SUTEL el oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026, como de seguido se dispone. ----------

POR TANTO

Con fundamento en la Ley General de Telecomunicaciones, Ley 8642 y su reglamento; Ley de la Autoridad Reguladora de los Servicios Públicos, Ley 7593; Ley General de la Administración Pública, Ley 6227, Reglamento sobre el Régimen de Protección al Usuario Final y demás normativa de general y pertinente aplicación, vistos los citados antecedentes y fundamentos jurídicos. ----------

EL CONSEJO DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES, RESUELVE:

I. **DAR POR RECIBIDO Y ACOGER** el 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)" ----------

II. **SOBRE LAS OPOSICIONES PLANTEADAS POR CALLMYWAY NY S.A. (CALL MY WAY)**, de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) Acoger la observación planteada por 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. ----------

b) 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. ----------

c) **Acoger** la observación 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. ----------

d) **Acoger** la observación respecto a ampliar el plazo según las fases de implementación gradual. ----------

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

III. **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 y conformidad con los fundamentos señalados

mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados. ----------

IV. **SOBRE LAS OPOSICIONES PLANTEADAS POR CLARO CR TELECOMUNICACIONES S.A. (CLARO)**, de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) **Acoger parcialmente** la observación 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. ----------

b) **Acoger** la propuesta 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 únicamente para mensajes A2P. ----------

c) **Acoger** la observación respecto a excluir el tráfico multimedia IP de las obligaciones contenidas en esta propuesta regulatoria. ----------

d) **Acoger de forma complementaria** la propuesta sobre permitir a los operadores el registro y validación de plantillas para mensajes A2P. ----------

e) **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. ----------

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

g) Acoger la observación respecto a incorporar en la fase 2 del cronograma el intercambio de información entre operadores y proveedores. ----------

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

V. **SOBRE LAS OPOSICIONES PLANTEADAS POR EL INSTITUTO COSTARRICENSE DE ELECTRICIDAD (EL ICE)** de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) **Acoger** la observación planteada respecto a ampliar el plazo de implementación. ----------

b) **Acoger parcialmente** la solicitud planteada respecto de emitir la presente propuesta regulatoria como una nueva regulación complementaria a la

dispuesta en la resolución RCS-294-2023. ----------

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

VI. **SOBRE LAS OPOSICIONES PLANTEADAS POR LIBERTY TELECOMUNICACIONES DE COSTA RICA LY, S.A. (LIBERTY)** de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) **Acoger** la observación respecto a ampliar el plazo de implementación. -------

b) **Acoger** la propuesta 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. ----------

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

VII. **SOBRE LAS OPOSICIONES PLANTEADAS POR EL MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES (MICITT)** de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) **Acoger** la observación planteada 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. ----------

b) **Acoger** la observación respecto a ampliar el plazo de implementación de las presentes disposiciones regulatorias. ----------

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

VIII. **SOBRE LAS OPOSICIONES PLANTEADAS POR LA CÁMARA DE INFOCOMUNICACIÓN Y TECNOLOGÍA (INFOCOM)** de conformidad con los fundamentos señalados mediante oficio número 05772-SUTEL-DGM-2026 del 12 de junio de 2026 de las Direcciones General de Calidad y Mercados, se dispone: ----------

a) **Acoger** la observación respecto a ampliar el plazo de implementación. -------

b) **Acoger** la observación respecto a emitir la presente propuesta regulatoria como una nueva regulación complementaria a la dispuesta en la resolución RCS-294-2023. ----------

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

IX. **RECHAZAR** en su totalidad las observaciones presentadas por **MILLICOM CABLE COSTA RICA, S.A. (TIGO)** por haber sido presentadas de forma extemporánea. ----------

X. **ESTABLECER LA IMPLEMENTACIÓN DE MEDIDAS REGULATORIAS CON EL FIN DE MINIMIZAR EL IMPACTO DE CIBERATAQUES MEDIANTE MENSAJES DE TEXTO SMS (SMISHING) Y LLAMADAS (VISHING)**, en los siguientes términos: ----------

1. SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P. ----------

Estas medidas aplican para la totalidad de operadores y proveedores de servicios de telecomunicaciones que brindan servicios de mensajería SMS, sea en modalidad P2P o A2P: ----------

A. Los operadores y proveedores son responsables de la seguridad de sus propias redes de telecomunicaciones y de verificar el tráfico que por ellas transita, además de, garantizar la seguridad de sus usuarios finales con los que mantienen relaciones comerciales mediante la suscripción de contratos de servicio, por lo que, los operadores y proveedores deben implementar mecanismos técnicos y administrativos para asegurar la trazabilidad del tráfico de mensajes SMS desde el origen y hasta el destino, bloqueando todo tráfico identificado como malicioso, no trazable o aquel que intente evadir filtros de seguridad, como mensajes con origen internacional que simulan ser local. Dicha relación comercial le brinda al operador o proveedor la potestad de inspeccionar y revisar la totalidad del tráfico de mensajes SMS que recibe en su red por rutas de interconexión internacional o local para garantizar la seguridad de sus usuarios finales. ----------

B. Los operadores y proveedores deben garantizar que el remitente del contenido SMS o el agregador de SMS utiliza y especifica atributos de identificación para los SMS enviados, de modo que permitan la identificación del remitente real como nombre alfanumérico del remitente, número específico, origen de la comunicación o red móvil desde la que se inició el mensaje SMS, así como otros atributos acordados entre las partes. Por lo que, los operadores y proveedores solo enviarán a los destinatarios o

reenviarán a otras redes fijas o móviles de otros operadores, los mensajes SMS que cumplan con los atributos de identificación coordinados entre operadores o proveedores, bloqueando todo el tráfico de mensajes SMS que no especifique atributos de identificación que permitan conocer el origen de la comunicación. ----------

C. Los operadores y proveedores 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) [24] en todos los mensajes SMS, con el único objetivo de buscar enlaces maliciosos o reconociendo patrones y comportamientos que identifiquen dichos mensajes como maliciosos. Estos sistemas deber ser capaces de revisar y analizar SMS binarios[25] y de cualquier otro formato técnico de codificación aplicable a los servicios de mensajería móvil que puedan utilizarse para instalar malwares u otras amenazas en los dispositivos de los usuarios finales. Además, deben disponer de herramientas automatizadas que identifiquen y bloqueen los mensajes maliciosos de tipo *smishing* y detecten el tráfico inflado artificialmente (AIT) originado por generadores de SMS o *SimBoxes*, además del tráfico internacional, 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. Las

[24] Técnica avanzada de seguridad de red que examina desde el encabezado del paquete hasta la carga útil (payload) de los datos en tiempo real para identificar malware y filtrar contenido. Analiza archivos y paquetes para buscar firmas específicas de virus, spam o palabras clave con el objetivo de identifica tráfico malicioso y bloquear amenazas.
[25] Mensajes de texto codificados en secuencias de bits (0 y 1) que permiten enviar datos, imágenes, audio o configuraciones, en lugar de limitarse a solo texto.

características mínimas de los firewalls de seguridad que deben cumplir los operadores son: ----------

1. Capacidad de identificar tráfico de tipo P2P o A2P que ingresa a la red del operador por rutas de interconexión internacional o local. ----------
2. 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. ----------
3. Capacidad de analizar el contenido completo de los mensajes mediante Inspección Profunda de Paquetes (DPI) para detectar manipulación de protocolos, enlaces maliciosos, malwares u otras amenazas, reconociendo patrones y comportamientos como cantidad similar de caracteres en múltiples mensajes SMS, que identifiquen dichos mensajes como maliciosos. ----------
4. Validación del Título Global (GT, Global Title) y verificación en tiempo real del origen del mensaje. ----------
5. Contar con mecanismos de geolocalización y densidad de señal para identificar dispositivos dañinos conectados en la red, que envían tráfico masivo como SimBoxes o cualquier otro equipo que enmascare o simule tráfico A2P como P2P. ----------
6. Uso de Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP)[26] para detectar variaciones en la ortografía del mensaje o el uso de caracteres especiales para evadir filtros. Además, realizar Análisis

[26] Uso de la Inteligencia Artificial para que las computadoras puedan entender, interpretar, manipular y generar lenguaje humano, tanto en texto como en voz.

Heurístico[27] con el fin de detectar malwares o cualquier otra amenaza contenida en el mensaje. ----------

7. Capacidad de identificar en el contenido de los mensajes SMS P2P y A2P enlaces maliciosos (completos o comodines) que lleven a los usuarios finales a sitios WEB fraudulentos o generen la descarga de malwares. ---

8. Uso de sistemas de reputación y conexión en tiempo real con al menos una base de datos global que permita determinar que un enlace contenido en un mensaje es malicioso. ----------

9. 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 malwares u otras amenazas en los dispositivos de los usuarios finales. --

10. Detección y bloqueo automático de números telefónicos o entidades que en un periodo de tiempo superen umbrales de tasa y volumen de mensajes no correspondientes a un comportamiento humano. Es decir, que la cantidad de mensajes enviados por segundo/minuto/hora es superior a la alcanzable por un humano (Rate Limiting)[28]. ----------

11. Identificación de campañas de smishing mediante: ----------

(a) Detección de un numero idéntico o similar de caracteres contenidos en mensajes SMS consecutivos. ----------

[27] Método de detección de virus mediante el cual se examina el código en busca de propiedades sospechosas. Detecta características sospechosas que se pueden encontrar en virus nuevos y desconocidos, versiones modificadas de amenazas existentes y en muestras de malwares conocidos.

[28] Estrategia para limitar el tráfico de red estableciendo un tope a la frecuencia con la que un usuario puede repetir una acción en un determinado marco de tiempo.

(b) Detección de cantidades considerables de SMS enviados desde un mismo número telefónico o desde varios, en cortos periodos de tiempo. ----------

(c) Detección de números telefónicos que envían la misma cantidad de SMS o una cantidad similar durante uno o varios días consecutivos. ----------

(d) Cualquier otra medida que colabore con la identificación de campañas de smishing. ----------

12. Detección de ráfagas de spam (Spam Burst)[29] e identificación de campañas de smishing rápidas que intenten entregar gran cantidad de mensajes en cortos periodos de tiempo. ----------

13. Análisis de simetría en las comunicaciones que permita identificar de manera bidireccionalidad el tráfico que nunca recibe respuesta, es decir, servicios que generan grandes cantidades de comunicaciones, pero nunca reciben respuesta, correspondiente al comportamiento de bots[30].

14. Los operadores y proveedores deben bloquear todo tráfico de mensajes SMS internacional que de cualquier manera simule ser de tipo local, incluyendo el tráfico que atraviesa rutas de interconexión. ----------

15. Detección de Tráfico Inflado Artificialmente (AIT) con monitoreo de variaciones en el tráfico de mensajes hacia destinos específicos. ----------

[29] Envío masivo, automático y desmedido de mensajes de texto en cortos periodos de tiempo para saturar bandejas de entrada o redes de telecomunicaciones con mensajes de smishing.
[30] Aplicaciones o software automatizados programados para realizar tareas repetitivas, predefinidas y rápidas sin intervención humana.

Según lo anterior, los operadores y proveedores deben implementar sistemas de firewall automatizados para el bloqueo de tráfico SMS malicioso recibido por rutas de interconexión tanto internacional como local con criterios razonables que le permitan identificar un mensaje SMS como sospechosos y bloquearlo en caso de ser malicioso o cuyo origen haya sido enmascarado, sin embargo, estos requerimientos no se limitan a otros criterios de identificación que pueda establecer el operador para mejorar la seguridad de las comunicaciones y bloquear el tráfico de mensajes SMS maliciosos. Asimismo, deben aplicar las medidas de suspensión de servicios por realizar prácticas prohibidas según las disposiciones del Reglamento sobre el Régimen de Protección al Usuario Final a aquellos usuarios que generen tráfico malicioso. ----------

D. Los operadores y proveedores deben utilizar sistemas de reputación de enlaces para bloquear mensajes que contengan enlaces a sitios WEB maliciosos o de dudosa procedencia, y además, deberán reportar a la SUTEL los mecanismos de esta índole implementados. ----------

E. Los operadores y proveedores por medio de sistemas informáticos automatizados y de procesamiento en tiempo real, 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, por lo que, los operadores y proveedores tienen prohibido procesar el contenido, el tráfico y otros datos relacionados a los mensajes SMS para fines distintos a los especificados en esta normativa. Además, Los operadores y proveedores deben aplicar

medidas técnicas y administrativas que garanticen la destrucción de los datos una vez hayan cumplido su cometido con el sistema de firewall de SMS, asegurando que no puedan ser reconstruidos. ----------

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. ----------

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. ----------

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). ----------

I. Los operadores y proveedores podrán establecer un registro de excepciones para servicios autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del usuario receptor. Este requerimiento aplica únicamente para mensajes A2P.----------

J. 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. ----------

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

Para garantizar la efectividad de las medidas, el bloqueo debe implementarse de forma transversal en la cadena de encaminamiento de la mensajería, considerando tanto SMS P2P (usuario a usuario) como SMS A2P (aplicación/plataforma -origen- hacia usuario) incluyendo el tráfico recibido por medio de rutas de interconexión, así como variantes técnicas utilizadas en campañas maliciosas (p. ej., mensajes binarios, remitentes alfanuméricos/alias, rutas grises, SimBoxes y tráfico inflado artificialmente). Se reitera que, los operadores deben garantizar la seguridad en la trazabilidad de la información de extremo a extremo para los usuarios finales que contrataron sus servicios, de modo que, los operadores deberán asegurar: ----------

- Validación del identificador de origen. ----------
- Control de rutas autorizadas, asegurando el control de tráfico extremo a extremo, origen a destino. ----------
- Filtrado del contenido para detección de enlaces maliciosos y patrones de smishing. ----------
- Trazabilidad del tráfico desde el origen hasta el destino. ----------
- Retroalimentación continua mediante listas y registros auditables. -----

A continuación, se muestra el diagrama de flujo para la normativa propuesta: -

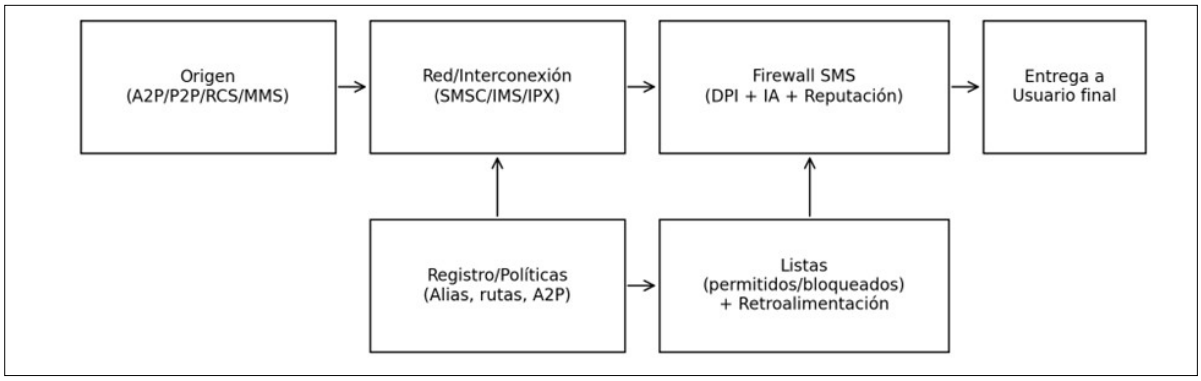

Imagen 2. Diagrama de implementación para filtrado o bloqueo de SMS P2P y A2P.

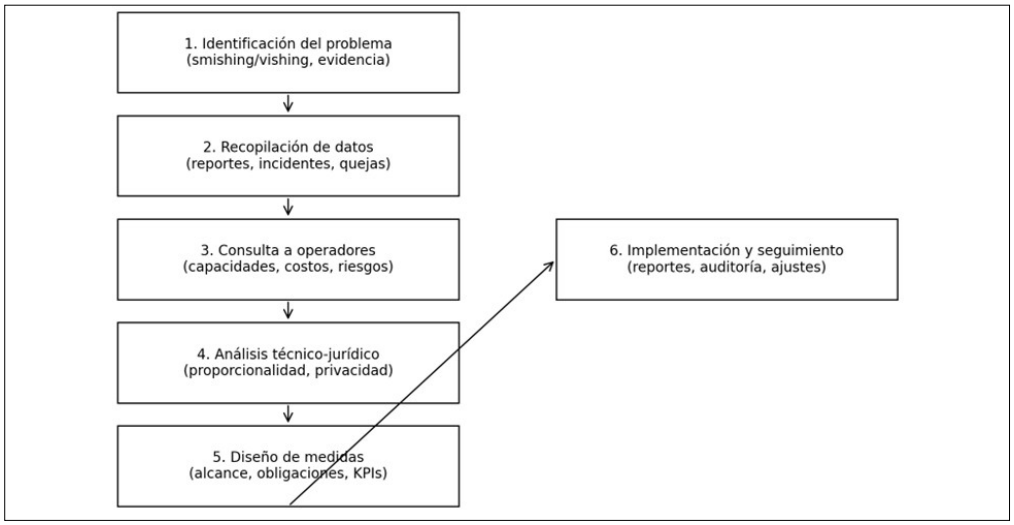

Imagen 3. Diagrama de metodología regulatoria para filtrado o bloqueo de SMS P2P y A2P.

3. SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P. ----------

Estas 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: --

A. Les corresponde a los operadores y proveedores validar y garantizar la legitimidad de las rutas mediante las cuales transita el tráfico A2P, por lo

que, son responsables de verificar el origen de las comunicaciones y tener control de extremo a extremo en las rutas de transporte, de modo que, deben 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. Los operadores solo permitirán el tráfico de mensajes A2P por las rutas oficiales y autorizadas mediante acuerdos formales suscritos con operadores, proveedores o agregadores, bloqueando todo el tráfico de mensajes A2P que utilice rutas no oficiales (rutas grises) y no garantice control de trazabilidad. ----------

B. Los operadores y proveedores deben implementar sistemas de firewall con capacidad de identificar si un mensaje que ingresa en su red es de tipo P2P o A2P, tanto por rutas de interconexión internacional como local, y bloquear la totalidad del tráfico A2P que ingrese por rutas de interconexión local, en el cual no se asegure la trazabilidad extremo-extremo, garantizando el tráfico de mensajes A2P únicamente por rutas oficiales y autorizadas entre operadores, proveedores o agregadores. ----------

C. Los operadores y proveedores deben garantizar la trazabilidad del tráfico A2P desde el origen del mensaje y hasta su destino, por lo que, deben 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. ----------

D. Los operadores y proveedores deben 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. ----------

E. Los operadores y proveedores podrán establecer registros de excepciones de las entidades o empresas autorizados a enviar tráfico de SMS A2P incluyendo 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 las entidades o empresas A2P y la finalidad en cuanto al uso que pretenden hacer de la modalidad de mensajería A2P, garantizando que solo empresas o entidades legítimas se encuentren en dicho registro, y bloquear todo el tráfico A2P saliente de clientes o servicios no incluidos en este registro, así como bloquear el tráfico de 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 los usuarios. Estos registros se deben compartir entre operadores y proveedores interconectados. ----------

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

El éxito del bloqueo de tráfico A2P malicioso o sospechoso recae sobre la capacidad de los operadores en identificar la totalidad del tráfico de tipo A2P que ingresa por sus rutas de interconexión tanto internacional como local, y bloquear todo el tráfico A2P que no permita garantizar control de la trazabilidad. Los siguientes diagramas muestran los esquemas de bloqueo que deben considerar los operadores y proveedores para implementar en sus rutas de interconexión tanto local como internacional: ----------

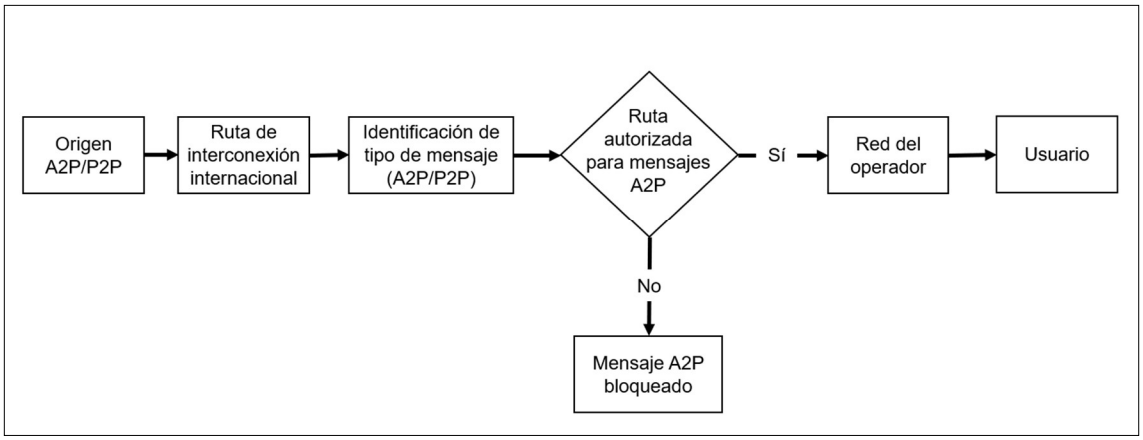

Imagen 4. Diagrama de implementación para bloqueo de SMS A2P por rutas de interconexión internacional.

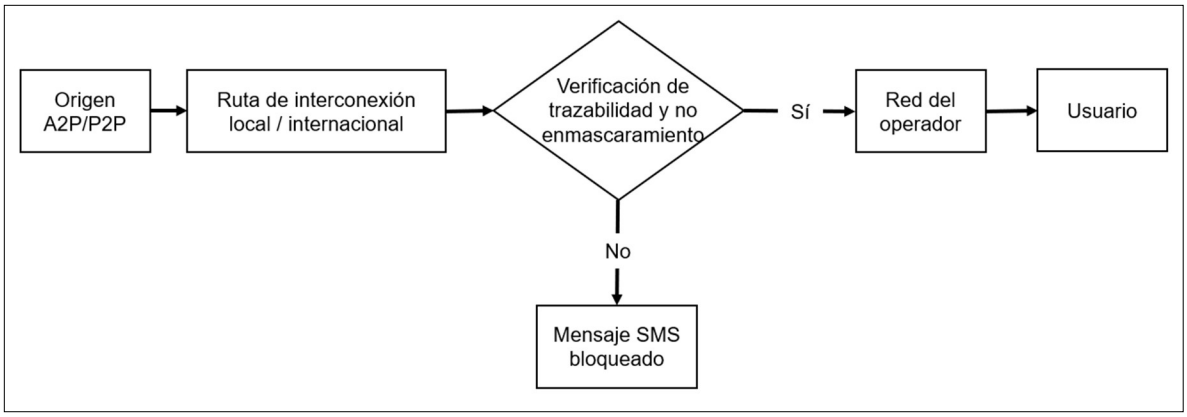

Imagen 5. Diagrama de implementación para bloqueo de SMS que no permiten trazabilidad o se encuentra enmascarado.

5. SERVICIOS DE LLAMADAS DE VOZ: ----------

Estas medidas aplican para la totalidad de operadores y proveedores de servicios de telecomunicaciones que brindan servicios de llamadas de voz: ----

A. Los operadores y proveedores deben implementar en sus redes, incluyendo rutas de interconexión, sistemas de firewall antispam en los servicios de voz que minimicen el impacto de los ataques tipo *vishing* a usuarios finales con al menos las siguientes capacidades: ----------

(a) Procesamiento masivo de registros de llamadas (CDRs)[31] para trazabilidad de las comunicaciones. ----------

(b) Procesamiento de información de señalización obtenida de las comunicaciones y por puntos de recopilación. ----------

(c) Detección de patrones de comportamiento sospechoso como frecuencia de llamadas, tasa de conexiones exitosas, duración de

[31] Call Detail Records.

las llamadas, duración de tonos, estadísticas de llamadas, entre otras. ----------

(d) Identificación de llamadas automatizadas que utilizan grabaciones de voz o voz sintética (robollamadas o robocalls). ----------

(e) Cualquier otra medida que colabore con la identificación de campañas de vishing. ----------

B. Los operadores y proveedores deben destinar un rango de números telefónicos para la implementación de cebos o señuelo que faciliten identificar generadores de spam, para su posterior bloqueo y aplicación de las suspensiones dispuestas en el RPUF sobre comisión de prácticas prohibidas. ----------

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. ----------

D. Los operadores y proveedores deben adoptar e implementar el estándar Out-of-Band SHAKEN (OOBS) para autenticación de todas las llamadas. ---------

E. Los operadores y proveedores deben mantener el cumplimiento de los lineamientos establecidos en la resolución RCS-294-2023 *"METODOLOGÍA REGULATORIA PARA LA IMPLEMENTACIÓN DE MEDIDAS CON EL FIN DE MINIMIZAR EL IMPACTO DE ESTAFAS TELEFÓNICAS MEDIANTE EL MÉTODO DEL ENMASCARAMIENTO DE LLAMADAS".* ----------

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. ----------

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). ----------

6. SOBRE EL PLAZO DE IMPLEMENTACIÓN. ----------

A. 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 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 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 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 sobre establecer registros de excepciones para servicios A2P autorizados a enviar grandes cantidades de mensajes informativos sin recibir respuesta del receptor. ----------

n) Inciso J sobre disponer de centros de atención al usuario final para el reporte de casos de smishing. ----------

Con respecto al apartado **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 **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 **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 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 sobre conservar los registros detallados de llamadas por un plazo mínimo de 4 años, conforme el artículo 52 del RPUF.”. ----------

7. 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. ----------

XI. **SOLICITAR** a la Secretaría del Consejo de esta Superintendencia que proceda con la notificación del oficio 05772-SUTEL-DGM-2026 del 12 de junio de 2026, a los participantes del proceso de consulta pública convocado en el diario oficial La Gaceta 65 del 10 de abril de 2026, tramitada en el expediente GCO-DGM-IET-00518-2026. ----------

XII. **SOLICITAR** a la Secretaría del Consejo de esta Superintendencia gestionar la publicación en el Diario Oficial La Gaceta el texto íntegro de la presente resolución. ----------

XIII. **REQUERIR** a la Unidad de Comunicación que, una vez publicada la resolución respecto a la "*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**. -----

En cumplimiento de lo que ordena el artículo 345 de la Ley General de la Administración Pública, se indica que contra esta resolución cabe el recurso ordinario de reposición ante el Consejo de la Superintendencia de Telecomunicaciones, a quien corresponde resolverlo y deberá interponerse en el plazo de tres días hábiles, contados a partir del día siguiente de la notificación de la presente resolución.--------

ACUERDO FIRME

NOTIFÍQUESE Y PUBLÍQUESE

La anterior transcripción se realiza a efectos de comunicar el acuerdo citado adoptado por el Consejo de la Superintendencia de Telecomunicaciones.----------

Atentamente,

CONSEJO DE LA SUPERINTENDENCIA DE TELECOMUNICACIONES

LUIS ALBERTO CASCANTE ALVARADO (FIRMA)

Firmado digitalmente por LUIS ALBERTO CASCANTE ALVARADO (FIRMA)
Fecha: 2026.06.24 08:35:32 -06'00'

Luis Alberto Cascante Alvarado

Secretario del Consejo

CONSTANCIA DE NOTIFICACIÓN

RCS-151-2026

"MEDIDAS REGULATORIAS CON EL FIN DE MINIMIZAR EL IMPACTO DE CIBERATAQUES MEDIANTE MENSAJES DE TEXTO SMS (SMISHING) Y LLAMADAS (VISHING) EN LAS REDES DE TELECOMUNICACIONES"

EXPEDIENTE: GCO-DGM-IET-00518-2026

Se notifica la presente resolución a:

CallMyWay: iprada@callmyway.com

Mitto: juan.santos@mitto.ch

Claro: notificaciones.sutel@claro.cr

ICE: notificacionesdrr@ice.go.cr

Liberty: legalcr@lla.com

Micitt: despacho.telecom@micitt.go.cr

Infocom: aramirez@infocom.cr

Tigo: notificaciones@tigo.co.cr