San José, 06 de marzo 2026
02238-SUTEL-DGM-2026

Señores
Miembros del Consejo.
Superintendencia de Telecomunicaciones.

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)

Estimados señores:

De conformidad con las funciones establecidas en los artículos del 41 al 44 del Reglamento Interno de Organización y Funciones de la Autoridad Reguladora de los Servicios Públicos y su Órgano Desconcentrado (RIOF), lo dispuesto en el artículo 60 incisos f) y g) de la Ley de la Autoridad Reguladora de los Servicios Públicos, Ley N°7593, el Decreto Ejecutivo 40943-MICITT Plan Nacional de Numeración y el artículo 64 del Reglamento de Acceso e Interconexión de Redes de Telecomunicaciones (RAIRT), la Dirección General de Mercados (en adelante DGM) y la Dirección General de Calidad (en adelante DGC) nos permitimos indicar lo siguiente: ----------

1. ANTECEDENTES.

1.1. 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).

1.2. El 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).

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

1.4. 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).

1.5. 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).

1.6. 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).

1.7. 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).

1.8. Mediante 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).

1.9. 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).

1.10. 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).

1.11. 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).

1.12. Mediante oficio N°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).

1.13. 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).

1.14. Mediante 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) --

1.15. 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)

1.16. 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).

1.17. 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)

1.18. 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).

1.19. Mediante 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).

1.20. 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) ---

1.21. 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)

1.22. 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).

1.23. 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).

1.24. 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) .

1.25. 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) .

1.26. 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).

1.27. 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.

1.28. 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).

1.29. 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).

1.30. 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).

1.31. 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).

1.32. 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).

1.33. 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).

1.34. 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).

1.35. 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).

1.36. 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.

1.37. 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).

1.38. 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)

1.39. Mediante 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).

1.40. 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).

1.41. Que mediante el acuerdo 023-049-2025 de la sesión ordinaria 049-2025 del Consejo de Sutel, celebrada el 4 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).

1.42. Mediante oficio 263-685-2025 del 08 de septiembre 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)

1.43. 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).

2. SOBRE LA PROBLEMÁTICA PLANTEADA.

2.1. SOBRE EL SMISHING (PHISHING MEDIANTE MENSAJES SMS)

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

[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

de mensajes de texto SMS, donde los atacantes engañan a las víctimas para que compartan información confidencial. ----------

El *smishing* está categorizado como un ataque de ingeniería social que se basa en la explotación de la confianza humana con el fin de engañar al destinatario para que ingrese a un enlace malicioso, donde los delincuentes utilizan *malwares* o sitios web fraudulentos para el robo de información confidencial. ----------

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. ----------

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. ----------

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

Asimismo, 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 septiembre 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],

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

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.----------

En la siguiente imagen se muestran ejemplos de intentos de *smishing* registrados por esta Superintendencia:----------

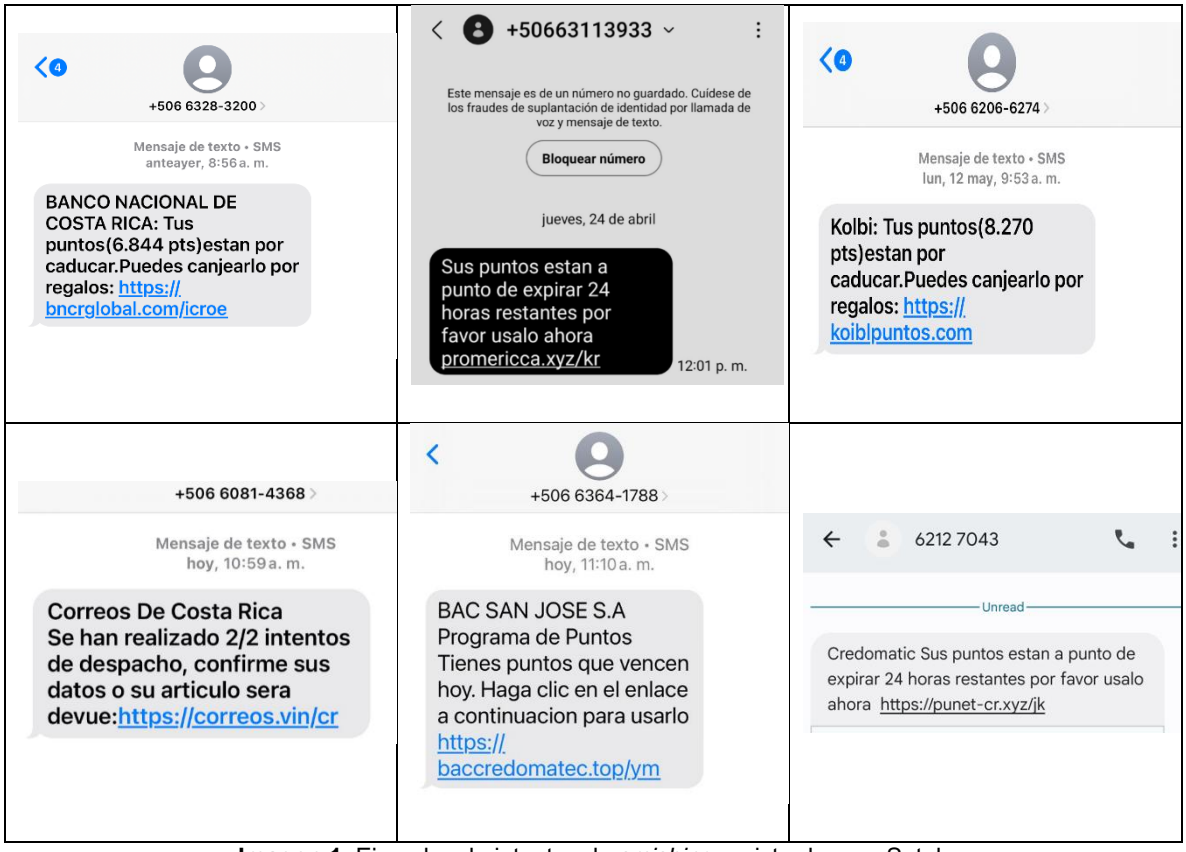

Imagen 1. Ejemplos de intentos de *smishing* registrados por Sutel.

Cabe señalar que, solo 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. ----------

[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

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."*

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

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 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. (…)"*. ----------

En cumplimiento con lo anterior, **Liberty Telecomunicaciones de Costa Rica LY, S.A.** mediante el oficio LY-Reg0245-2025 del 26 de septiembre 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.----------

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 septiembre de 2025, denominada ***"Fraude por SMS: el vacío legal que facilita la estafa de millones en Costa Rica"***[12], de modo que,

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

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. ----------

Es importante mencionar que, el artículo 2 inciso f) de la Ley N°8642, Ley General de Telecomunicaciones establece como uno de sus objetivos promover el desarrollo y uso de los servicios de telecomunicaciones como **apoyo a la seguridad ciudadana**, de modo que, tanto este regulador como los operadores se encuentran en la obligación de realizar todos los esfuerzos para bloquear las comunicaciones maliciosas, ya que, se está utilizando la numeración asignada a los operadores para realizar acciones ilícitas y de mala fe que perjudican la seguridad y los derechos de los demás usuarios finales.----------

Por lo anterior, mediante el presente documento se propone un marco regulatorio para que los operadores identifiquen y bloqueen el tráfico malicioso de mensajes de texto SMS tanto en sus redes de telecomunicaciones como en los puntos de interconexión entre operadores y proveedores, de conformidad con las recomendaciones internacionales para la lucha contra el *smishing*. ----------

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

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.

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.----------

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

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 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.

[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

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. ----------

Asimismo, 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"***[15], 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. ----------

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. ----------

[15] https://ncrnoticias.com/internacional/lo-pueden-extorsionar-%F0%9F%98%9E-asi-funciona-el-vishing-nueva-estafa-telefonica-en-la-que-utilizan-ia/

2.3. MENSAJES SMS P2P Y A2P.

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. ----------

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. ----------

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*)[16]. ----------

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. ----------

No obstante, 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). ----------

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

[16] 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.

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

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:

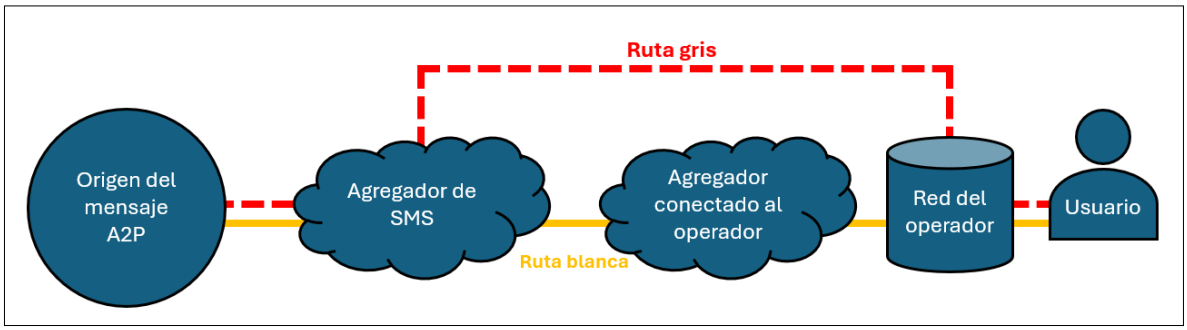

Imagen 2. Arquitectura de tráfico de mensajes SMS A2P.

Además, se ha detectado que operadores locales[17] utilizan rutas de interconexión local con otro operador 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.

De acuerdo con el desarrollador de plataformas de comunicación en la nube Infobip[18], 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

[17] 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.
[18] https://www.infobip.com/glossary/what-is-an-sms-gray-route

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.

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. -------

Asimismo, 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[19]. ---

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[20], destacando los casos de éxito en Reino Unido, Irlanda y España con la implementación de un registro de remitentes de mensajes A2P autorizados.----------

Por otro lado, 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 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)[21], 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. ----------

[19] https://www.infobip.com/glossary/global-title
[20] https://mobileecosystemforum.com/sms-senderid-protection-registry/
[21] 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.

Editoriales como ScienceDirect, recomiendan el uso de herramientas basadas en Machine Learning (aprendizaje automático con Inteligencia Artificial) para combatir el smishing[22].---

Además, 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. ----------

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.-

- 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*.---------

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.

[22] https://www.sciencedirect.com/science/article/pii/S1877050925009834

3. SOBRE LA COMPETENCIA DE LA SUTEL.

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. ----------

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. ----------

En ampliación de lo anterior, mediante la Ley No. 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. ----------

De tal manera, 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. ----------

Por otra parte, 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 N°8642 y sus reformas. ----------

Así las cosas; es importante mencionar, 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 N°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.

4. NORMATIVA APLICABLE

4.1. 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. ---

4.2. 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."*[23] 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)."*[24]. ----------

4.3. Que a través de la Ley N° 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.

[23] 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.*
[24] ibid. Nuevos métodos derivados de la digitalización para obtener información. Página 18

4.4. Que a partir de los años 2012 y 2013; mediante la Ley No. 9048 y Ley No. 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, 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.----------

4.5. 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.----------

4.6. 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*". ----------

4.7. Que por su parte, la Ley N°8642 es conteste con lo desarrollado en la Ley N°7593, siendo que resulta de vital importancia la protección de los derechos de los usuarios finales, 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 N°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.

4.8. 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."

4.9. 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 (…)".* ----------

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.

4.10. 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.

4.11. 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. ----------

4.12. 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. ----------

4.13. Que mediante el Decreto Ejecutivo N° 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."*----------

4.14. 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."----------

5. SOBRE LA CONSULTA A LOS OPERADORES Y PROVEEDORES DE SERVICIOS DE TELECOMUNICACIONES Y PERTINENCIA DE LA ACTUALIZACIÓN REGULATORIA DE LA RCS-294-2023.

En el marco del *por tanto* numeral 6 de la resolución RCS-294-2023, y ante la evidencia de que las modalidades de fraude han migrado hacia otros medios tecnológicos (particularmente la mensajería de texto SMS en sus modalidades P2P y A2P), la Dirección General de Mercados realizó una consulta mediante oficio número 03422-SUTEL-DGM-2025 del 24 de abril de 2025 a los operadores y proveedores con numeración asignada, con el fin de recabar criterios técnicos sobre acciones adicionales que permitan ampliar el alcance de las medidas de bloqueo y mitigación del fraude en redes públicas de telecomunicaciones.----------

De las respuestas recibidas, se desprenden elementos comunes relevantes: i) la factibilidad de reforzar la autenticación del identificador de origen en troncales SIP mediante mecanismos como *P-Asserted-Identity* y controles de ANI por troncal, con el objetivo de impedir la suplantación de numeración asignada; ii) la necesidad de incorporar controles específicos sobre tráfico de mensajería A2P, dada su naturaleza automatizada y su potencial para facilitar campañas masivas de *smishing*; iii) la conveniencia de adoptar medidas basadas en estándares internacionales de autenticación y verificación del origen (p. ej., *STIR/SHAKEN*[25]) o, alternativamente, esquemas de consentimiento/*opt-in/opt-out*.-

Adicionalmente, se identificaron consideraciones operativas sobre la carga administrativa de los reportes periódicos y sobre la heterogeneidad de capacidades técnicas entre agentes (por ejemplo, proveedores que iniciaron operaciones recientemente), lo cual resulta determinante para diseñar obligaciones graduadas, medibles y proporcionales. ----------

En consecuencia, la actualización regulatoria se estima pertinente y necesaria por razones de seguridad jurídica y eficacia regulatoria, y con el objetivo de proteger los derechos de los usuarios y la privacidad y confidencialidad de las comunicaciones, procurando así que se obtengan los mejores beneficios del progreso tecnológico y de la convergencia, sin menoscabo de la seguridad de las comunicaciones.----------

[25] Estándar de protocolos para autenticar llamadas telefónicas con el objetivo de combatir la suplantación de identidad y las llamadas automáticas fraudulentas en redes de VoIP.

En esa línea es necesario tener presente los siguientes puntos que evidencian la necesidad de la adopción de una medida regulatoria específica sobre los SMS: (a) la RCS-294-2023 se diseñó con enfoque principal en llamadas de voz y enmascaramiento (*spoofing*) y no cubre de forma expresa la mensajería SMS A2P/P2P; (b) existe evidencia de afectación a usuarios finales mediante *smishing*, con utilización indebida de numeración asignada; y (c) las soluciones técnicas disponibles en el mercado permiten implementar, con criterios de proporcionalidad, mecanismos de bloqueo y filtrado específicos para SMS sin desnaturalizar el servicio ni vulnerar el marco de privacidad, siempre que se delimiten finalidades, controles y salvaguardas de tratamiento de datos. ----------

Es importante tener presente que pese a que la Junta Directiva de la ARESEP mediante resolución RJD-019-2013 del 4 de abril del 2013 declaró los SMS como servicios de información, el artículo 51 de la Ley 8642 le otorga a la SUTEL la potestad de imponer a los proveedores de estos servicios entre otras, la obligación de ajustarse a normas o regulaciones técnicas para interconexión, cuando se determine que esto se requiere para resguardar los derechos de los usuarios. ----------

En este sentido, se ha determinado que es necesario imponer obligaciones en materia de interconexión a los SMS con el objetivo de proteger los derechos de los usuarios y la privacidad y confidencialidad de las comunicaciones, si bien la regulación en cuestión puede significar una carga jurídica para los operadores y proveedores dicha carga no resulta mayor que el beneficio esperado de dicha regulación, que es el resguardo de los derechos de los usuarios y la seguridad de los servicios de telecomunicaciones, por tanto se verifica la razonabilidad y proporcionalidad de dicha medida. ----------

6. REGULACIONES Y RECOMENDACIONES INTERNACIONALES.

6.1. RECOMENDACIÓN ITU-T X.1247 *"MARCO TÉCNICO PARA LUCHAR CONTRA EL CORREO BASURA EN LA MENSAJERÍA MÓVIL".*

La Unión Internacional de Telecomunicaciones (en adelante UIT) mediante su recomendación **ITU-T X.1247** ***"Marco técnico para luchar contra el correo basura en la mensajería móvil"*** brinda una propuesta general de los procesos contra el correo basura (en adelante *spam*) en la mensajería móvil. En dicho marco se especifican las funciones y procedimientos de trabajo para cada entidad involucrada, así como, mecanismos para compartir información sobre la lucha contra el *spam* en la mensajería móvil. ----------

En esta recomendación define el dominio antispam en la mensajería móvil cuya estructura comprende las siguientes funciones: ----------

- **Función de administración antispam en la mensajería móvil (AMgmt):** recibe información estadística sobre tráfico *spam* de la Amon y actualiza las reglas de filtrado en su dominio. También comparte información sobre tráfico spam con el servicio de notificación. ----------

- **Función de monitoreo y vigilancia antispam en la mensajería móvil (AMon):** recibe el tráfico de mensajería móvil sospechoso de la APr y verifica si se trata de *spam*. También proporciona el análisis y la información estadística sobre spam a la AMgmt tras agregar y analizar los datos relativos a dicho tráfico. ----------

- **Función de procesado de antispam en la mensajería móvil (APr):** aplica reglas a los mensajes móviles y filtra el tráfico spam. También recibe las reglas de filtrado de la AMgmt y la información del usuario por medio de los clientes de mensajería móvil. ----------

- **Clientes de mensajería móvil:** pueden contribuir mediante el servicio de notificación enviando información a la APr sobre aclaraciones de mensajes marcados como *spam* incorrectamente. ----------

- **Servicio de notificación:** se recomienda para mejorar el resultado del filtrado. Recibe el informe de *spam* enviado por el cliente. Puede ser una línea de atención al cliente, un sitio web o un centro de notificación de mensajes SMS, con objeto de que el operador pueda adaptar las reglas de filtrado. Requiere autorización por parte del usuario para enviar información al operador. ----------

La estructura del dominio antispam en la mensajería móvil propuesta en la recomendación ITU-T X.1247 se muestra en la siguiente imagen: ----------

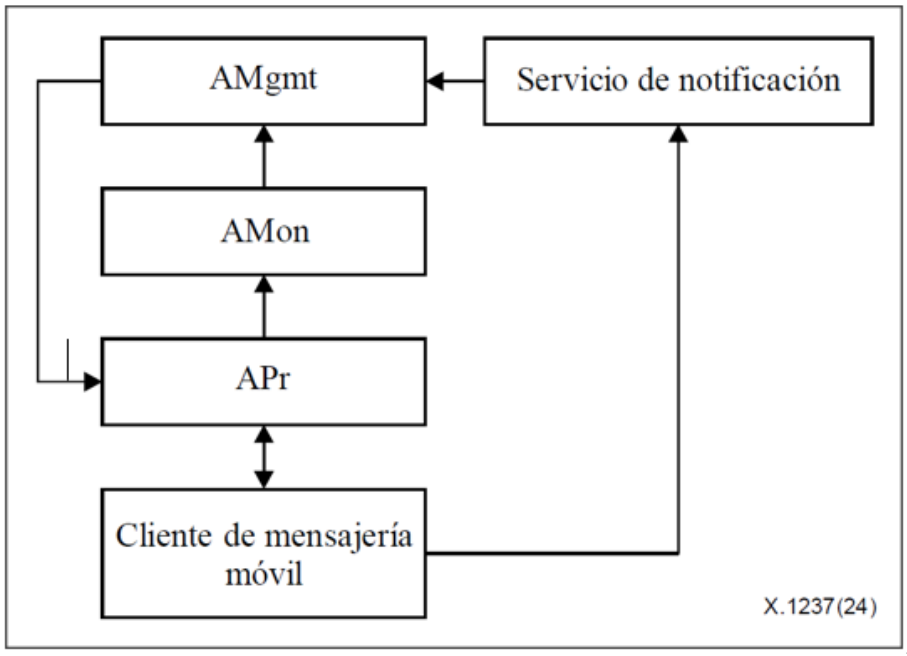

Imagen 3. Estructura general para un dominio antispam en la mensajería móvil. Fuente Rec. UIT-T X.1247.

Además, la recomendación ITU-T X.1247 menciona que, la eficiencia y el rendimiento de las medidas antispam en un dominio aumenta con la existencia de interconexiones e inter-funcionamiento entre operadores, estableciendo mecanismos de colaboración entre sus dominios antispam. Esta comunicación se realiza mediante relaciones fiables donde se comparten datos sobre tráfico spam, autenticación de origen del mensaje e informes de usuario. En la siguiente imagen se muestra el modelo propuesto en la recomendación ITU-T X.1247 para dos dominios antispam en mensajería móvil con acuerdos que permiten compartir información antispam entre sí. En la siguiente imagen E, F y G son interfaces lógicas seguras entre dominios: ----------

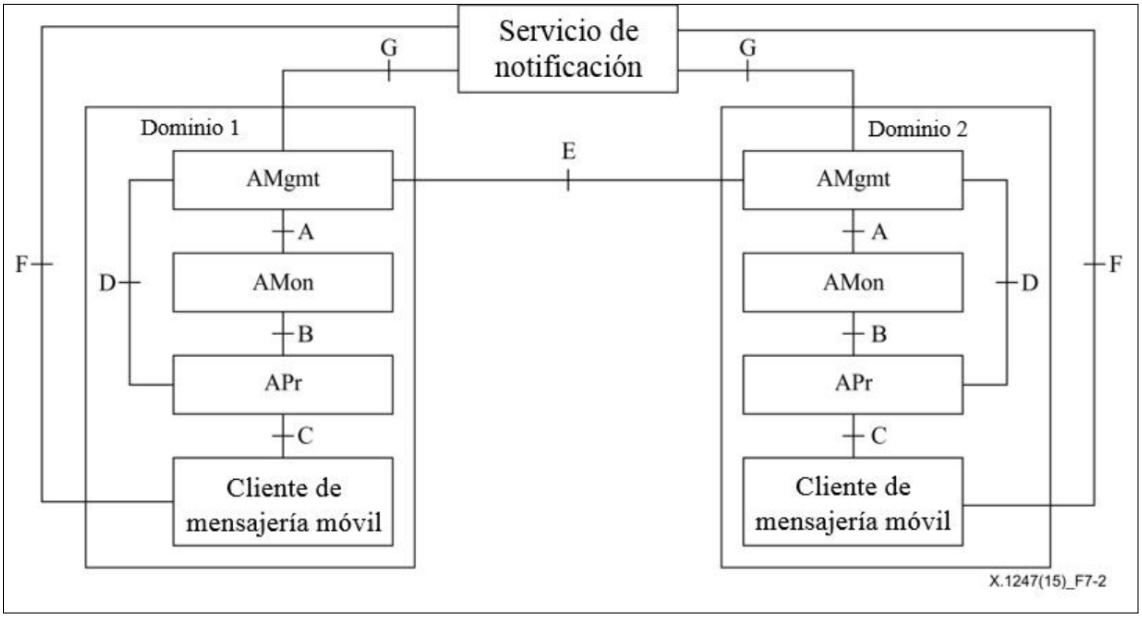

Imagen 4. Estructura para dos dominios antispam en la mensajería móvil que comparten información. Fuente Rec. UIT-T X.1247.

Asimismo, la UIT recomienda el uso de señuelos en la APr para detectar el tráfico *spam*, los cuales consisten en cuentas *"trampa"* con números de teléfono no otorgados a usuarios, de este modo, todos los mensajes que sean distintos de los previstos pueden ser procesados como tráfico sospechoso para analizar su contenido. Los señuelos deben cumplir una etapa de aprendizaje para verificar el tráfico sospechoso y filtrar el tráfico que no es spam antes de generalizar sus características. ----------

Esta recomendación también menciona otras medidas que pueden tomar los operadores para identificar el tráfico spam antes de enviarlo a los clientes receptores, las cuales dependen de las características del mensaje o de su patrón de envió, según se enlistan a continuación: ----------

- **Lista blanca/lista negra del MSISDN (*Mobile Station International Subscriber Directory Number*):** Los operadores móviles pueden bloquear los mensajes de

remitentes de spam reconocidos, y los abonados pueden definir sus propias listas negras/blancas para bloquear o aceptar mensajes de remitentes específicos. -------

- **Reconocimiento aproximado:** filtrado de *spam* ante medidas de confusión como incluir de forma arbitraria caracteres específicos o sustituirlos por otros similares, por lo que, la función del reconocimiento aproximado es reconocer este intento de eludir el filtrado. ----------

- **Frecuencia de envío:** los remitentes de mensajes *spam* pueden enviarlos a numerosos receptores en un corto periodo de tiempo y a una velocidad mucho mayor que la de un remitente regular, con un intervalo de tiempo entre mensajes menor. Si la frecuencia de envío de un usuario supera un umbral establecido previamente, se identificará a ese usuario como un remitente de mensajes *spam* altamente sospechoso.----------

- **Tasa de envío satisfactorio de mensajes:** Dado que los mensajes spam se envían a receptores desconocidos de forma aleatoria la tasa de envío satisfactorio de mensajes spam es sustancialmente inferior a la del envío de mensajes móviles.----

- **Registro de llamadas del remitente (CDR):** puede ayudar al operador a analizar el patrón de envío. Si el mensaje se envía a muchos abonados y obtiene una baja tasa de respuesta, el remitente podrá considerarse un remitente de correo basura sospechoso, además, los remitentes de mensajería *spam* habitualmente utilizan un número telefónico solamente para el servicio de mensajería SMS, sin usar otros servicios como llamadas de voz. ----------

- **Configuración de reglas específicas para cada usuario:** mecanismos de configuración para cada usuario que permitan definir el tipo de mensajes que no desea recibir e informar de ello al sistema de filtrado.----------

- **Re-encaminamiento a la Red móvil de origen del receptor HPLMN (*Home Public Land Mobile Network* o Red Móvil Terrestre Pública Local):** para evitar que los receptores que se encuentren en una zona de itinerancia (*roaming*) reciban mensajes sin que se aplique un filtrado antispam, los mensajes enviados a los clientes en zona de itinerancia se reenvían al dominio antispam en la HPLMN, donde son filtrados antes de ser enviados a la red móvil visitada VPLMN (*Visited Public Land Mobile Network* o Red Móvil Terrestre Pública Visitada). ----------

Además, para el procesado del tráfico spam en la mensajería móvil, la recomendación ITU-T X.1247 señala la importancia de un mecanismo adaptativo que se ajuste a los nuevos tipos de *spam* que surgen constantemente y sus variaciones, por lo que, la solución implementada por parte de los operadores para combatir el *smishing* debe disponer de dominios de seguridad con capacidades de detección, administración y procesamiento del tráfico de mensajes maliciosos, además de compartir información al respecto entre los dominios de seguridad de cada operador para bloquear el tráfico de mensajes maliciosos.----------

6.2. RECOMENDACIÓN UIT-T X.1237 *"MARCO TÉCNICO DE SEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN DE IDENTIFICACIÓN PERSONAL EN LA LUCHA CONTRA EL SPAM EN LA MENSAJERÍA MÓVIL".*

Por otro lado, la recomendación UIT-T X.1237 ***"Marco técnico de seguridad para la protección de la información de identificación personal en la lucha contra el spam en la mensajería móvil"*** toma en cuenta la protección de la información de identificación personal para el diseño y aplicación de soluciones para contrarrestar el *spam* en la mensajería móvil, además, propone un marco técnico de seguridad para la protección de la información de identificación personal en la lucha contra el *spam*. -----

La información de identificación personal puede ser generada a partir de los mensajes enviados por el usuario, a partir de la información compartida con otro operador, o generada por el sistema antispam de mensajería móvil. Estos datos pasan por varios dominios funcionales y etapas durante su ciclo de vida, según se muestra en el siguiente diagrama:----------

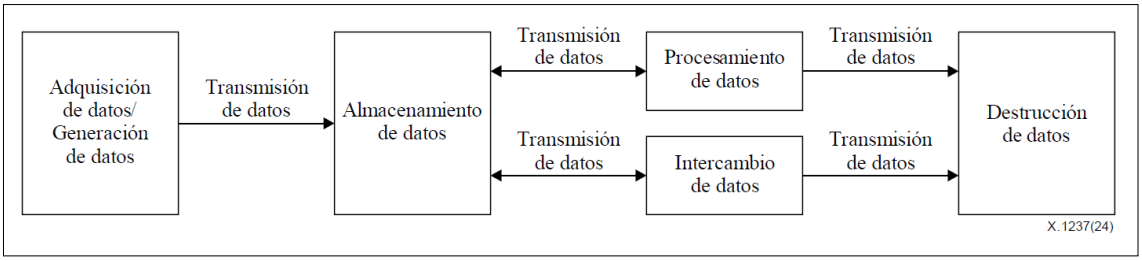

Imagen 5. Ciclo de vida de los datos en el proceso de lucha contra el spam en la mensajería móvil. Fuente Rec. UIT-T X.1237.

Según la imagen anterior, una vez que los datos son adquiridos o generados y almacenados, son procesados con el fin de extraer las características del spam. Al mismo tiempo los datos son intercambiados entre operadores, lo que resulta indispensable en la lucha contra el spam en la mensajería móvil. Finalmente, la destrucción de datos es la última etapa del ciclo de vida de los datos. ----------

De acuerdo con la recomendación UIT-T X.1237, cada dominio funcional tiene en cuenta la protección de los datos en las fases de diseño y aplicación, por lo que, dispone las correspondientes capacidades de seguridad en cada una de las entidades funcionales que integran el dominio antispam en la mensajería móvil para la protección de los datos. Esto incluye mecanismos de encriptación que aseguren la confidencialidad e integridad de los datos, así como su adecuada destrucción sin posibilidad de ser restaurados. ----------

Por lo anterior, los sistemas de seguridad implementados por los operadores deben procesar el contenido de los mensajes única y exclusivamente para bloquear el tráfico malicioso, según los fines que se proponen en esta resolución, garantizando su

confidencialidad y destrucción cuando sean obsoletos para el sistema, sin posibilidad de ser restaurados. ----------

6.3. Estándar ETSI TR 103 421 *"Network Gateway Cyber Defence"*.

El Instituto Europeo de Normas de Telecomunicaciones, en adelante ETSI (European Telecommunications Standards Institute), en su estándar TR 103 421 propone que la defensa de ciberseguridad en las redes de telecomunicaciones debe estar integrada en el gateway[26] (puerta de enlace) de la red, y no de forma periférica, de modo que, el gateway es el único punto de acceso al dominio de seguridad. ----------

El firewall en el gateway debe incluir el escaneo de tráfico, la búsqueda de amenazas como malware, la protección de todo tipo de clientes y la prevención de dispositivos maliciosos que ataquen las redes. Además, este estándar incita a la cooperación de todos los operadores que transportan tráfico para no poner en peligro las redes ni a sus usuarios finales, mediante el desarrollo y la aplicación de especificaciones y la firma de acuerdos de servicio que exigen que el tráfico cumpla ciertos requisitos, como estar libre de malware o identidades suplantadas, de modo que, la defensa y seguridad debe ocurrir en los puntos de interconexión, garantizando que un mensaje malicioso proveniente de otra red o de internet, debe ser interceptado antes de entrar en el núcleo de la red del operador. ----------

Este estándar resalta la importancia de observar características en los datos que permitan identificar el tráfico malicioso, como: ----------

- Identificadores de clase y tipo de dispositivo.
- Definición de direcciones IP y puertos.
- Nombres de dominio.
- URL[27] (tanto completas como con comodines[28]).
- Información de aplicaciones y sistema.
- Hashes[29] de los archivos enviados en la red.
- Información del cliente.
- Referencias de registro en la red.
- Sellos de tiempo precisos y confiables.

Esta información facilitará la toma de decisiones de ciberseguridad según las políticas implementadas por cada operador. Si bien algunos de estos datos son sensibles y pueden afectar la privacidad, la ciberdefensa también desempeña un papel importante

[26] Punto de acceso e interconexión entre redes, protocolos o tecnologías. Gestiona la entrada y salida de datos en la red de un operador, permitiendo la comunicación y el flujo de datos.
[27] URL (Uniform Resource Locator) es la dirección única y específica utilizada para localizar recursos en Internet, como páginas web, imágenes o documentos.
[28] Direccion URL con caracteres especiales, generalmente asterisco (*), para representar un conjunto de caracteres en una dirección web, por ejemplo *sutel.go.cr/*
[29] Huella digital única de cada archivo para verificar la integridad de archivos, garantizando que no han sido modificados o corrompidos.

en su disponibilidad, de modo que se debe lograr un equilibrio adecuado entre ciberseguridad y privacidad. ----------

6.4. RECOMENDACIÓN ITU-T X.1242 *"SISTEMA DE FILTRADO DE CORREO BASURA EN EL SERVICIO DE MENSAJES CORTOS (SMS) BASADO EN REGLAS ESPECIFICADAS POR EL USUARIO".*

Otra alternativa brindada por la UIT se encuentra en la recomendación **ITU-T X.1242** ***"Sistema de filtrado de correo basura en el servicio de mensajes cortos (SMS) basado en reglas especificadas por el usuario"***, donde describe la estructura del sistema de filtrado de spam en SMS basado en reglas especificadas por el usuario, tanto en las redes móviles como en las fijas. Es un servicio de tipo optativo para los usuarios, los cuales deben brindar su consentimiento de suscripción, ya que, algunos mecanismos de filtrado pueden afectar la privacidad del tráfico de telecomunicaciones, dado que el sistema de filtrado debe leer la información contenida en el mensaje con el objetivo de determinar si es *spam* o no. Por consiguiente, los sistemas de filtrado de *spam* en SMS deben considerar las precauciones para cumplir la legislación aplicable a privacidad de la información. ----------

Esta recomendación señala la importancia de implementar mecanismos de sincronización entre los sistemas de filtrado de spam en SMS tanto en el lado del operador remitente como en el lado del operador destinatario, además, define los procesos de filtrado de *spam* en SMS para mensajes enviados al sistema de filtrado desde el lado del destinatario y desde el lado del remitente. ----------

Los sistemas de filtrados de *spam* en SMS con reglas especificadas por el usuario deben ofrecer a los usuarios métodos de gestión y configuración de las reglas de filtrado, mediante SMS y web, donde los usuarios pueden especificar sus reglas de filtrado, basadas en la dirección, la hora y el contenido del mensaje. ----------

6.5. RECOMENDACIÓN ITU-T X.1244 *"CARACTERÍSTICAS GENERALES DE LA LUCHA CONTRA EL CORREO BASURA (SPAM) EN APLICACIONES MULTIMEDIOS BASADAS EN IP".*

La recomendación **ITU-T X.1244** ***"Características generales de la lucha contra el correo basura (spam) en aplicaciones multimedios basadas en IP"***, describe los conceptos y características de los tipos de *spam* que se dan en las aplicaciones de multimedios IP como la telefonía IP, la mensajería instantánea, entre otros, y expone aspectos de consideración para los operadores de telecomunicaciones en la lucha contra el *spam* en aplicaciones de multimedios IP, desde el punto de vista técnico y de seguridad. ----------

Esta recomendación señala los tipos más habituales de spam que pueden sufrir las aplicaciones de multimedios IP, los cuales se clasifican por comunicaciones en tiempo real o no, es decir, la comunicación con el receptor se establece en tiempo real (por

ejemplo, una llamada), o por el tipo de medio IP utilizado, sea texto, voz o video (la clasificación video incluye imágenes), según se muestra en la siguiente imagen: --------

	Texto	Voz	Vídeo
Tiempo real	• Spam en mensajería instantánea • Spam en charla	• Spam en VoIP • Spam en mensajería instantánea	• Spam en mensajería instantánea
Tiempo no real	• Spam de texto/multimedios • Spam de texto en el servicio de compartición de ficheros P2P • Spam de texto en sitio web	• Spam de voz/multimedios • Spam de voz en el servicio de compartición de ficheros P2P • Spam de voz en sitio web	• Spam de vídeo/multimedios • Spam de vídeo en el servicio de compartición de ficheros P2P • Spam de vídeo en el sitio web

Imagen 6. Clasificación de spam en aplicaciones de multimedios IP. Fuente Rec. UIT-T X.1244.

De acuerdo con citada normativa, el aumento de spam por multimedios IP se debe al bajo coste monetario que facilitan los multimedios IP, por lo que, expone las amenazas de seguridad relacionadas con el spam en multimedios IP, las cuales se definen desde el punto de vista del envío de spam a la red, y se clasifican según la técnica de ataque, como se muestra en la siguiente imagen:

Técnica de ataque	Amenaza de seguridad de spam
Código maligno/control remoto	Bot de spam
Pirateo de sesión	Pirateo de sesión
Inyección SQL	Inyección SQL
Rastreo	Rastreo de información de registro
Falsificación de identidad	Falsificación de emisor, envenenamiento de cache, control de encaminamiento
Otras	Recopilación de identificadores, sistema de gestión vulnerable

Imagen 7. Amenazas de seguridad de spam en multimedios IP clasificadas por técnica de ataque. Fuente Rec. UIT-T X.1244.

No obstante, menciona que, implementando contramedidas de autentificación, autorización y gestión de seguridad, se pueden mitigar las amenazas expuestas anteriormente. Además, existen otros mecanismos para la lucha en contra del *spam* en aplicaciones de multimedios IP, como las enlistadas a continuación: ----------

- **Lista negra/blanca:** consiste en filtrar mensajes o llamadas procedentes de emisores que figuren en las listas. ----------
- **Sistema de reputación:** la valoración del emisor ayuda al receptor a decidir si acepta o rechaza la comunicación. ----------
- **Círculos de confianza:** compartición de listas blancas entre dominios fiables.------
- **Enmascaramiento de dirección:** es un método preventivo que evita exponer la dirección IP del usuario, a los programas de extracción automática de direcciones utilizados por los ciberdelincuentes. ----------
- **Prueba interactiva humana:** desafío que sólo un humano pueda entender y no una máquina.----------
- **Filtrado de contenido:** filtra según el texto contenido en un mensaje o correo electrónico.----------
- **Autentificación por intercambio de claves:** identifica de manera segura al emisor de un mensaje y contribuye a bloquear ataques de tipo falsificación.
- **Filtrado de spam en red:** con mecanismos como rechazo de paquetes en la entidad de red, lista negra distribuida o cortafuegos de *spam*. ----------
- **Sello en línea:** si el servicio no se encuentra en la lista blanca debe pagar un sello para establecer comunicaciones.----------
- **Filtrado de spam por autorización:** se filtran las comunicaciones en función de las políticas del usuario o de la red. ----------
- **Medidas jurídicas y reglamentos:** definir leyes y reglamentos que prohíban el *spam*.----------

La recomendación ITU-T X.1244 menciona que la utilización de uno o dos métodos no conseguirá eliminar todos los tipos de *spam* en multimedios IP, por lo que, se debe analizar los distintos tipos de *spam* que afectan las diversas aplicaciones de multimedios IP y los métodos de lucha contra el *spam* de conformidad con las características de la aplicación multimedios IP que se utilice.

6.6. RECOMENDACIÓN ITU-T X.1245 *"MARCO PARA LA LUCHA CONTRA EL CORREO BASURA EN APLICACIONES MULTIMEDIOS IP".*

La recomendación **ITU-T X.1245** ***"Marco para la lucha contra el correo basura en aplicaciones multimedios IP"***, describe los métodos que pueden emplearse sobre las aplicaciones de multimedios IP para luchar contra el *spam* en multimedios IP, aprovechando las características especiales del spam que lo distinguen de las

aplicaciones de multimedios IP legitimas, como la fuente, sus características y el contenido, no obstante, reitera que la utilización de una sola técnica podría no bastar para combatir eficazmente el *spam* en multimedios IP, por lo que, es importante aplicar simultáneamente más de una técnica. ----------

Mediante el análisis de la fuente de la comunicación, como la información sobre la reputación o el historial de la fuente es posible determinar la procedencia de una aplicación de multimedios IP, donde deben tomarse medidas como la sólida autentificación de las fuentes de las aplicaciones multimedios IP y la gestión eficaz de las políticas de identificación de *spam*. ----------

En cuanto al método de análisis de características, los multimedios IP poseen varias características especiales que permiten distinguir el tipo de tráfico, como la cantidad de mensajes enviados o la información del protocolo utilizado. Por otro lado, el método de análisis del contenido señala que este debe realizarse en un plazo razonable y obteniendo resultados con alto nivel de calidad, por lo que, se deben emplear tecnologías avanzadas para el reconocimiento de sonido e imagen, dado que el análisis del contenido multimedia puede resultar más complejo en comparación con el análisis de textos. ----------

Basado en lo anterior, la recomendación ITU-T X.1245 describe el marco para combatir el *spam* en multimedios IP, el cual, ha sido diseñado para abarcar diversos medios, con la finalidad de proteger a los usuarios y las redes contra correos indeseables. Este marco está conformado por **funciones SAS** (funciones de antispam en el lado emisor) destinadas a identificar y bloquear el *spam* en multimedios IP del lado de la fuente antes de que este se propague a lo largo de la red, **funciones RAS** (funciones de antispam en el lado receptor) cuyo objetivo es identificar y bloquear el *spam* que se quiere enviar al receptor, **funciones CAS** (funciones de núcleo antispam) con capacidades para gestionar las políticas y controlar las funciones RAS y SAS, donde se analiza la fuente o las características de las aplicaciones multimedios IP con miras a identificar y filtrar el *spam* en el trayecto de paquetes IP entre los generadores de *spam* y los receptores. Finalmente, las **funciones SR** (funciones de receptor de *spam*) son mecanismos que permiten a los usuarios establecer políticas antispam para protegerse ellos mismos. Estas cuatro funciones principales conforman el marco de seguridad dispuesto por la UIT para combatir el spam en aplicaciones de multimedios, según se muestra en la siguiente imagen:----------

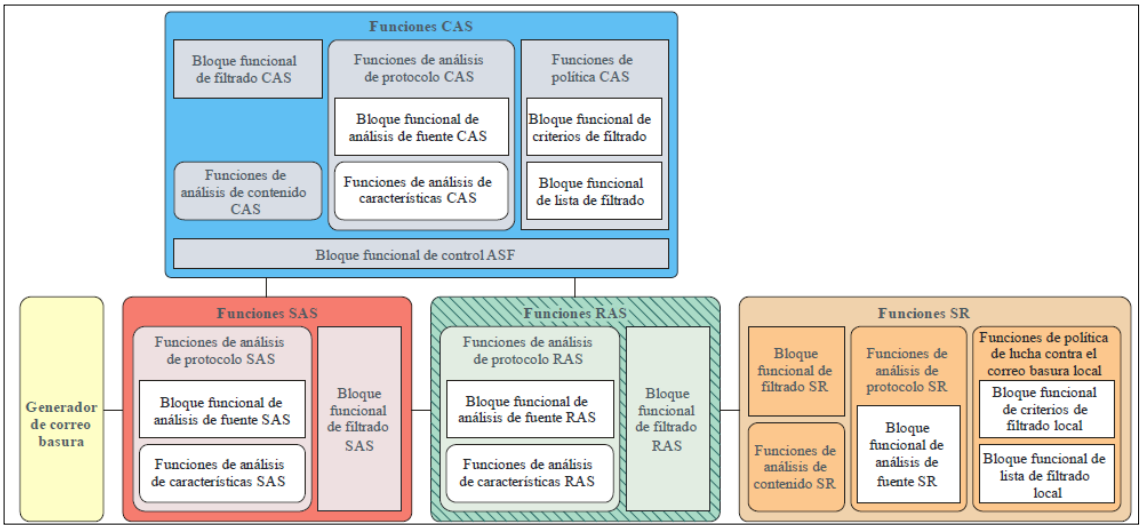

Imagen 8. Marco para la lucha contra el spam en multimedios IP.
Fuente Rec. UIT-T X.1245.

Las características y procedimientos de cada uno de los bloqueos funcionales son detallados ampliamente en la recomendación ITU-T X.1245 para mitigar el spam en multimedios IP.----------

6.7. RECOMENDACIÓN ITU-T X.1246 *"TECNOLOGÍAS IMPLICADAS EN LA LUCHA CONTRA EL SPAM DE VOZ EN LAS ORGANIZACIONES DE TELECOMUNICACIONES".*

La recomendación **ITU-T X.1246** ***"Tecnologías implicadas en la lucha contra el spam de voz en las organizaciones de telecomunicaciones"***, presenta las tecnologías y procesos antispam en voz para las redes de telecomunicaciones con conmutación de circuitos, tanto del lado de la red y como del usuario, así como el mecanismo de colaboración entre ellos. Además, se proponen otras soluciones antispam, como los registros de datos de señalización, la verificación interactiva de sospechosos y medidas de control para restringir el *spam* de voz.----------

Entre las tecnologías que pueden ser implementadas del lado de la red, se mencionan:

- **Recopilación y registro de señalización:** consiste en recopilar los registros detallados de una llamada en tiempo real para ser analizado. Entre los mecanismos mencionados se encuentra la señalización SS7[30] con puntos de recopilación de señalización implantados en la red de forma paralela al enlace de señalización a fin de recopilar los registros de señalización SS7 que contienen datos detallados de las llamadas. También incluye otros métodos como red inteligente y cebos o señuelos para atraer generadores de *spam*. ----------

[30] Conjunto de protocolos de señalización utilizados en redes telefónicas y móviles para establecer llamadas, gestionar SMS, y manejar funciones como la portabilidad numérica y el roaming.

- **Análisis:** revisión de indicadores como frecuencia de llamada, tasa de conexión, tiempo de finalización de llamada, duración de tono y estadísticas de llamado.------
- **Verificación interactiva:** verificación de los números de llamantes que figuren en una lista de sospechosos y pruebas de llamadas hacia números en dicha lista o los determinados por un cebo como *spam*.----------
- **Control:** restringe a los generadores de *spam* de voz confirmados para proteger a los usuarios, con métodos como listas blancas/negras y mecanismos de rastreo. --

Asimismo, esta recomendación señala la importancia de implementar tecnología antispam del lado del usuario como un suplemento eficaz de las tecnologías del lado de la red. Entre las tecnologías que pueden ser implementadas del lado del usuario se encuentran las listas blancas/negras, configuración de umbrales de tiempo para la duración de los tonos de llamada, canales para que los usuarios informen a los operadores sobre *spam* en voz, y colaboración entre operadores y usuarios con sistemas de compartición de la información sobre *spam* de voz, las cuales son detalladas en esta recomendación.----------

6.8. Estándar ATIS-1000105 *"Signature-based Handling of Asserted information using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM"*.

El protocolo STIR/SHAKEN es un gran aliado para la autenticación de llamadas maliciosas realizadas mediante redes IP (VoIP), agregando encabezados robustos que verifican la autenticidad del número llamante mediante certificados digitales. No obstante, esta solución únicamente funciona en entornos donde todas las llamadas transitan en redes IP, ya que, las redes tradicionales de conmutación de circuitos utilizan protocolos en sus comunicaciones que no fueron diseñados en su momento para incluir encabezados robustos como los requeridos por STIR/SHAKEN. Esto provoca conflictos en las llamadas al transitar entre redes IP y redes de conmutación de circuitos, ya que, las redes de conmutación de circuitos al no ser capaces de procesar el encabezado IP con la información de autenticación para STIR/SHAKEN, simplemente lo eliminan. Asimismo, las llamadas legítimas generadas en redes de conmutación de circuitos pueden ser bloqueadas por redes IP que utilicen STIR/SHAKEN dado que dichas llamadas no cuentan con los encabezados de autenticación requeridos.----------

Por lo anterior, la Alianza para Soluciones de la Industria de las Telecomunicaciones, en adelante ATIS (Alliance for Telecommunications Industry Solutions) y el SIP Forum desarrollaron el estándar **ATIS-1000105** ***"Signature-based Handling of Asserted information using Tokens (SHAKEN): Out-of-Band PASSporT Transmission Between Service Providers that Interconnect using TDM"***, el cual propone una alternativa para la autenticación de llamadas que coexisten en entornos de redes IP y conmutación de circuitos. ----------

Dicho estándar establece el Out-of-Band SHAKEN (OOBS) que permite autenticar llamadas incluso cuando atraviesan redes que no soportan encabezados IP. Esto se

logra utilizando dos vías para autenticar la comunicación, de modo que, el certificado que autentica la llamada es enviado por Internet mediante servicios seguros en la nube para la generación de certificados y colocación de llamadas (STI-CPS), en lugar de enviar el certificado en la misma llamada.----------

Para la transición de una llamada entre dichas redes, se genera el certificado de autenticación y los operadores no completarán la comunicación hasta recibir confirmación de autenticidad, por lo que, el uso de OOBS debe disponer de tiempos de espera razonables para la autenticación de llamadas, con el fin de evitar latencias excesivas en el establecimiento de las llamadas. ----------

Además, dicho estándar muestra los esquemas de implementación para los diferentes escenarios que se pueden presentar en la transición de llamadas entre redes IP y de conmutación de circuitos. ----------

6.9. RESOLUCIÓN DE LA REPÚBLICA DE LITUANIA.

La Autoridad Reguladora de las Comunicaciones de la República de Lituania publicó el 25 de enero de 2024 la resolución sobre el procedimiento que deben seguir los operadores para la identificación de mensajes SMS maliciosos *(Resolution on the approval of the description of the procedure for identifying malicious short masajes (SMS))*, donde establece los criterios y procedimientos para identificar mensajes SMS potencialmente maliciosos, según se muestran en los siguientes puntos: ----------

- Los operadores y proveedores deben garantizar que el remitente del contenido SMS o el agregador de SMS puedan especificar atributos de identificación para los SMS enviados mediante identificadores de remitente alfanuméricos o numéricos, permitiendo la identificación del remitente real, como nombre alfanumérico del remitente, número específico, agregador de SMS o red pública de comunicaciones móviles desde la que se inicia el SMS, así como otros atributos de identificación acordados con el proveedor. De modo que, los proveedores solo enviarán a los destinatarios o reenviarán a las redes públicas de comunicaciones móviles de otros operadores los SMS que cumplan con los atributos de identificación acordados. ----------

- Los operadores y proveedores deben identificar el tráfico SMS malicioso que cumpla con al menos uno de los siguientes criterios:----------

  - Los SMS se envían desde operadores extranjeros o agregadores de SMS.-

  - El campo *“Número de remitente”* del SMS contiene un identificador alfanumérico o un número no especificado en el Plan Nacional de Numeración.----------

  - Los SMS se envían a través de navegadores de internet, servicios A2P u otras aplicaciones. ----------

- Los SMS enviados consecutivamente tienen un número idéntico o similar de caracteres.----------

- El intervalo entre envíos de SMS es extremadamente corto, es decir, menor que el tiempo que tarda una persona en escribir y enviar un SMS. ----------

- Se envía una gran cantidad de SMS simultáneamente desde el mismo número o desde varios. ----------

- Se envía la misma cantidad de SMS o una cantidad similar durante uno o varios días consecutivos. ----------

- Los operadores y proveedores tienen la potestad de aplicar otros criterios que indiquen razonablemente que un SMS enviado puede ser malicioso.

- Los operadores y proveedores deben utilizar herramientas de filtrado técnico automatizadas para determinar si los SMS contienen un enlace a un sitio web, en cuyo caso, deberán verificar, mediante herramientas de filtrado técnico automatizadas, si el enlace está incluido en la Lista de Recursos Dañinos administrada por el Centro Nacional de Ciberseguridad del Ministerio de Defensa Nacional de Lituania (NCSC). En caso afirmativo los mensajes deben ser bloqueados inmediatamente. ----------

- Si un mensaje contiene un enlace a un sitio web que no está incluido en la Lista de Recursos Dañinos, dicho SMS se considerará potencialmente malicioso y los Proveedores deberán, de inmediato: ----------

  - Aplicar las medidas técnicas y organizativas adecuadas para advertir a los destinatarios de dichos SMS sobre los mensajes potencialmente maliciosos. ----------

  - Si el operador sospecha que el enlace es perjudicial, puede solicitar al NCSC evaluar su inclusión en la Lista de Recursos Dañinos. ----------

- Los proveedores procesarán y conservarán el contenido, el tráfico y los datos relacionados de los SMS necesarios para identificar SMS maliciosos o potencialmente maliciosos solo en la medida necesaria para llevar a cabo las acciones contempladas en la resolución.----------

- Los proveedores tienen prohibido procesar el contenido, el tráfico y otros datos relacionados de los SMS para fines distintos a los especificados en la resolución. ----------

- Los proveedores deben aplicar medidas técnicas y organizativas que garanticen que el contenido de los SMS, excepto los enlaces a sitios web, no pueda reconstruirse una vez destruido. ----------

7. NORMATIVA COMPARADA SOBRE LAS ESTAFAS POR MENSAJERÍA DE TEXTO (SMS YSUS MODALIDADES) Y SUS OBLIGACIONES DE BLOQUEO.

Con el fin de identificar buenas prácticas regulatorias comparables, se revisaron enfoques recientes en otras jurisdicciones respecto a la mitigación de estafas mediante mensajería móvil (*smishing*) y el uso indebido de identificadores de remitente (alias/CLI). A continuación, se resumen elementos relevantes de España (CNMC y Orden TDF/149/2025), México (IFT), Colombia (CRC) y Perú (marco MTC y actuaciones OSIPTEL). ----------

Tabla 1. Cuadro comparativo de medidas adoptadas por otros países.

Jurisdicción / regulador	Instrumento o referencia	Medidas sobre SMS/estafas	Observaciones
España – CNMC / Ministerio (Orden TDF/149/2025)[31]	Consulta CNMC sobre Registro de alias (2025) y obligaciones de bloqueo desde junio 2026.	Registro de alias (remitente alfanumérico) + bloqueo de mensajes con alias no registrado/no habilitado; medidas contra suplantación por SMS/MMS/RCS.	Incorporar registro/validación de remitentes A2P y reglas de bloqueo por alias/identificador no validado, incluyendo tráfico internacional.
México – IFT[32]	Catálogo de prácticas prohibidas (spam/flooding) y consideraciones sobre SMS con números cortos o remitentes enmascarados.	Definiciones operativas para spam/flooding (umbrales) y controles para evitar abuso; discusión sobre requisitos para habilitar SMS con remitente de marca/alias.	Definir criterios mínimos de detección (umbral/velocidad/volumen) y obligaciones de bloqueo/mitigación para A2P y P2P, con trazabilidad del agregador.
Colombia – CRC[33]	Registro de Números Excluidos (RNE) y acciones regulatorias frente a abuso de comunicaciones; iniciativas sobre fraude cibernético en móviles.	Opt-out para publicidad no deseada; énfasis en identificación del responsable del mensaje y medidas para reducir SMS invasivos y suplantación.	Complementar bloqueo técnico con medidas de preferencia del usuario y obligaciones de identificación del emisor de contenidos.
Perú – MTC / [34]OSIPTEL	Reglas recientes para trazabilidad y uso adecuado de	Enfoque de trazabilidad: bloqueo de comunicaciones con	Refuerza necesidad de controles de origen (numeración

[31] Comisión Nacional de los Mercados y la Competencia (CNMC). (2025). *Consulta pública sobre el registro de alias para la prevención del fraude mediante SMS*. Madrid, España https://www.cnmc.es/consultas-publicas/telecomunicaciones/registro-alias.
[32] Instituto Federal de Telecomunicaciones (IFT). (2024). *Lineamientos y disposiciones en materia de comunicaciones no solicitadas y prevención de prácticas fraudulentas en servicios de telecomunicaciones*. Ciudad de México, México https://www.ift.org.mx/sites/default/files/industria/temasrelevantes/24428/documentos/anteproyectodelineamientosseguridadvozclilimpio.pdf
[33] Comisión de Regulación de Comunicaciones. (2025). *Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles. https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-alternativas-regulatorias-identificacion-medida-fraude-cibernetico-servicios-moviles.pdf.*
[34] Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL). (2024). *Medidas regulatorias para la prevención del fraude mediante llamadas y mensajes SMS*. Lima, Perú. https://www.osiptel.gob.pe/media/nrribtmd/informe087-2025-dapu.pdf

Jurisdicción / regulador	Instrumento o referencia	Medidas sobre SMS/estafas	Observaciones
	numeración en llamadas y SMS; OSIPTEL difunde y supervisa obligaciones asociadas a comunicaciones mediante SMS.	numeración falsa/no asignada o enmascarada; fortalecimiento de control y supervisión.	asignada/consentida) y supervisión con reportes e indicadores de cumplimiento.

En cuanto a los elementos técnicos que caracterizan estas regulaciones sobre la activación de mecanismos normativos regulatorios para mitigar el efecto de las estafas o recepción de mensajería maliciosa se indica lo siguiente:----------

- En todos los casos se observa la combinación de: i) autenticación/validación de identificadores; ii) obligaciones de bloqueo en red; iii) monitoreo y reporte; y iv) coordinación interinstitucional (ciberseguridad, protección al consumidor y seguridad pública). ----------
- Enfoque de trazabilidad de extremo a extremo de las comunicaciones y uso adecuado del recurso numérico para impedir enmascaramiento, con obligaciones de bloqueo por numeración falsa/no asignada y supervisión del cumplimiento (Perú). ----------
- Mecanismos de preferencia del usuario (opt-out) mediante registros de exclusión para mensajes comerciales y medidas para mejorar la identificación del responsable del contenido (Colombia). ----------
- Reglas de buenas prácticas y umbrales cuantitativos para identificar spam/flooding en servicios de mensajería y obligaciones de interconexión/gestión del abuso entre concesionarios (México). ----------
- Registro/validación de alias alfanuméricos: obligación de bloquear mensajes que utilicen alias no inscritos o no habilitados por un proveedor autorizado (España). -

8. ANÁLISIS DE LOS RESULTADOS Y EL ALCANCE DE LA RCS-294-2023.

El establecimiento de las medidas regulatorias definidas en la resolución RCS-294-2023, instruyen a los operadores y proveedores que brindan servicios de telefonía entre otros aspectos a remitir a la Sutel, a partir del año 2024, un reporte cuatrimestral con la cantidad de llamadas que han sido bloqueadas, con el fin de validar su efectividad y el alcance de dichas medidas regulatorias. ----------

Es importante señalar que el alcance de estas medidas regulatorias abarca tanto el servicio de telefonía fija como el de telefonía móvil. Respecto al servicio de telefonía móvil, el mercado consta de 3 operadores (Liberty, Kolbi y Claro), mientras que por su

parte el mercado de telefonía fija consta actualmente de 20 operadores y proveedores que brindan este servicio. ----------

La participación por operador para estos mercados se muestra en las siguientes tablas: ----------

Tabla 2. Participación operadores telefonía fija.

Operadores y proveedores servicio de telefonía fija	Participación en el mercado	Aporta información de llamadas bloqueadas
INSTITUTO COSTARRICENSE DE ELECTRICIDAD	78,077%	Si
LIBERTY TELECOMUNICACIONES DE COSTA RICA LY SOCIEDAD ANONIMA	15,883%	Si
MILLICOM CABLE COSTA RICA S.A.	3,358%	Si
TELECABLE ECONÓMICO T.V.E., S.A.	1,298%	No posee conexión internacional
CALL MY WAY S.A.	0,313%	Si
R & H INTERNATIONAL TELECOM SERVICES S.A.	0,216%	Si
CLARO CR TELECOMUNICACIONES, S.A.	0,162%	Si
BLUE SAT SERVICIOS ADMINISTRADOS DE TELECOMUNICACIONES S.A.	0,157%	No
COOPERATIVA ELECTRIFICACION RURAL DE GUANACASTE	0,145%	No posee conexión internacional
AMERICAN DATA NETWORKS	0,125%	No
INTERPHONE S.A.	0,122%	No posee conexión internacional
RING CENTRALES DE COSTA RICA, S.A.	0,075%	Si
NAVEGALO S.A.	0,027%	No posee conexión internacional
COMUNICACIONES METROPOLITANAS METROCOM, S.A.	0,021%	No posee conexión internacional
GCI SERVICE PROVIDER S.A.	0,016%	No posee conexión internacional
COSTA RICA INTERNET SERVICE PROVIDER S.A. (CRISP)	0,004%	No
SERVICIOS TECHNOLOGICOS ANTARES DE COSTA RICA	0,001%	No
DIDWW CR SOCIEDAD ANONIMA	0,000%	Si
P.R.D. INTERNACIONAL, S.A.	0,000%	No
REDES INTEGRADAS CORPORATIVAS LIMITADA	0,000%	No

Tabla 3. Participación operadores telefonía móvil

Operadores y proveedores servicio de telefonía fija	Participación en el mercado	Aporta información de llamadas bloqueadas
INSTITUTO COSTARRICENSE DE ELECTRICIDAD	37%	Si
LIBERTY TELECOMUNICACIONES DE COSTA RICA LY SOCIEDAD ANONIMA	40%	Si
CLARO CR TELECOMUNICACIONES, S.A.	23%	Si

Cabe mencionar que los reportes sobre bloqueo de llamadas remitidos por los operadores que brindar servicios tanto móviles como fijos los brindaron de manera conjunta incluyendo ambos servicios ----------

De la información obtenida de estos reportes cuatrimestrales remitidos por los operadores desde la implementación de la normativa en el mes de febrero del año 2024, se extrae la siguiente tabla en la cual se resume la cantidad total de llamadas bloqueadas por cada operador y el porcentaje representativo del total reportado.----------

Tabla 4. Reporte de llamadas bloqueadas por operador.

OPERADOR	TOTAL, DE LLAMADAS BLOQUEADAS	PORCENTAJE DEL TOTAL DE LLAMADAS BLOQUEADAS
ICE	10 861 879	70,17%
CallMyWay NY S.A.	2 239 524	14,47%
Claro CR Telecomunicaciones S.A.	2 207 198	14,26%
Liberty Telecomunicaciones Móviles LY, S.A.	167 374	1,08%
R&H International Telecom Services, S.A.	1333	0,01%
Millicom Cable de Costa Rica S.A.	1 099	0,01%
DIDWW CR S.A.	0	0,00%
Ring Centrales de Costa Rica S.A.	0	0,00%
TOTAL	**15 478 407**	**100,00%**

A partir de los datos recopilados, es de relevancia indicar que: ----------

- El Instituto Costarricense de Electricidad como operador con mayor participación en el mercado en telefonía fija y el segundo en telefonía móvil, es el operador con mayor número de llamadas bloqueadas, concentrando un 70,17% del total de llamadas bloqueadas. ----------

- El operador CallMyWay NY S.A a pesar de poseer una cuota de participación de 0.33% en el mercado de telefonía fija, se posiciona como el segundo operador con mayor cantidad de llamadas bloqueadas reportadas, representado un 14,47% del total.----------

- La empresa Ring Centrales de Costa Rica S.A. y DIDWW CR S.A., aunque remitieron reportes, no reportaron bloqueo de llamadas en sus redes durante el periodo análizado.----------

- El operador Liberty Telecomunicaciones Móviles LY, S.A., a pesar de contar la mayor cuota de participación en el mercado de telefonía móvil y la segunda cuota de participación en el mercado de telefonía fija, reportó únicamente un 1,08% del total de llamadas bloqueadas.----------

- Del total de operadores que brindan el servicio de telefonía fija, 8 operadores remitieron los reportes correspondientes, 6 operadores indicaron que no contar con conexión internacional directa, y 6 operadores no remitieron los reportes solicitados.

- Los tres operadores del servicio de telefonía móvil remitieron sus respectivos reportes de correspondientes concentran un aproximando de un 85.51% del total de llamadas bloqueadas reportadas a esta Superintendencia.----------

9. SOBRE LA REGULACIÓN PROPUESTA

Con base en los puntos expuestos anteriormente y con el objetivo de garantizar la seguridad de los usuarios finales y las redes de los operadores, se somete a valoración del Consejo de Sutel las siguientes medidas para requerir a la totalidad de operadores y proveedores de servicios de telecomunicaciones identificar y bloquear el tráfico malicioso en sus redes:

9.1. 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) [35] 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[36] 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 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

[35] 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.
[36] 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.

SimBoxes o cualquier otro equipo que enmascare o simule tráfico A2P como P2P.----------

6. Uso de Inteligencia Artificial con Procesamiento de Lenguaje Natural (NLP)[37] para detectar variaciones en la ortografía del mensaje o el uso de caracteres especiales para evadir filtros. Además, realizar Análisis Heurístico[38] 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)[39].----------

11. Identificación de campañas de smishing mediante:

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

[37] Uso de la Inteligencia Artificial para que las computadoras puedan entender, interpretar, manipular y generar lenguaje humano, tanto en texto como en voz.
[38] 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.
[39] 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.

12. Detección de ráfagas de spam (Spam Burst)[40] 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[41].----------

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. ----------

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 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.----------

[40] 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.
[41] Aplicaciones o software automatizados programados para realizar tareas repetitivas, predefinidas y rápidas sin intervención humana.

9.2. 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: ----------

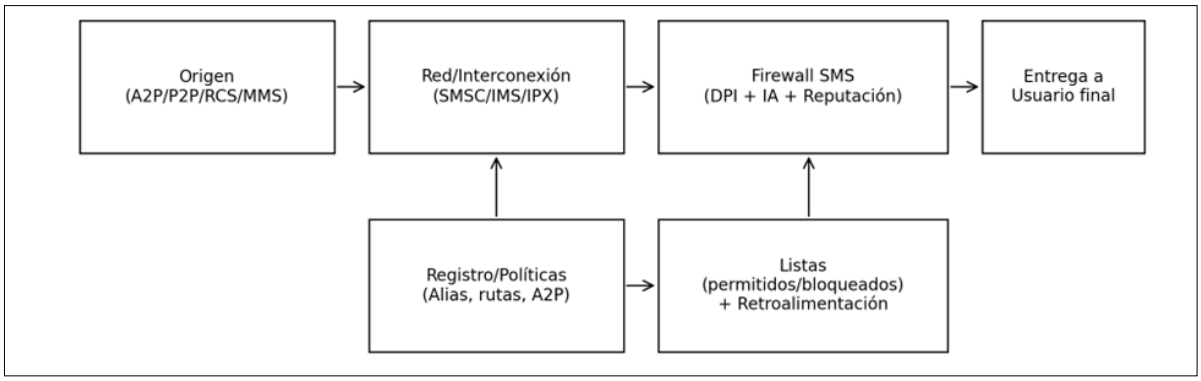

Imagen 9. Diagrama de implementación para filtrado o bloqueo de SMS P2P y A2P.

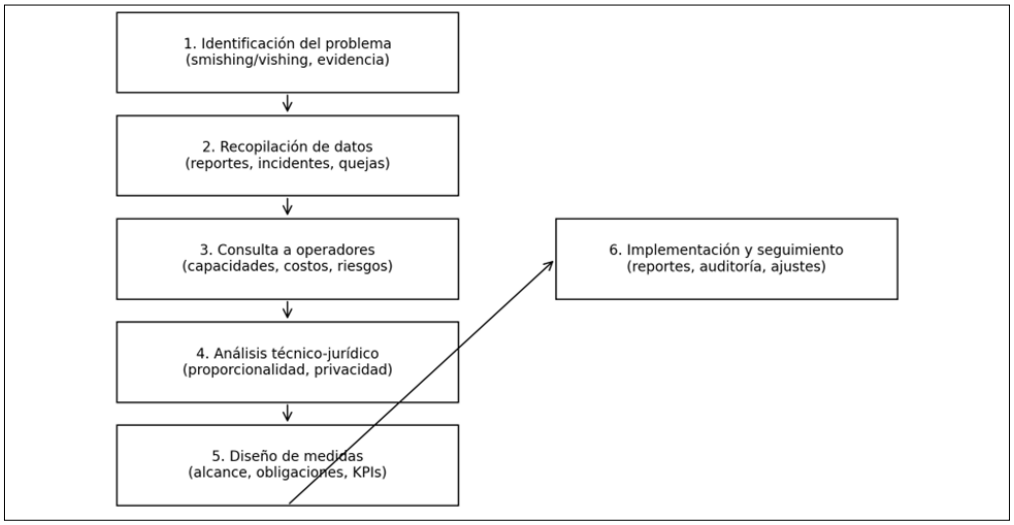

Imagen 10. Diagrama de metodología regulatoria para filtrado o bloqueo de SMS P2P y A2P.

9.3. 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 deben establecer registros de las entidades desde las cuales se envía y recibe tráfico de SMS A2P. Este registro será actualizado con el ingreso o retiro de una entidad emisora de mensajes SMS A2P, donde se indique el nombre de la empresa y el segmento de numeración que hace uso. Además, esta Superintendencia podrá consultar a los operadores y proveedores dichos registros de generadores de mensajes SMS A2P. ----------

9.4. 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: ----------

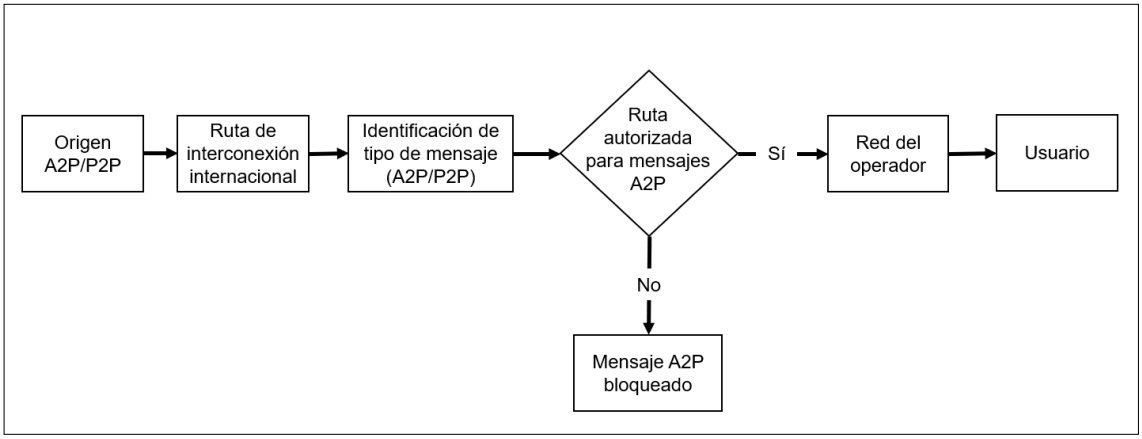

Imagen 11. Diagrama de implementación para bloqueo de SMS A2P por rutas de interconexión internacional.

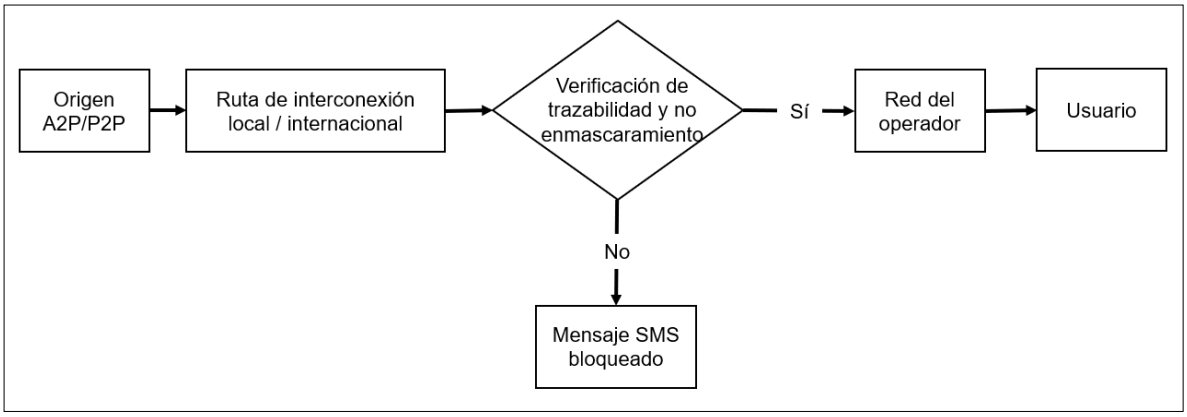

Imagen 12. Diagrama de implementación para bloqueo de SMS que no permiten trazabilidad o se encuentra enmascarado.

9.5. 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)[42] 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 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. ----------

[42] Call Detail Records.

C. Los operadores y proveedores deben disponer de medios de atención al público para que los usuarios finales 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".* ----------

9.6. SOBRE EL PLAZO DE IMPLEMENTACIÓN.

A. Otorgar el plazo de 180 días naturales a los proveedores y operadores con numeración asignada por esta Superintendencia, una vez publicada la presente metodología regulatoria en el diario Oficial La Gaceta para que se proceda a su implementación, plazo en el cual, deberán realizar las configuraciones necesarias a nivel de sus sistemas para proceder con los ajustes técnicos e implementación de las medidas regulatorias dispuestas en los apartados "***9.1.SERVICIOS DE MENSAJERÍA DE TEXTO SMS P2P y A2P; .9.2. ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS P2P Y A2P.; 9.3. SERVICIOS DE MENSAJERÍA DE TEXTO SMS A2P y 9.4. ESQUEMA DE IMPLEMENTACIÓN DE BLOQUEO Y METODOLOGÍA REGULATORIA PARA MENSAJERÍA SMS A2P"***.----------

10. CONCLUSIONES

10.1. El establecimiento de las medidas regulatorias definidas en la resolución RCS-294-2023, específicamente el bloqueo generalizado de llamadas internacionales entrantes con prefijos nacionales ha generado un impacto importante dado la cantidad de llamadas que han sido bloqueadas desde su implementación.

10.2. Según el análisis de regulación comparada y recomendaciones internacionales, es necesaria la implementación de una regulación complementaria que establezca disposiciones para la gestión del tráfico SMS con el fin de garantizar la seguridad de los usuarios, evitando prácticas como el "*smishing*" entre otras.

11. RECOMENDACIONES

11.1. RECIBIR Y APROBAR el informe 02238-SUTEL-DGM-2026 de fecha del 06 de marzo del 2026.

11.2. MANTENER las medidas regulatorias definidas en la resolución administrativa RCS-294-2023.

11.3. ADOPTAR la propuesta regulatoria dispuesta en el ***APARTADO 9*** del oficio número 02238-SUTEL-DGM-2026 del 06 de marzo del 2026, para su consulta pública con los operadores y proveedores de servicios de telecomunicaciones.

11.4. INSTRUIR a la Secretaría del Consejo a realizar el respectivo proceso de publicación y consulta pública conforme a lo dispuesto en los artículos 240 y 361 de la Ley General de Administración Pública, Ley N°6227 y atender conjuntamente las observaciones derivadas a la consulta pública.

11.5. INSTRUIR a la Dirección General de Mercados y a la Dirección General de Calidad atender las objeciones y observaciones que se presenten producto del proceso de consulta pública y plantear una propuesta final de resolución al Consejo.

Atentamente,
SUPERINTENDENCIA DE TELECOMUNICACIONES

DERYHAN MUÑOZ BARQUERO (FIRMA)
PERSONA FISICA, CPF-06-0328-0822.
Fecha declarada: 06/03/2026 11:55:24 a. m.

Deryhan Muñoz Barquero
Directora General
Dirección General de Mercados

GLENN FALLAS FALLAS (FIRMA)
Firmado digitalmente por GLENN FALLAS FALLAS (FIRMA)
Fecha: 2026.03.06 11:25:01 -06'00'

Glenn Fallas Fallas
Director General
Dirección General de Calidad

JUAN GABRIEL GARCIA RODRIGUEZ (FIRMA)
Firmado digitalmente por JUAN GABRIEL GARCIA RODRIGUEZ (FIRMA)
Fecha: 2026.03.06 11:57:42 -06'00'

Juan Gabriel García Rodriguez
Jefe, Dirección General de Mercados

CESAR GUSTAVO VALVERDE CANOSSA (FIRMA)
Firmado digitalmente por CESAR GUSTAVO VALVERDE CANOSSA (FIRMA)
Fecha: 2026.03.06 11:06:40 -06'00'

Cesar Valver Canossa
Jefe, Unidad de Calidad de Redes

JOSUE CARBALLO HERNANDEZ (FIRMA)
Firmado digitalmente por JOSUE CARBALLO HERNANDEZ (FIRMA)
Fecha: 2026.03.06 10:02:58 -06'00'

Josué Carballo Hernández
Dirección General de Mercados

JOSE ALFONSO SANCHEZ SAENZ (FIRMA)
Firmado digitalmente por JOSE ALFONSO SANCHEZ SAENZ (FIRMA)
Fecha: 2026.03.06 11:29:52 -06'00'

José Alfonso Sánchez Sáenz
Dirección General de Calidad

YORLENY ROJAS LOPEZ (FIRMA)
Firmado digitalmente por YORLENY ROJAS LOPEZ (FIRMA)
Fecha: 2026.03.06 11:37:49 -06'00'

Yorleny Rojas López
Dirección General de Mercados

JUAN PABLO GUZMAN FERNANDEZ (FIRMA)
Firmado digitalmente por JUAN PABLO GUZMAN FERNANDEZ (FIRMA)
Fecha: 2026.03.06 11:32:30 -06'00'

Juan Pablo Guzmán Fernández
Dirección General de Mercados

Exp: GCO-DGM-IET- 00518-2026