



Bogotá D.C., 23 de junio de 2026.

Doctor

FELIPE AUGUSTO DÍAZ SUAZA

Director Ejecutivo

COMISIÓN DE REGULACIÓN DE COMUNICACIONES – CRC

Calle 59 A bis No. 5-53, Edificio Link Siete Sesenta P9

Bogotá D.C.

Asunto: Comentarios de TIGO al proyecto de resolución *“por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones”* – Proyecto regulatorio 2000-41-7-1.

Respetado Doctor Díaz:

En atención a la consulta pública adelantada respecto del proyecto de resolución del asunto, desde **TIGO** agradecemos a la Comisión la oportunidad de comentar y reconocemos el riguroso ejercicio técnico que sustenta esta iniciativa. El fraude cibernético es hoy un fenómeno estructural y creciente: de acuerdo con la información que la propia Comisión recogió en el documento soporte, el valor de las reclamaciones por smishing y vishing pasó de cerca de \$30.622 millones en 2022 a \$92.235 millones en 2024 —prácticamente se triplicó en dos años—, con un crecimiento particularmente acelerado del smishing, cuyo principal vector de contacto es el mensaje de texto. Este fenómeno afecta gravemente a los usuarios, al sistema financiero y a los propios PRST, que también somos víctimas dentro de la cadena de valor.

Por ello, TIGO respalda el propósito del proyecto y considera necesario medidas para prevenir y atacar este fenómeno. Valoramos especialmente que la Comisión haya recogido las observaciones de las fases previas y que, para el tráfico A2P, haya estructurado un ecosistema de trazabilidad —SENDER ID por marca, código corto A2P único por agente con conexión directa, conocimiento del cliente (KYC), plantillas de contenido y validador centralizado— que ataca la causa estructural del problema: la imposibilidad de atribuir responsabilidad sobre el originador real del mensaje. Consideramos que esta es la línea adecuada y que el validador centralizado, con un seguimiento y un financiamiento bien diseñados, es el esquema correcto.

No obstante, para que el proyecto sea efectivo, proporcional y sostenible, respetuosamente solicitamos a la CRC que se atiendan cuatro ejes: (i) que el nuevo régimen A2P venga acompañado de la desregulación de la tarifa mayorista del SMS A2P, condición necesaria y anterior para financiar las inversiones que el propio proyecto exige; (ii) que los plazos de implementación se amplíen a un mínimo de doce (12) meses, en línea con el alcance técnico real de las medidas reconocido por la propia Comisión; (iii) que las medidas de voz se replanteen bajo criterios de proporcionalidad y costo-eficiencia, trasladando las cargas a los agentes que originan y transportan el tráfico irregular —originadores y carriers internacionales— y no al PRST terminante; y (iv) que el nuevo esquema asegure la debida remuneración de la red y preserve la continuidad en la entrega de los mensajes legítimos, sin imponer cargas desproporcionadas sobre el tráfico de voz cursado en las redes de los PRST; a continuación desarrollamos estos puntos.



I. COMENTARIOS GENERALES

1. El régimen A2P debe venir acompañado de la desregulación de la tarifa mayorista del SMS A2P

La CRC ya dio un primer paso relevante al separar la discusión del SMS A2P del tráfico P2P y trasladar a este proyecto el análisis de la remuneración. Ese movimiento es acertado y reconoce que el A2P no es mensajería entre usuarios, sino un insumo corporativo (B2B) utilizado por bancos, plataformas digitales, comercios, entidades públicas y agregadores para autenticación, alertas, notificaciones transaccionales y comunicaciones masivas. Recordamos que, mientras el SMS P2P se ajustó a tres centavos de peso en el proyecto de remuneración móvil, el SMS A2P se mantuvo en un peso de 2022 a la espera de este proyecto, y que la Resolución CRC 8183 de 2026 remitió expresamente la revisión tarifaria integral del A2P a esta actuación, anunciando que la decisión se adoptaría con posterioridad.

La estructura económica, técnica y de riesgo del A2P es distinta a la del P2P: exige integración con APIs, gestión de capacidad y reservas de transacciones por segundo (TPS) para sostener picos de tráfico, control de ráfagas, trazabilidad de inicio a fin, firewalls antifraude, filtros antispam, soporte operativo permanente y acuerdos comerciales con PCA/IT y agregadores. El propio documento soporte reconoce que el tráfico A2P presenta volúmenes mayores y necesidades de entrega más exigentes que el P2P. Además, es un mercado sometido a fuerte presión competitiva de canales sustitutos como WhatsApp Business, RCS, notificaciones push, soft tokens, correo electrónico y los canales propios de las aplicaciones, lo que acota cualquier riesgo de poder de mercado y hace innecesaria la regulación tarifaria ex ante.

Las medidas planteadas para mitigar el fraude a través de SMS y servicios de voz implican inversiones cuantiosas, permanentes y especializadas por parte de los operadores. Su implementación requiere plataformas de monitoreo en tiempo real, herramientas de detección de patrones anómalos, firewalls de mensajería, capacidades de bloqueo preventivo, trazabilidad de origen y destino, integración con bases de datos, ajustes en sistemas de interconexión, fortalecimiento de equipos operativos, mecanismos de reporte y procesos de auditoría. Estos desarrollos generan costos de inversión inicial, licenciamiento, mantenimiento, personal especializado y actualización continua, especialmente en un entorno en el que las modalidades de fraude evolucionan rápidamente y exigen capacidades dinámicas de detección y respuesta.

Este esfuerzo recae sobre líneas de servicio que enfrentan condiciones económicas cada vez más restrictivas. En el caso del SMS, la existencia de una tarifa regulada limita la posibilidad de reflejar en el precio los costos reales de prestación, operación, seguridad y modernización del servicio, lo que genera márgenes mínimos frente a una estructura de costos creciente. En el caso de la voz tradicional, el mercado se encuentra en una tendencia estructural de declive por la sustitución hacia servicios OTT, aplicaciones de mensajería, llamadas sobre internet y otros canales digitales. En consecuencia, la CRC estaría imponiendo nuevas obligaciones de inversión sobre productos con menor capacidad de generar retornos suficientes para financiarlas. Desde una perspectiva económica, cuando la regulación incrementa significativamente los costos de operación y cumplimiento de un servicio sin habilitar mecanismos adecuados de recuperación, se reducen los incentivos para mantener, modernizar o ampliar esa línea de negocio, lo que puede traducirse en menor inversión futura, despriorización tecnológica, deterioro gradual de la calidad o restricciones en la oferta comercial.

En este contexto, la desregulación tarifaria del mercado SMS A2P permitiría generar una señal económica más adecuada para sostener las inversiones exigidas por el nuevo régimen de mitigación del fraude cibernético. A diferencia del SMS P2P y de la voz tradicional, el A2P corresponde a un servicio corporativo B2B con mayor valor agregado, mayores exigencias de calidad, trazabilidad, seguridad, integración y

capacidad, y con dinámicas comerciales distintas frente a bancos, plataformas digitales, comercios, entidades públicas, agregadores e integradores. Permitir la libre negociación de tarifas y capacidades en este mercado facilitaría que los operadores recuperen parte de las inversiones requeridas en firewalls, monitoreo, filtros antifraude, analítica, integración y soporte operativo, evitando que dichas obligaciones deban financiarse exclusivamente con servicios regulados, de bajo margen o en declive. Por ello, la desregulación del SMS A2P no debe entenderse únicamente como una medida de eficiencia comercial, sino como un mecanismo necesario para alinear la política regulatoria antifraude con la sostenibilidad económica de las redes y plataformas que la soportan.

Mantener una tarifa A2P regulada ex ante genera una señal económica equivocada: reduce los ingresos que permiten financiar las plataformas de mensajería, la capacidad adicional, el monitoreo permanente y, precisamente, las herramientas antifraude y los desarrollos de integración que este mismo proyecto exige; y transfiere rentas a los eslabones aguas arriba —PCA, integradores y plataformas globales— sin garantía de traslado al usuario final ni a las empresas que utilizan el servicio. Existe, por tanto, una incoherencia que conviene resolver: no es razonable imponer al PRST nuevas obligaciones de inversión e integración mientras se congela la remuneración del insumo que debe financiarlas. La sostenibilidad del canal A2P y la viabilidad misma de las inversiones antifraude requieren libertad tarifaria y negociación de capacidades.

Por lo anterior, TIGO solicita que la CRC avance hacia la desregulación tarifaria del SMS A2P, sustituyendo el esquema de tarifa regulada ex ante por un modelo de libre negociación comercial entre PRST, PCA/IT, integradores y originadores de tráfico, con intervención regulatoria únicamente en caso de controversia o de conductas abusivas. Idealmente, esta definición debería ser concomitante con la entrada en vigencia del nuevo régimen A2P, de modo que las obligaciones de inversión y la señal de remuneración queden alineadas en el tiempo.

2. Los plazos de implementación deben ampliarse a un mínimo de 12 meses

El proyecto prevé un período de transición de seis (6) meses contados a partir de la resolución de remuneración, estructurado en cuatro fases, con una **selección del validador limitada a 54 días** (artículos 18 y 19). Estos plazos son insuficientes frente al alcance real de las medidas, y la propia Comisión aporta los elementos que lo demuestran.

En efecto, el documento soporte reconoce que las plataformas de mensajería (SMSC) hoy desplegadas no cuentan con APIs ni interfaces para la administración dinámica del código corto —su parametrización es manual, gestionada como cambios controlados sobre el Core con SLA cercanos a tres días hábiles— y que no incorporan mecanismos nativos de autenticación criptográfica ni de validación centralizada. La consecuencia, expresada por la propia CRC, es que cualquier implementación de un modelo centralizado requeriría desarrollos específicos, integración de APIs externas y adecuaciones sobre las plataformas SMSC y los motores de enrutamiento. Es decir, no se trata de parametrizar lo existente, sino de desarrollar e integrar capacidades nuevas en sistemas críticos de red.

A ello se suma una secuencia de hitos concatenados y dependientes de terceros: **(i)** seleccionar y contratar al validador centralizado; **(ii)** que este se constituya, integre y active sus APIs; **(iii)** que los PRST y los asignatarios de código corto realicen las adecuaciones técnicas, las integraciones por APIs y el redimensionamiento que demande concentrar el tráfico en un único código corto por agente; **(iv)** registrar y aprobar plantillas y adelantar pruebas de integración en entornos no productivos; y **(v)** consolidar y migrar la numeración existente sin afectar a los usuarios. Cada uno de estos hitos toma tiempo y la falla o demora de cualquiera de ellos —en particular la del tercero que opere como validador— arrastra a toda la cadena.

Existe, además, incertidumbre técnica relevante que hoy impide dimensionar con certeza el esfuerzo: no está definido aún el detalle de arquitectura para la interoperabilidad de las APIs, los tiempos de respuesta ni cómo se garantizaría la disponibilidad exigida en condiciones de alta demanda. Por estas razones, solicitamos que el período de transición y la entrada en vigencia plena del régimen A2P no sea inferior a dieciocho (12) meses, con fases que prevean márgenes razonables para contratación, desarrollo, integración y pruebas, y que se evite encadenar hitos críticos en ventanas de pocos días.

3. Necesidad de especificidad de flujo operativo de validación de mensajes

TIGO respalda el modelo de establecer un identificador (SENDER ID) por marca, código corto A2P único por agente y validador centralizado, por cuanto mejora la trazabilidad de inicio a fin y la atribución de responsabilidades, y resulta más costo-eficiente que esquemas dependientes de validaciones contractuales dispersas. Su diseño guarda similitud con el de la base de datos administrativa de portabilidad numérica (BDO), modelo neutro y probado en el país; recomendamos incorporar, en lo pertinente, sus reglas de gobernanza, neutralidad, niveles de servicio que han funcionado satisfactoriamente. Asimismo, consideramos que el modelo de financiamiento es el adecuado.

No obstante, la implementación debe resolver de manera previa aspectos técnicos hoy indefinidos que tienen impacto directo en la operación y el dimensionamiento de la red: la forma de interacción del validador con el flujo de mensajes y su efecto sobre la señalización y los tiempos de establecimiento; la especificación de las APIs seguras; el plan de contingencia ante indisponibilidad del validador; el funcionamiento con tráfico bidireccional entre el PCA y el usuario final, y la capacidad (TPS) que demanda concentrar el tráfico de múltiples marcas en un único código corto por agente. Este último punto es crítico: hoy la capacidad se asigna y se dimensiona por relación de acceso, y la consolidación en un único código no debe traducirse en cuellos de botella que retrasen o impidan la entrega oportuna de los mensajes —en particular los de autenticación y transaccionales, donde la inmediatez es esencial—.

4. Cobertura completa del riesgo y preservación de la facultad de negociar capacidad

La diferenciación de roles —integrador tecnológico, PCA, código corto A2P único por agente y SENDER ID por marca— clarifica las responsabilidades de cada actor y representa un cambio de paradigma positivo: traslada el control riguroso del acceso a la red de los PRSTM a un único código por agente, y a partir de allí ordena la cadena hacia quien genera el contenido. Sobre esta base, formulamos dos precisiones.

(a) Cobertura completa del riesgo — numeración no geográfica E.164. Las medidas se concentran en los códigos cortos, pero la numeración no geográfica (numeración larga E.164) asignada a algunos PCA también puede emplearse para cursar tráfico de mensajería y, por tanto, para fraude; ambos recursos son sustituibles para estos fines. Si el régimen no aborda en paralelo esta numeración, los agentes que requieran más recursos —o que pretendan eludir el nuevo control— podrían migrar hacia ese canal menos regulado, reabriendo el círculo que el proyecto busca cerrar. Solicitamos que se deje claro la extensión del régimen de trazabilidad, KYC y control a la numeración E.164 no geográfica utilizada para SMS, o disponer su devolución y la restricción de su uso para mensajería A2P.

(b) Preservación de la facultad de negociar capacidad. El nuevo esquema debe asegurar la debida remuneración de la red y preservar expresamente la facultad de los PRST de ofrecer y cobrar servicios de dimensionamiento y capacidad adicional que la regulación (Res 6522 de 2022) hoy permite negociar (por ejemplo, servicios adicionales). Dentro de la preservación de la facultad de negociar recursos adicionales de

red para la gestión del tráfico, deberán tenerse en cuenta, de manera independiente, aquellos destinados a la validación centralizada.

5. Las medidas de voz deben replantearse bajo criterios de proporcionalidad y costo-eficiencia

5.1. El mercado de voz móvil en Colombia se encuentra claramente en la fase de declive del ciclo de vida utilizado por la CRC

La etapa de introducción y crecimiento ocurrió antes de 2011, cuando se expandieron las redes y la penetración; entre 2011 y 2014 el mercado entró en madurez, con líneas aun creciendo, pero tráfico prácticamente estancado e ingresos ya descendiendo. Entre 2015 y 2020 se produjo una madurez avanzada marcada por la comoditización: el tráfico aumentó 69,3%, pero los ingresos cayeron 58,1% y el ingreso promedio por minuto se redujo 75,3%, evidencia de que la voz dejó de monetizarse como producto independiente y pasó a incluirse en paquetes móviles. Desde 2020, el declive es estructural e inequívoco: aunque las líneas aumentaron 41,3%, de 67,7 a 95,6 millones, el tráfico cayó 49,8%, de 175,3 a 88,1 mil millones de minutos, y los minutos mensuales por línea disminuyeron 64,7%, de 220,9 a 77,9. A su vez, los ingresos de voz bajaron 37,2% desde 2020 y acumulan una caída de 78,7% frente al máximo de 2012, mientras el ingreso mensual de voz por línea se redujo 88,9% desde 2011. En este contexto, resulta poco eficiente trasladar nuevas cargas al PRST terminante, que no controla el origen del fraude y que ha visto disminuidos sus ingresos.

El declive del mercado de VOZ móvil es claramente estructural, sistemático y acelerado en Colombia, derivado de una sustitución tecnológica natural hacia los servicios de datos móviles y aplicaciones OTT (Over-The-Top). Obligar a los PRSTM a ejecutar cuantiosas inversiones en CAPEX y a asumir altos costos fijos de OPEX para adaptar plataformas complejas sobre un canal en desuso, configura un escenario de ineficiencia económica y destrucción de valor sectorial.

Además, conviene precisar el punto de partida técnico. Los PRSTM ya operan capacidades antifraude en voz —plataformas y motores de reglas, monitoreo de tráfico en tiempo real sobre núcleos IMS y elementos SIP/SBC, correlación de CDR y metadatos, e indicadores como CAPS y ACD— que hoy cumplen la obligación regulatoria de disponer de herramientas tecnológicas adecuadas. El punto, por tanto, no es que carezcamos de herramientas, sino que el modelo propuesto exige inversiones y desarrollos adicionales significativos sobre esas plataformas para soportar obligaciones nuevas (validación frente al RNE en línea, ampliación de patrones, etiquetado y verificación de identidad CLI), en un mercado de voz móvil en fase decreciente. En ese contexto, el modelo impone costos elevados sobre las redes de los PRST sin un impacto proporcional en la mitigación del fraude, que en buena medida se origina y se controla fuera del PRST terminante.

5.2. Confusión de Capas Arquitectónicas: El Etiquetado como Función Exclusiva de la Capa de Aplicación

La inviabilidad económica descrita se ve agravada por un error de concepto fundamental en la arquitectura técnica de la propuesta: la pretensión de regular el core de telecomunicaciones para obligar a los operadores a ejecutar el etiquetado informativo de llamadas ("Llamada de origen publicitario", "Sospecha de fraude").

El procesamiento, la interfaz visual (UI) y la renderización de las etiquetas en la pantalla de un dispositivo móvil ocurren estrictamente a nivel de la capa de aplicación. Esta capa es gestionada de manera exclusiva por los desarrolladores de sistemas operativos (Google Android, Apple iOS) y por aplicaciones especializadas de gestión de contactos de terceros. El desarrollo, mantenimiento y actualización de aplicaciones de usuario

final no es, bajo ninguna circunstancia, del resorte, competencia ni capacidad técnica de los PRST ni de los elementos de su red CORE (IMS, SBC, etc.).

Para que el CORE de un operador pudiese inyectar y garantizar la visualización de una etiqueta enriquecida en el terminal, se requeriría obligar a la industria a desarrollar e instalar aplicaciones propietarias en el 100% de los terminales del país para desplazar las interfaces de llamada nativas, lo cual alteraría las condiciones de competencia y la homologación internacional de equipos; o en su defecto, pretender de forma inviable que los protocolos de señalización de red (SIP/ISUP) fueren la modificación del código fuente de sistemas operativos globales.

La CRC no puede imponer una obligación de resultado a los PRST cuando las herramientas para lograrlo dependen enteramente de terceros actores globales de software que están fuera de la jurisdicción del regulador y del control técnico de los operadores. Intentar que las redes de telecomunicaciones asuman funciones de desarrollo de software aplicativo desnaturaliza el rol de los PRST como proveedores de infraestructura y transporte, configurando una obligación materialmente imposible de cumplir.

5.3. Etiquetado de llamadas con fines publicitarios y validación frente al RNE (artículo 2.1.10.7.2.2.2.1)

Frente a la propuesta contenida en el artículo 2.1.10.7.2.2.2.1, reiteramos que la obligación de etiquetar llamadas con fines publicitarios debe ser revisada desde su viabilidad técnica. En los servicios tradicionales de voz, el PRST no controla integralmente la forma en que una etiqueta será presentada en el dispositivo del usuario final, la cual se hace en la capa de aplicación del modelo OSI. La visualización de una advertencia o de una categoría de llamada depende de elementos que no están bajo control exclusivo del operador, como las capacidades del terminal, el sistema operativo, la interoperabilidad con otras redes y las funcionalidades habilitadas por fabricantes o terceros.

Adicionalmente, consideramos que la obligación de bloquear llamadas publicitarias por una supuesta validación frente al RNE excede el alcance de la Ley 2300 de 2023 y desnaturaliza el rol del PRST. Dicha ley regula la contactabilidad comercial y publicitaria entre productores o proveedores de bienes y servicios y los consumidores, por lo que la carga de consultar el RNE, depurar las bases de datos, verificar autorizaciones y definir si una campaña puede ejecutarse recae en quien origina la comunicación y conoce su finalidad, destinatarios, base legal y autorizaciones aplicables.

Trasladar al PRST la obligación de verificar, llamada a llamada, si el destinatario está inscrito en el RNE y, con base en ello, bloquear la comunicación, implica imponerle una función material de vigilancia, calificación jurídica y restricción de comunicaciones que corresponde al originador de la campaña y, en caso de incumplimiento, a las autoridades competentes. El PRST no cuenta con información suficiente para determinar si una llamada es publicitaria, transaccional, de servicio, solicitada por el usuario, autorizada con posterioridad a la inscripción en el RNE o amparada en alguna excepción legal. En consecuencia, la medida puede generar bloqueos indebidos de comunicaciones legítimas y afectar derechos de usuarios y empresas, sin una relación directa y proporcional con la prevención del fraude cibernético.

5.4. Monitoreo y filtrado en tiempo real (artículo 2.1.10.7.2.2.2)

Reiteramos que existen limitaciones técnicas relevantes para que el etiquetado de llamadas pueda visualizarse como una advertencia efectiva en el dispositivo del usuario final. La presentación de una etiqueta, alerta o categoría durante la llamada no depende exclusivamente del PRST, sino de factores externos a su control.

Por otra parte, el análisis de patrones durante el establecimiento de la llamada supone una carga técnica y operativa significativa. La detección en tiempo real de comportamientos como llamadas cortas, volúmenes atípicos, marcación secuencial, suplantación o tráfico anómalo exige capacidades avanzadas de procesamiento, correlación y parametrización, cuyo despliegue puede ser complejo, costoso y no necesariamente uniforme entre redes.

Por lo anterior, consideramos que la propuesta no debería exigir la concurrencia de un número mínimo de patrones ni imponer una metodología cerrada de análisis. La regulación vigente reconoce el uso de herramientas tecnológicas para la gestión y prevención de prácticas irregulares, pero no establece una tipología obligatoria ni predeterminada de patrones que deban ser aplicados en todos los casos. En esa medida, la nueva disposición debería preservar la flexibilidad técnica del PRST para definir, según la arquitectura de su red, la información disponible y sus capacidades operativas, los criterios más adecuados para identificar riesgos.

En lugar de condicionar la actuación del operador a la verificación de múltiples patrones simultáneos, sugerimos que la norma permita el uso de al menos uno de los criterios mínimos de análisis. Este enfoque permite avanzar en la mitigación del fraude sin imponer cargas desproporcionadas y sin restringir la innovación en herramientas de detección.

5.5. Enmascaramiento del CLI y STIR/SHAKEN (artículo 2.1.10.7.2.2.1 y concordantes)

El enmascaramiento se origina y puede modificarse en el origen, fuera del control del PRST terminante. El propio documento soporte constata que en Colombia no existen hoy implementaciones activas de STIR/SHAKEN, que no es un estándar de uso global —en el benchmark internacional aparece principalmente en países como Brasil, Canadá y Estados Unidos, mientras la mayoría privilegia el bloqueo de llamadas internacionales con numeración local y las listas DNO— y que no es compatible con las redes tradicionales (SS7/ISUP) sin adaptadores, por lo que su efectividad depende de los originadores y de los carriers internacionales. En consecuencia, las obligaciones en voz deben asignarse principalmente a los carriers internacionales y a los originadores del tráfico, sin recargar al último eslabón de la cadena.

Como la misma Comisión lo reconoce explícitamente en la Sección 11 del documento soporte (Limitaciones y sensibilidad del modelo), la "Migración a redes full IP reduce costos de STIR/SHAKEN". Este reconocimiento técnico constituye el eje central de nuestra postura: el gran reto del regulador debe ser asegurar que la carga económica exigida vaya al estricto ritmo de la modernización e inversión en infraestructura de cada operador, evitando forzar inversiones artificiales en tecnologías que están destinadas a desaparecer.

6. Campañas pedagógicas de los asignatarios y operadores (Artículo 6.14.1.3.)

Respecto del apartado que establece que “La CRC definirá mediante una circular un hashtag oficial para el seguimiento de estas campañas en cada trimestre, así como los criterios mínimos de contenido, alcance y medios que deberán cumplir (SFT)” consideramos que es suficiente con la definición del hashtag oficial como estrategia para el seguimiento y trazabilidad de las campañas.

No obstante, establecer criterios mínimos trimestre tras trimestre, relacionados con el contenido, el alcance y los medios de comunicación, podría generar rigideces innecesarias; resultaría más efectivo que la CRC establezca unos lineamientos generales y orientadores de carácter permanente, que puedan ser adoptados por cada uno de los asignatarios de recursos de identificación y los PRST de manera tal que se tenga flexibilidad en el uso de herramientas y recursos pedagógicos tales como: guías de prevención, ejemplos basados en casos reales debidamente anonimizados, alertas sobre modalidades emergentes, recomendaciones

prácticas y mensajes de autocuidado digital que puedan ser utilizados de manera dinámica según la situación y el riesgo identificado en cada momento.

Adicionalmente, la adopción de lineamientos generales favorecería la innovación en las estrategias de comunicación, focalizando los esfuerzos en la efectividad de los mensajes y la generación de impacto en las diferentes audiencias, más que en el cumplimiento periódico de requisitos específicos de forma o contenido.

Así mismo se tendría oportunidad de contrastar las diferentes campañas de divulgación de los actores del sector, enriqueciéndose el análisis del impacto de estas y con ello facilitar la identificación de buenas prácticas y acciones de mayor impacto.

7. Formación interna en materia de prevención del fraude (Artículo 6.14.1.5.)

En cuanto a la periodicidad establecida para la formación interna en materia de prevención de fraude, de mínimo 4 sesiones al año, consideramos que se debe reevaluar ya que la efectividad de los programas de formación no es directamente proporcional al número de sesiones, sino más bien depende de la calidad, pertinencia, utilización de contenidos actualizados y de la debida apropiación por parte de los colaboradores.

Por lo anterior, sugerimos una periodicidad mínima de dos (2) sesiones de formación al año (una sesión por semestre), manteniendo la obligación de cubrir los contenidos definidos por la comisión. En este sentido, dos jornadas de capacitación al año, adecuadamente estructuradas, permiten abordar de manera integral los temas relacionados con la prevención del fraude, nuevas modalidades identificadas y cambios en los procedimientos internos. Estas jornadas de formación eventualmente se podrían complementar con esquemas continuos de divulgación interna cuando surjan nuevas amenazas o modalidades de fraude que representen un riesgo significativo.

II. SOLICITUD CONCRETA

De manera respetuosa, TIGO solicita a la CRC realizar los siguientes ajustes, alineados con los comentarios expuestos:

Solicitud 1. Acompañar el nuevo régimen A2P de la desregulación de la tarifa mayorista del SMS A2P, sustituyendo la tarifa regulada ex ante por un esquema de libre negociación comercial entre PRST, PCA/IT, integradores y originadores, con intervención regulatoria únicamente ante controversia o conductas abusivas, idealmente concomitante con la entrada en vigencia del nuevo régimen, de forma anterior a la entrada en vigencia de las normas aquí dispuestas con por lo menos 6 meses, a su efectiva implementación.

Solicitud 2. Ampliar el período de transición y la entrada en vigencia plena del régimen A2P a un mínimo de doce (12) meses, con fases que prevean márgenes razonables para la contratación del validador, los desarrollos, las integraciones por APIs y las pruebas, evitando hitos concatenados de pocos días.

Solicitud 3. Trasladar al cliente corporativo/originador el deber de consultar el RNE y de abstenerse de contactar a los inscritos, haciendo un llamado a la SIC para que incorpore reglas claras que le apliquen a las empresas de manera general, eliminando la obligación de validación y bloqueo en tiempo real del RNE a cargo del PRST en el tráfico de voz.

Solicitud 4. Acotar el alcance de las medidas aplicables a SMS P2P y voz, de manera que la obligación se limite a la implementación de herramientas tecnológicas basadas en al menos un criterio razonable de análisis de patrones, y no en la exigencia acumulativa de todos los patrones previstos en la propuesta regulatoria.

Esto permitiría preservar la flexibilidad técnica de los PRST evitando cargas y costos desproporcionados de implementación.

Solicitud 5. Replantear las medidas de voz bajo criterios de proporcionalidad y costo-eficiencia, asignando las cargas a los carriers internacionales y a los originadores, y previendo que las medidas que afecten el tráfico sean posteriores, confirmadas y reversibles.

Solicitud 6. Excluir las Obligaciones Asociadas a la Capa de Aplicación, no es pertinente imponer obligaciones que responsabilizan a los PRST por la visualización, desarrollo o implementación de etiquetas informativas en los terminales de los usuarios. Cualquier medida de mitigación de fraude debe limitarse estrictamente a variables de señalización técnica de transporte y no a la provisión de software o interfaces de usuario, por ser una actividad ajena a las capacidades del CORE de red.

Solicitud 7. Asegurar que la carga económica exigida en los servicios VOZ se oriente a la modernización e inversión en infraestructura de cada operador, y la migración hacia redes Full-IP evitando forzar inversiones artificiales en tecnologías que están destinadas a desaparecer.

Solicitud 8. Extender las obligaciones de trazabilidad, KYC y control a la numeración E.164 no geográfica utilizada para SMS, o disponer su devolución, cerrando el riesgo de migración hacia un canal menos regulado.

Solicitud 9. Asegurar la debida remuneración de la red y evitar cargas desproporcionadas sobre el tráfico de voz cursado en las redes de los PRST.

Solicitud 10. Solicitamos que para las campañas pedagógicas que son responsabilidad de los asignatarios y operadores no se establezcan criterios cada trimestre, sino que la CRC defina unos lineamientos generales y orientadores de carácter permanente, que puedan ser adoptados por cada uno de los asignatarios de recursos de identificación y los PRST de manera tal que se tenga flexibilidad en el uso de herramientas y recursos pedagógicos.

Solicitud 11. Respecto a la formación interna en materia de prevención del fraude se solicita ajustar la periodicidad de sesiones al año, disminuyendo de 4 a 2 sesiones por año, manteniendo la obligación de cubrir los contenidos definidos por la comisión, con la posibilidad de complementar con esquemas continuos de divulgación interna cuando surjan nuevas amenazas o modalidades de fraude que representen un riesgo significativo.

Agradecemos a la Comisión la oportunidad de participar en esta consulta y reiteramos nuestro respaldo a los objetivos del proyecto. **TIGO manifiesta su disposición a participar en las mesas técnicas que la CRC estime pertinentes** para precisar los aspectos técnicos, los plazos y el esquema de remuneración que permitan que estas medidas sean idóneas, proporcionales y sostenibles en el tiempo frente a la evolución del fraude.

Cordialmente,


SAMUEL HOYOS MEJÍA
Vicepresidente de Asuntos Externos