

COMENTARIOS Y OBSERVACIONES:

Proyecto prevención y mitigación del contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

Compania: Sinch Colombia S.A.S

Fecha: 23 de junio 2026

Documento de Análisis Técnico y Regulatorio



Tabla de Contenido:

- 1. Comentarios sobre las Temáticas y Sub-temáticas: 4
 - 1.1. Identificación del Remitente (SENDER ID en A2P): 4
 - 1.2. Trazabilidad y Controles en A2P (Validador Centralizado):..... 4
 - 1.3 Control de SMS P2P y Planes Ilimitados: 5
- 2. Comentarios sobre Régimen de Administración de Recursos de Identificación:..... 6
- 3. Comentarios sobre la Propuesta y el Proceso Regulatorio General:..... 7
- 4. Aspectos a Considerar y Retos de la Propuesta:..... 7
- 5. Oportunidades para Fortalecer la Propuesta: 8
- 6. Otros Comentarios:..... 8
 - 6.1. Desregularización de la tarifa de SMS de A2P:..... 8

El presente documento contiene los comentarios de Sinch Colombia S.A.S en materia de servicios de mensajería de texto, en el marco del proyecto “Identificación de Medidas para Mitigar el Fraude Cibernético por Medio de Servicios Móviles”, en respuesta a las iniciativas y propuestas planteadas en el documento de soporte de junio de 2026:

<https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-41-7-1/Propuestas/documento-soporte-mitigacion-fraude-servicios-moviles.pdf>

1. Comentarios sobre las Temáticas y Sub-temáticas:

1.1. Identificación del Remitente (SENDER ID en A2P):

Impacto positivo en la confianza del usuario:

Reemplazar códigos numéricos genéricos por un SENDER ID alfanumérico es una de las medidas más efectivas para mejorar la experiencia del usuario. Permite identificar visualmente y de inmediato a entidades legítimas (como bancos o tiendas), reduciendo drásticamente la efectividad del smishing.

Reto operativo:

- El éxito de esta medida dependerá de que la CRC establezca un proceso de validación sumamente ágil pero riguroso para la asignación de los SENDER IDs, evitando que actores malintencionados logren registrar nombres similares a marcas reconocidas (técnicas de spoofing o suplantación tipográfica).
- Adicionalmente, los tiempos de registro pueden constituir una barrera para los proveedores de contenido que necesiten enviar campañas utilizando Sender IDs vinculados a los productos o servicios de una empresa, especialmente cuando dichas campañas requieren una implementación rápida.
- De igual manera, queda por resolver la gestión y gobernanza del registro de Sender IDs en un escenario multi-proveedor, donde diversos PCAs pueden coexistir para el envío de SMS de una sola entidad.
- Asimismo, se solicita aclarar el número máximo de Sender IDs que pueden asignarse a un mismo código corto A2P gestionado por el agente solicitante.

1.2. Trazabilidad y Controles en A2P (Validador Centralizado):

La implementación de KYC no reduce el fraude:

La propuesta ya exige la creación y asignación de un **SENDER ID**. El simple hecho de que un cliente empresarial logre registrar y obtener este identificador alfanumérico ya actúa como un mecanismo robusto de autenticación.

Es decir, a través del SENDER ID, el ecosistema ya tiene la certeza de que el originador es legítimo y de que su tráfico es genuino. Exigir un proceso adicional de KYC sobre una empresa que ya cuenta con un identificador unívoco y regulado es duplicar esfuerzos sin añadir una capa de seguridad proporcional y contribuye a destruir el dinamismo inherente del servicio SMS.

Posible fricción en el mercado:

- Aunque no representa una mejora real para la seguridad, exigir la pre-aprobación de todas las plantillas de mensajes traducirá la regulación en más procesos de burocracia, fricción y demoras para las empresas legítimas. El “validador centralizado” deberá contar con tecnología (posiblemente automatización o IA) para intentar aprobar plantillas rápidamente sin afectar el dinamismo del comercio electrónico..
- Al trasladar la totalidad de los costos a los asignatarios de código corto A2P, se puede generar una barrera de entrada desproporcionada para nuevos proveedores o agregadores más pequeños. Aunque se menciona que la tarifa puede ser diferenciada por volumen, los costos fijos de la implementación tecnológica inicial podrían encarecer el acceso al recurso.
- La Validación de plantillas en "tiempo real" puede dar espacio a cuellos de botella. La aprobación o rechazo manual/semiautomático de plantillas de contenido y la consulta en tiempo real antes del enrutamiento imponen un desafío de latencia crítico. En el ecosistema A2P, donde la inmediatez (por ejemplo, mensajes de OTPs) es vital, depender de una consulta externa centralizada para cada mensaje puede degradar la calidad del servicio y generar caídas si el validador experimenta indisponibilidad.
- La falta de exigencia de APIs convertirá al Validador en un cuello de botella: Si el sistema no está automatizado desde su concepción, los procesos serán insosteniblemente lentos. Para evitar esta fricción operativa, la norma debe obligar al Validador Centralizado a exponer APIs estandarizadas, robustas y de ultra-baja latencia (para el registro de plantillas y consultas de enrutamiento), prohibiendo cualquier tipo de procesamiento manual en la ruta crítica del tráfico.
- ¿Qué sucede si el validador aprueba por error una plantilla que resulta ser fraude (phishing), o bloquea injustificadamente tráfico legítimo debido a un fallo en sus bases de datos? El texto debe delimitar claramente la responsabilidad civil y contractual ante estos escenarios para proteger a los asignatarios de pérdidas reputacionales y económicas.
- Se requiere un procedimiento expedito para que los asignatarios puedan apelar decisiones del validador (como el rechazo de una plantilla o marca) sin tener que recurrir directamente a un proceso administrativo largo ante la CRC, asegurando la continuidad del negocio.

1.3 Control de SMS P2P y Planes Ilimitados:

Cierre de una brecha crítica (Granjas de SIMs):

- A medida que se endurecen los controles en el tráfico empresarial (A2P), los estafadores suelen migrar al tráfico de persona a persona (P2P) usando planes de SMS ilimitados. Implementar controles aquí es fundamental para no dejar una “puerta trasera” abierta al fraude.

Equilibrio entre seguridad y privacidad:

- La exigencia a los operadores de monitorear patrones atípicos es acertada, pero deberá aplicarse con cuidado para no vulnerar la privacidad de las comunicaciones. Los operadores deben enfocarse en monitorear metadatos (volumen, frecuencia) y ciertamente, el esquema de respuesta escalonada protege a los usuarios regulares de falsos positivos (bloqueos accidentales por uso legítimo intensivo).

2. Comentarios sobre Régimen de Administración de Recursos de Identificación:

Corresponsabilidad y Descentralización:

- Empoderar a los operadores (PRST) para suspender o terminar contratos con integradores reincidentes descentraliza la vigilancia. Esto obliga a los integradores a ejercer un control estricto sobre sus propios clientes, creando una cadena de custodia digital; sin embargo, también habilita un escenario de mayor control de mercado por parte de los operadores, con el riesgo latente de vulnerar los derechos de los agregadores que aportan un tráfico minoritario a la red.
- Con respecto al proceso de suspensión y revocación de códigos cortos, se recomienda priorizar la definición de políticas y procedimientos internos por parte de los PRST. Dado que administran directamente la información de tráfico, se encuentran en una posición idónea para validar si la severidad y el volumen de las reclamaciones de los usuarios justifican la baja del servicio.

En la práctica actual, se constata la revocación de códigos cortos motivada por incidentes aislados (una o dos quejas), lo que introduce una alta inestabilidad operativa y comercial para los agregadores y sus clientes. Por consiguiente, es imperativo establecer un umbral o métrica de tolerancia de quejas que garantice la proporcionalidad de la medida antes de ejecutar cualquier desconexión.

En esta misma línea, antes de que la CRC determine que un código debe ser suspendido o revocado, el PCA debe tener la oportunidad formal de discutir la situación directamente con el PRST. Para esto, debería implementarse un sistema o mesa de análisis de fraude donde todos los miembros del ecosistema (los PRST, los PCA y la CRC) tengan el espacio para evaluar conjuntamente el tema, asegurando que las decisiones no se tomen de forma unilateral o guiadas exclusivamente por el regulador.

Finalmente, es imperativo advertir sobre el riesgo de mercado que conllevan estas medidas punitivas. En el escenario actual, cualquier proceso que derive en la revocación de un código corto significa, en la práctica, que la recuperación de dicho código sea casi imposible.

Esta extrema rigidez e inestabilidad comercial está provocando que las empresas que dependen del SMS como parte vital de sus procesos operativos decidan abandonar el servicio por falta de garantías, optando por mudar su tráfico de manera definitiva hacia otros canales alternativos como WhatsApp, lo que en última instancia debilita la industria formal y regulada de los mensajes de texto.

Eficacia de la Medida Cautelar de Suspensión:

- La suspensión provisional del tráfico es la herramienta más efectiva a corto plazo, ya que evita que los actores maliciosos sigan operando durante el tiempo que toman los procesos administrativos tradicionales. Sin embargo, para garantizar la seguridad jurídica de la operación, es indispensable establecer políticas claras que definan con precisión qué casos ameritan esta suspensión. Asimismo, resulta prioritario diseñar un procedimiento ágil de reactivación del tráfico para mitigar el impacto en caso de que la suspensión se ejecute de manera errónea o injustificada.

3. Comentarios sobre la Propuesta y el Proceso Regulatorio General:

- La co-responsabilidad y gestión integral de la cadena de valor destaca por su enfoque sistémico, distribuyendo responsabilidades claras entre el ente regulador (registro de *Sender IDs*), agregadores (protocolos *KYC*), operadores de red y marcas para crear un perímetro de defensa colaborativo; aunque esto tiene la gran ventaja de cerrar brechas de seguridad desde el origen y garantizar la equidad operativa al no sobrecargar financieramente solo a los operadores, también conlleva retos regulatorios significativos, como la inmensa complejidad de supervisar a múltiples actores y el riesgo de que la responsabilidad se diluya entre las partes si las reglas no son lo suficientemente claras ante una filtración de tráfico fraudulento.
- La viabilidad del nuevo marco técnico dependerá de un periodo de transición realista que permita integrar a los operadores y registrar a las marcas sin interrumpir las comunicaciones críticas de las empresas. El enfoque debe ser en un despliegue por fases evita fallos masivos en el servicio y protege el tráfico SMS legítimo. No obstante, el desafío radica en que un plazo de adaptación demasiado largo mantendrá la vulnerabilidad al fraude y postergará la definición de las tarifas A2P, prolongando la incertidumbre financiera en el sector.

4. Aspectos a Considerar y Retos de la Propuesta:

- **Burocracia y pérdida de dinamismo comercial:**
La obligatoriedad de pre-aprobar plantillas de texto (Template IDs) limita la agilidad de los comercios. Por ejemplo, si una marca necesita lanzar una oferta relámpago basada en una coyuntura del día, no podrá hacerlo de inmediato si tiene que esperar el visto bueno de la plantilla por parte del validador.
- **Costos de implementación trasladados al usuario final:**
El costo de crear y mantener la infraestructura del Validador Centralizado, además del registro de los Sender IDs, será asumido inicialmente por los operadores y agregadores. Muy probablemente, este costo adicional se trasladará a las empresas y, finalmente, a los usuarios a través de tarifas de servicios más caras.
- **Tensión con la privacidad en el monitoreo P2P:**
La exigencia a los operadores de monitorear conductas “atípicas” en mensajes personales (P2P) camina sobre una línea muy delgada en términos de privacidad de datos. Aunque se aclara que es un análisis de patrones, existe el riesgo de un monitoreo intrusivo o de la generación de falsos positivos (por ejemplo, bloquear a un usuario legítimo que simplemente está enviando invitaciones masivas para un evento personal).

5. Oportunidades para Fortalecer la Propuesta:

- **Canales de reclamación rápidos para el usuario bloqueado:**

El documento menciona el bloqueo temporal y la terminación de contratos para usuarios P2P con conductas atípicas, pero no especifica un mecanismo de defensa o reclamación rápida para el usuario. Si el algoritmo de un operador bloquea por error la línea de una persona, el ciudadano queda incomunicado sin un debido proceso claro para demostrar su inocencia de manera ágil. Se debería establecer un canal de atención prioritario y directo con los operadores para la gestión operativa de quejas y reclamos. Esto permitirá resolver las controversias de manera ágil en una primera instancia, sin la necesidad de escalar cada incidente directamente ante el regulador (CRC), evitando así la congestión administrativa y demoras innecesarias.

- **Coordinación con plataformas OTT (WhatsApp, Telegram, etc.):**

Al endurecer la regulación de los SMS, la delincuencia migrará inmediatamente hacia canales IP de mensajería como WhatsApp. Una regulación que solo se enfoque en los SMS tradicionales soluciona únicamente una parte del problema; hace falta una visión convergente que involucre la cooperación de las plataformas OTT y los reguladores de internet.

Adicionalmente, el análisis de estas medidas no debe realizarse exclusivamente desde un punto de vista técnico, sino que es imperativo incorporar una perspectiva comercial.

Aunque el SMS ofrece, en teoría, puede ofrecer una mayor protección al usuario, su sobrerregulación dificulta drásticamente la operatividad haciéndolo inviable frente a sus competidores. Ante la acumulación de barreras regulatorias, procesos burocráticos y precios regulados, los PCAs verán en WhatsApp su única opción viable.

Una reducción crítica en el volumen de tráfico SMS afectaría aún más la rentabilidad de los operadores (PRST) y agregadores (PCA), comprometiendo definitivamente la viabilidad a largo plazo de este canal de comunicación.

- **Sanciones específicas para el Validador Centralizado:**

Así como se imponen obligaciones estrictas a los operadores y marcas, la regulación debe establecer multas y sanciones severas al Validador Centralizado si este incumple con los Acuerdos de Niveles de Servicio o si sufre una brecha de seguridad que filtre la base de datos de los Sender IDs y la información de KYC de las empresas del país.

6. Otros Comentarios:

6.1. Desregularización de la tarifa de SMS de A2P:

Por medio del presente, solicitamos respetuosamente a la CRC considerar la **desregulación total de los precios para la terminación de mensajes SMS A2P**, permitiendo que estos sean definidos por las dinámicas de libre competencia del mercado.

Nuestra solicitud se fundamenta en los siguientes puntos críticos para la sostenibilidad y seguridad del ecosistema de telecomunicaciones en Colombia:

1. **Protección contra el fraude cibernético (Smishing y Spam):** Como lo ha advertido ampliamente el sector, una reducción drástica o una regulación estricta a la baja en los costos de los SMS A2P reduce las barreras de entrada para actores malintencionados. Un modelo de precios regulados a la baja facilita el envío masivo de mensajes fraudulentos, poniendo en riesgo directo a los usuarios del sistema financiero, comercial y de telecomunicaciones.
2. **Incentivo a la inversión en seguridad:** La lucha contra el cibercrimen requiere de inversiones constantes en plataformas de filtrado, firewalls avanzados y monitoreo de redes. La desregulación de los precios A2P permite a los operadores generar los ingresos necesarios para sostener, actualizar y fortalecer esta infraestructura crítica de seguridad, garantizando un servicio confiable para las empresas y los usuarios finales.
3. **Naturaleza del mercado B2B:** A diferencia del mercado P2P, el ecosistema A2P es un entorno netamente corporativo (Business-to-Business) en el que participan grandes empresas, agregadores e instituciones. En este contexto, los precios responden al valor agregado, la calidad del enrutamiento y la seguridad garantizada en la entrega del mensaje, por lo que el mercado tiene la madurez suficiente para autorregularse sin necesidad de topes artificiales.
4. **Migración a canales OTT:** Un esquema de precios regulados destruyen la operatividad del SMS y lo hacen inviable frente a sus competidores. Esta asimetría competitiva provocará una migración masiva e irreversible de los clientes hacia WhatsApp, reduciendo críticamente el tráfico SMS y amenazando la rentabilidad y supervivencia a largo plazo de operadores (PRST) y agregadores (PCA). Por lo tanto, para evitar la extinción del canal SMS y permitirle competir en igualdad de condiciones, el eje central de la discusión debe ser la desregularización del precio del SMS.

Entendemos y apoyamos el objetivo de la CRC de proteger a los usuarios. Sin embargo, consideramos que la mejor forma de lograrlo no es forzando una tarifa a la baja que precarice el servicio, sino permitiendo que el mercado A2P opere bajo libre competencia. Esto asegurará que el costo del SMS refleje el verdadero valor de entregar comunicaciones seguras, verificadas y libres de fraude.