

OBSERVACIONES CONJUNTAS AL PROYECTO DE RESOLUCIÓN DE LA CRC

«Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones» — Código 2000-41-7-1

LLAMADO A LA REFORMULACIÓN INTEGRAL DE LA PROPUESTA

Documento suscrito por

BLIP-BLIP · INALAMBRIA · NEXVIA

Dirigido a: Comisión de Regulación de Comunicaciones — CRC

Asunto: Comentarios dentro del término de participación ciudadana al proyecto regulatorio de la referencia y solicitud de reformulación integral.

Fecha: Colombia, junio de 2026.

TABLA DE CONTENIDO

I. Presentación e interés legítimo de los firmantes	3
II. Petición central: reformulación integral del proyecto	3
III. Premisa compartida: compartimos el fin, objetamos los medios	3
IV. El error de diagnóstico: se combate con burocracia un problema tecnológico y de precios	4
V. Observaciones comunes y puntos de alineación	4
V.1. El Validador Centralizado: conflicto de interés estructural y captura regulatoria	4
V.2. La unicidad del código corto A2P: un punto único de falla sistémico	5
V.3. El régimen de plantillas de contenido: parálisis del canal y sobrecostos	6
V.4. Suspensión y desconexión unilateral: el PRST como juez y parte	6
V.5. La desaparición del Integrador Tecnológico	7
V.6. La asimetría regulatoria a favor del duopolio	7
V.7. KYC: traslado indebido y duplicación de obligaciones	8
VI. Efectos colaterales sistémicos	8
VI.1. Migración del fraude de A2P a P2P	8
VI.2. Desconexión de Colombia del mundo	8
VI.3. Migración a canales OTT no regulados	9
VI.4. Exclusión de las pequeñas y medianas empresas	9
VI.5. Afectación a las comunicaciones críticas y al usuario final	9
VII. Incongruencias normativas y contradicciones internas	9
VIII. Modelo alternativo propuesto	10
IX. Solicitudes concretas	11
Firmas	13

I. Presentación e interés legítimo de los firmantes

Las empresas que suscriben este documento BLIP-BLIP, INALAMBRIA y NEXVIA S.A.S.— son Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT) inscritos en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI), asignatarias de recursos de identificación y titulares de relaciones de acceso e interconexión SMPP vigentes con los principales PRST del país. En conjunto, sostenemos la operación de mensajería A2P de miles de empresas colombianas y extranjeras: bancos, entidades de salud, comercio, plataformas globales y entidades del Estado, así como las comunicaciones críticas que de ellas dependen —códigos OTP, alertas de seguridad, notificaciones transaccionales y citas médicas—.

Compartimos plenamente el fin que persigue la Comisión: combatir el fraude cibernético a través de redes móviles. Es un objetivo en el que invertimos capacidades técnicas propias todos los días y que defendemos como condición de confianza del canal. Por esa misma razón presentamos estas observaciones de manera conjunta: no controvertimos el fin, sino la viabilidad técnica, la proporcionalidad, la coherencia interna y, sobre todo, los efectos colaterales del conjunto de medios escogidos, que en su diseño actual no mitigan el fraude, sino que desestabilizan un ecosistema hasta hoy competitivo y reconfiguran el mercado en favor de los operadores dominantes.

Este documento recoge los puntos en los que las cuatro compañías coincidimos. La convergencia de agentes que compiten entre sí en torno a un mismo diagnóstico crítico es, en sí misma, una señal que la Comisión debería ponderar.

II. Petición central: reformulación integral del proyecto

Solicitamos respetuosamente a la Comisión que **no expida el proyecto en su forma actual y que lo reformule de manera integral**. No se trata de ajustar artículos aislados: el número de incongruencias normativas, contradicciones internas y efectos colaterales sistémicos es de tal magnitud que las correcciones parciales resultan insuficientes. El proyecto debe reconstruirse desde sus premisas, partiendo de la realidad operativa del negocio A2P, de un análisis de impacto que cuantifique sus efectos y de un diálogo técnico con todos los actores del ecosistema.

La presente comunicación expone (i) el error de diagnóstico que vicia la propuesta; (ii) las observaciones comunes a las disposiciones más graves; (iii) los efectos colaterales que la regulación desencadenaría; (iv) las incongruencias internas y las contradicciones con la propia doctrina reciente de la Comisión; y (v) un modelo alternativo que preserva íntegramente la finalidad antifraude sin destruir el ecosistema.

III. Premisa compartida: compartimos el fin, objetamos los medios

El fraude por SMS y por voz es un problema real, dinámico y en permanente evolución. Quienes firmamos este documento operamos la primera línea de detección: filtramos contenidos, bloqueamos cuentas, identificamos patrones de suplantación, SIM boxing y SMS

pumping, y contenemos a diario tráfico fraudulento con inversión tecnológica propia. El tráfico fraudulento representa, según nuestros monitoreos, una fracción menor del total de SMS cursados; el reto regulatorio consiste en atacar esa fracción sin poner en riesgo el tráfico legítimo del que dependen millones de usuarios.

El proyecto invierte esa lógica. En lugar de fortalecer la inteligencia compartida y las herramientas tecnológicas —incluidos los avances recientes en inteligencia artificial, que son hoy el mejor aliado para prevenir proactivamente el fraude—, opta por una arquitectura de control previo, validadores privados, autorizaciones de contenido y sanciones de desconexión que recaen sobre los agentes formales del ecosistema, no sobre los defraudadores. El resultado previsible es doble: el fraude no se reduce y el canal legítimo se encarece, se ralentiza y se contrae.

IV. El error de diagnóstico: se combate con burocracia un problema tecnológico y de precios

La propuesta intenta resolver, a punta de burocracia —nuevos comités, procesos, aprobaciones previas y entidades creadas para el efecto—, un problema que es esencialmente tecnológico y de precios. La consecuencia directa de esa elección no es la mitigación del fraude, sino una disminución considerable del volumen de mensajería A2P legítima que se cursa en Colombia, que afecta de manera directa a los integradores y, a través de ellos, a las empresas usuarias del canal.

La analogía es ilustrativa: pretender reducir un delito organizado obligando a todos los actores legales a registrarse y a demostrar que no son delincuentes no detiene a quien opera en la ilegalidad. Quien vive del fraude nunca se registrará ante el validador, no solicitará SENDER ID ni someterá plantillas a aprobación; seguirá encontrando caminos para evadir los controles —entre ellos, como se explica más adelante, el tráfico P2P—. Los únicos que cargan con el peso del nuevo régimen son los agentes formales, precisamente los que hoy invierten en prevención.

A ello se suma un punto en el que coincidimos con énfasis: **el mecanismo de «recuperación de códigos», que el propio sector y el regulador han reconocido como ineficaz para prevenir el fraude**, se convierte en el eje sobre el que se construye toda la nueva regulación. Es altamente punitivo, desconoce el carácter dinámico del problema y se apoya en una palanca débil para sostener el crecimiento de una categoría importante del sector de telecomunicaciones del país.

V. Observaciones comunes y puntos de alineación

Las cuatro compañías coincidimos en que las siguientes disposiciones, por sí solas y de manera acumulativa, justifican la reformulación integral del proyecto.

V.1. El Validador Centralizado: conflicto de interés estructural y captura regulatoria

El proyecto entrega a una persona jurídica privada —seleccionada por los PRST conforme a condiciones que ellos mismos elaboran, pero financiada por los PCA e IT— la facultad de aprobar o rechazar las plantillas de contenido sin las cuales ningún agente puede cursar tráfico, y todo ello sin recurso administrativo alguno contra sus decisiones. Quien selecciona y controla al árbitro es competidor directo de los agentes sometidos a su validación.

Esto reproduce, ahora en SMS, el esquema del administrador centralizado de la portabilidad: un tercero designado por los operadores que se convierte en un nuevo «big brother» de la mensajería empresarial colombiana, capaz de definir qué se envía, qué no se envía y con qué urgencia. Las objeciones que compartimos son las siguientes:

- Conflicto de interés y riesgo de captura regulatoria: el validador depende, para su designación y permanencia, de los competidores directos de los sujetos que valida, mientras el tráfico A2P propio de los PRST queda exento de la validación que sí se impone a los independientes.
- Sobrecostos desconectados del régimen de remuneración: el costo de validar cada mensaje, sumado a los demás cargos del canal, puede encarecer el SMS por encima de su valor regulado —tal como ya ocurre con otros esquemas centralizados—, en abierta tensión con la filosofía de costo eficiente más utilidad razonable.
- Traslado indebido de una relación privada a un tercero: dejar en manos de un centralizador la fiscalización de la relación comercial privada entre un IT o PCA y su cliente es restrictivo de la libre competencia y de la libertad de contratación, y expone información confidencial de los clientes a un agente que no debería tenerla.
- Indeterminación operativa: el proyecto no precisa el modo de operación del validador (flujo de revisión de plantillas, integración por API, conciliación de tráfico real entre el centralizado y cada PRST, respeto de las TPS pactadas en la OBI y en los contratos de interconexión), lo que genera incertidumbre técnica y jurídica.
- Ausencia de garantías: el rechazo de una plantilla paraliza la operación sin que exista recurso de reposición ni apelación, en desmedro del debido proceso.

V.2. La unicidad del código corto A2P: un punto único de falla sistémico

La regla que limita a cada agente a un único código corto A2P (artículo 6.4.1.4 y su correlato en el numeral 6.4.2.2.2) desconoce el principio de uso eficiente de los recursos escasos y la propia naturaleza del recurso, concebido para diferenciar tipos de servicio, contenido, modalidad y tarifa. Sus efectos comunes preocupan a las cuatro compañías:

- Convierte el código corto en un punto único de falla: su recuperación produce la invalidación masiva y automática de la totalidad de los SENDER ID vinculados, de modo que un agente que cursa millones de comunicaciones críticas puede quedar fuera de operación en segundos. La pluralidad de códigos que hoy opera como redundancia natural desaparece.
- Hace inoperante la mensajería interactiva de doble vía (MO/MT): con un solo código para todos los clientes y unidades de negocio resulta inviable identificar y enrutar correctamente el tráfico de doble vía, lo que destruye un segmento entero del negocio.

- Restringe un mercado que debería crecer: obligar a cada empresa usuaria a tramitar su propio código y SENDER ID generará una ola de solicitudes y activaciones difícil de absorber, y excluirá de hecho a quienes hoy operan bajo códigos compartidos.

V.3. El régimen de plantillas de contenido: parálisis del canal y sobrecostos

La exigencia de que ningún mensaje A2P pueda cursarse sin una plantilla previamente aprobada y vigente en el sistema del validador (numerales 6.4.3.1.7 y 6.13.4.7.2, entre otros) instala un régimen de autorización previa de contenidos que es incompatible con la naturaleza dinámica del negocio:

- Paraliza servicios críticos y campañas urgentes: un comercio que necesita enviar una promoción de inmediato, o una entidad de salud que debe alertar sobre un riesgo sanitario urgente, quedan sujetos a un trámite de aprobación. En mensajería transaccional, minutos de indisponibilidad se traducen en afectación directa al usuario final. La oportunidad hace la diferencia.
- Vulnera la libertad de comunicación e introduce riesgos de privacidad: someter el contenido de las comunicaciones empresariales a la aprobación de un tercero limita la libertad de empresas e individuos para comunicarse con sus usuarios y expone información sensible.
- Genera sobrecostos recurrentes: la vigencia y renovación mensual de las plantillas impone una carga operativa permanente a toda la cadena, reduce la productividad y encarece el canal.
- Es un reto técnico de gran escala: implementar la validación previa de plantillas manteniendo los volúmenes actuales —del orden de miles de millones de SMS al mes— supone un desafío técnico cuya viabilidad el proyecto no acredita.
- Duplica obligaciones ya existentes: la identificación del remitente vía SENDER ID ya es exigible bajo la Ley 2300; el proyecto la reproduce con un nuevo recurso y un nuevo costo.

V.4. Suspensión y desconexión unilateral: el PRST como juez y parte

El Parágrafo 4 del artículo 6.1.1.8 propuesto autoriza al PRST a suspender unilateralmente, por un mes, la relación de acceso con el PCA/IT ante la segunda recuperación de un código, y a solicitar la terminación definitiva ante la tercera. Esta es, a nuestro juicio, la disposición de mayor gravedad del proyecto:

- Sanción sin debido proceso: la suspensión de la relación de acceso es, por sus efectos materiales, una sanción que priva al agente de su capacidad operativa, le impide cumplir contratos vigentes y le inflige un daño reputacional y económico que puede ser irreversible —para una empresa del sector, un mes desconectada equivale a la pérdida de su cartera—. Se impone sin procedimiento previo que garantice la defensa.
- Delegación de poder coercitivo en un competidor: el PRST es simultáneamente titular de la instalación esencial, asignatario de códigos cortos y competidor directo en el mercado

A2P. Entregarle la facultad de excluir a sus competidores convierte una potestad que corresponde al Estado en un instrumento de exclusión comercial.

- Regla de los «tres strikes» activable con quejas mal intencionadas: bajo el nuevo esquema, **tres recuperaciones —incluso injustificadas— bastarían para desconectar definitivamente a un integrador del que dependen miles de empresas.** Cualquier empresa integradora con clientes de reventa quedaría fuera del mercado en semanas. Las recuperaciones de códigos documentadas en 2025 y 2026 muestran que numerosos agentes formales —incluidos los propios firmantes— habrían quedado por fuera del negocio bajo esta regla. Ver tabla.

CAUSAL RECUPERACION	6.4.3.2.1	6.4.3.2.2	6.4.3.2.4	6.4.3.2.8	6.4.3.2.9	Grand Total
EMPRESA	RESOLUCION (Count All)					
ELIBOM	13	2		14		29
COLOMBIA TELECOMUNICACIONES			17	1		18
A2P	5	7		5		17
ESTRATECT	6	3		6		15
SPECTER LINE	1	1	9	1		12
ATENEA MOBILE	2	2		6		10
INALAMBRIA				5	1	6
TELECOM SMS		1		3		4
COLOMBIA MOVIL		1	1	2		4
HABLAME				4		4
AXESNET				3		3
PARTNERS TELECOM		1		2		3
INFOBIP				3		3
COMCEL		2		1		3
INTICO		1		2		3
MASIVIAN		1		1		2
ATH			2			2
BEMOBI			2			2
DIGITAL BLEND			2			2
KRONOS MOBILE				1		1
MESSANGI		1				1
SINCH				1		1
TECHNOKEY				1		1
SERVICIOS DE APOYO				1		1
SIGMA MOVIL				1		1
Grand Total	27	23	33	64	1	148

- Penalización automática que ignora la realidad del fraude: se puede cumplir íntegramente la regulación y, aun así, las organizaciones de fraude encontrarán caminos nuevos. La recuperación no debería operar de manera automática, sino solo cuando, en actuación con debido proceso, se demuestre negligencia o incumplimiento imputable al asignatario.
- Duplicación innecesaria de una potestad estatal: la propia CRC conserva la facultad de suspender preventivamente el recurso; duplicarla en manos de un privado interesado no añade protección al usuario, solo una barrera de exclusión.

V.5. La desaparición del Integrador Tecnológico

El proyecto invierte la arquitectura funcional del ecosistema que la propia Comisión definió. El Integrador Tecnológico es, por definición, el agente que provee la infraestructura de conexión entre los PRST y los PCA sin conexión directa; el PCA «puede o no» estar conectado

directamente. Al exigir conexión directa e infraestructura propia, prohibir el tráfico en nombre de terceros, negar el SENDER ID a los proveedores de infraestructura y limitar a los IT a un único código, el proyecto desdibuja y vuelve obsoleta la figura del IT:

- Desintermediación forzosa: si ser integrador se vuelve tan riesgoso —por la amenaza de desconexión definitiva— y los PCA deben (o pueden) contratar directamente con el PRST, el intermediario especializado pierde su razón de ser. El nuevo negocio se traslada a los PRST, aumentando la complejidad para las empresas y desconociendo la función misma de los IT: eliminar la complejidad de la red celular para el uso de mensajería en aplicaciones de valor.
- Concentración del mercado en los operadores: cada recuperación a un agente independiente opera, en la práctica, como una transferencia forzosa de clientela hacia el PRST verticalmente integrado, que controla la terminación en su red, dispone de códigos propios y no está expuesto a suspensión por terceros. La sanción al independiente se convierte en premio comercial para su competidor.
- Eliminación de un eslabón del ecosistema: se suprime —intencionalmente o no— una capa que ha permitido masificar el uso efectivo del SMS en Colombia, en contravía de los avances regulatorios logrados durante la última década.

V.6. La asimetría regulatoria a favor del duopolio

El proyecto descansa sobre la ficción de que los PRST son infraestructura neutral. La realidad es que los PRST son también asignatarios masivos de códigos cortos, compiten en el mercado de contenidos y han sido objeto reiterado de recuperación de recursos por las mismas causales que el proyecto agrava únicamente para los PCA e IT independientes. Sin embargo, la consecuencia agravada de la reincidencia —suspensión y desconexión— solo opera en una dirección: hacia abajo.

Tras la integración Tigo–Movistar, dos grupos concentran la inmensa mayoría del mercado móvil colombiano. En ese contexto, la red móvil es una instalación esencial sin sustituto técnico para la terminación de SMS, y toda facultad de exclusión entregada a sus titulares opera como barrera de entrada definitiva. **Pasamos así del «riesgo operador» que existía antes de la regulación al nuevo «riesgo regulatorio» que favorece a los operadores, precisamente cuando se configura un nuevo duopolio en el sector.**

V.7. KYC: traslado indebido y duplicación de obligaciones

El proceso de conocimiento del cliente (KYC) es, por naturaleza, una vinculación privada entre dos personas jurídicas, sujeta a la libre capacidad de contratación y al riesgo que cada parte asume. Dejar su fiscalización en manos de un centralizador —un tercero sin control legítimo sobre la información confidencial de los clientes— es conflictivo y mina los modelos de enrolamiento en línea. Las medidas antifraude que requieren intervención sobre la relación comercial deberían recaer en las autoridades y, en lo operativo, articularse con esquemas basados en el comportamiento y la calidad del tráfico de cada agente, no en una capa burocrática adicional de costo incierto.

VI. Efectos colaterales sistémicos

Más allá de cada disposición, el conjunto de la propuesta desencadena efectos colaterales que agravarían la situación que dice combatir.

VI.1. Migración del fraude de A2P a P2P

Al concentrar todos los controles —plantillas, registro, validación— sobre el tráfico A2P, el proyecto crea un incentivo perverso para que las comunicaciones empresariales, y con ellas el fraude, migren al tráfico P2P, donde no existe control de plantillas ni necesidad de registro. Las nuevas obligaciones impuestas a los PRST para bloquear el P2P con fines A2P son inefectivas frente a la realidad del problema. El resultado es un juego del gato y el ratón entre operadores, agregadores, PCA y delincuentes, con el fraude desplazándose al canal menos controlado.

VI.2. Desconexión de Colombia del mundo

La exigencia de NIT o sucursal en Colombia para ser asignatario de SENDER ID, sumada a la prohibición de cursar tráfico en nombre de terceros, clausura las comunicaciones transaccionales globales. Agregadores internacionales y plataformas de uso masivo —Microsoft, SAP, Salesforce, Google, Meta, Uber, Didi, Temu, Siigo, entre otras— entregan a los usuarios colombianos códigos OTP, confirmaciones y alertas en virtud de relaciones de servicio que el propio usuario contrató. Ninguna de ellas constituirá una sucursal local para terminar mensajes de valor unitario ínfimo: simplemente dejarán de llegar o migrarán a canales no regulados, deteriorando la seguridad del usuario, el efecto exactamente inverso al buscado.

VI.3. Migración a canales OTT no regulados

Cerrado o encarecido el cauce lícito del SMS, las comunicaciones empresariales no desaparecen: migran hacia canales OTT sobre redes de datos (WhatsApp y plataformas análogas) que escapan a la regulación de la CRC, a sus instrumentos antifraude, a sus recursos de identificación y a la jurisdicción nacional. El proyecto desconoce la característica diferencial del SMS que justifica su protección: llega a todo usuario con cobertura 2G, 3G, 4G o 5G, sin plan de datos, sin teléfono inteligente y sin aplicación instalada. Expulsar el tráfico hacia canales de datos no mitiga el fraude: lo traslada a un terreno sin supervisión y, de paso, excluye a los usuarios de menor conectividad, que son los de mayor vulnerabilidad.

VI.4. Exclusión de las pequeñas y medianas empresas

La carga operativa, administrativa y económica del nuevo régimen —tramitar código y SENDER ID propios, contratar acceso directo con un PRST, someter plantillas y financiar al validador— hará inviable el canal para las pequeñas y medianas empresas y para los pequeños negocios en territorios apartados, privándolos del SMS como canal universal de comunicación allí donde no hay datos. La solución implícita que el modelo les ofrece —migrar a WhatsApp— es una admisión de que la regulación no es viable para quien más depende del SMS.

VI.5. Afectación a las comunicaciones críticas y al usuario final

El encadenamiento rígido entre código corto, SENDER ID y plantilla, junto con la regla de unicidad y los efectos de arrastre de la recuperación, hace recaer las consecuencias sobre

terceros inocentes: recuperado el código de un asignatario, todos los SENDER ID vinculados —entidades financieras, prestadores de salud, plataformas— pierden su canal de manera instantánea. El plazo de treinta días hábiles para que esos terceros acrediten una nueva relación comercial es técnicamente insuficiente para una migración contractual, registral y técnica completa. Durante ese vacío, el usuario deja de recibir claves OTP, confirmaciones transaccionales y alertas de seguridad: el riesgo de fraude no se mitiga, se amplifica, porque el defraudador encuentra a un usuario desconectado de sus canales legítimos de verificación. La medida castiga al usuario que dice proteger.

VII. Incongruencias normativas y contradicciones internas

El proyecto adolece, además, de contradicciones que comprometen su coherencia y su motivación:

1. **Contradicción con la estrategia de simplificación de la propia Comisión.** La propuesta va en completa contravía de la orientación reciente del regulador hacia la simplificación regulatoria: en lugar de simplificar, complejiza el sector con nuevos roles, reglas específicas, comités y entidades, sin que ello aporte a la disminución real del fraude.
2. **Contradicción con la doctrina de corrección de asimetrías (Resolución CRC 8144 de 2026).** Apenas meses antes, la Comisión reconoció que la regulación debe «preservar o restablecer el equilibrio que debe existir entre aquellos actores que abrigan intereses legítimos contrapuestos» y asegurar que ningún operador se vea desproporcionadamente afectado por las asimetrías. El presente proyecto hace exactamente lo contrario: en lugar de dotar de mecanismos compensatorios al agente más débil, amplifica la asimetría entregando al más fuerte facultades coercitivas sobre el más débil.
3. **Asimetría en los plazos de transición.** La misma Resolución 8144 concedió a los operadores una ventana de transición de varios meses, con pruebas técnicas, para una simple adecuación de sistemas de medición. El proyecto otorga, en cambio, plazos perentorios de diez y quince días hábiles para decisiones estructurales —consolidar códigos, migrar servicios con millones de usuarios, renegociar contratos— y treinta días hábiles a terceros inocentes para una migración completa. La disparidad de trato procedimental opera como regla no escrita en favor de los operadores.
4. **Contradicción interna entre la unicidad y el régimen de reincidencia.** Si cada agente solo puede tener un código corto, la recuperación de ese único código lo desconecta de facto desde el primer instante; la suspensión por segunda recuperación y la terminación por tercera presuponen una pluralidad de códigos que el propio proyecto prohíbe. Ambas reglas no pueden coexistir.
5. **Contradicción entre el documento soporte y el articulado.** El documento soporte ilustra el SENDER ID con formatos diferenciados por propósito dentro de una misma entidad —«Banco XX – Citas», «Banco XX – Transacciones», «Banco XX – Mercadeo»—, granularidad que el articulado hace imposible al limitar la asignación a un

único SENDER ID por NIT. La inconsistencia constituye un vicio de motivación que debe subsanarse.

6. **Ausencia de análisis de impacto.** El proyecto ordena migraciones masivas, devolución de recursos en operación y consolidación de códigos con usuarios activos, sin que el documento soporte cuantifique ese impacto ni lo pondere contra beneficio antifraude alguno. Ninguna modalidad de fraude documentada se origina en la pluralidad de códigos de asignatarios formales.

VIII. Modelo alternativo propuesto

Las objeciones anteriores no dejan a la Comisión sin instrumentos. Los firmantes proponemos un modelo que preserva íntegramente la finalidad antifraude, devolviendo la función coercitiva a su titular constitucional y protegiendo la continuidad del servicio al usuario:

- **Reserva estatal de la coerción.** Suspensiones, bloqueos definitivos, recuperaciones y desconexiones se ordenan exclusivamente por la CRC mediante acto administrativo motivado, dentro de actuaciones con traslado y derecho de defensa. Los PRST y el validador detectan y reportan; no sancionan.
- **Continuidad del servicio como principio.** Portabilidad operativa inmediata del SENDER ID entre asignatarios de códigos y continuidad transitoria del tráfico de terceros inocentes ante recuperaciones, protegiendo los OTP y las comunicaciones críticas. Pluralidad de códigos como redundancia que evita puntos únicos de falla.
- **Identificación sobre recursos existentes.** Aprovechamiento de las obligaciones ya vigentes (Ley 2300) para la identificación del remitente, incorporando los requisitos de verificación documental sin crear recursos paralelos ni capas de costo redundantes.
- **Inteligencia compartida e inclusiva.** Comité técnico de lucha contra el fraude con membresía plena de PCA e IT —que operan la primera línea de detección—, y construcción de una plataforma de alertas en tiempo real y revisión periódica de parámetros con participación de todos los segmentos, apalancando las capacidades tecnológicas y de inteligencia artificial del ecosistema.

IX. Solicitudes concretas

Con fundamento en lo expuesto, los firmantes solicitamos respetuosamente a la Comisión de Regulación de Comunicaciones:

1. **PRIMERO. Reformular integralmente el proyecto**, reconstruyéndolo a partir de la realidad operativa del negocio A2P y de los principios del modelo alternativo propuesto, en lugar de expedirlo con correcciones parciales.
2. **SEGUNDO. Reformular o eliminar el régimen del Validador Centralizado** (selección pública por la CRC, gobernanza multiactor, validación simétrica del tráfico de los PRST, financiación proporcional y recurso de reposición con efecto suspensivo), o sustituirlo por un esquema de detección distribuida con decisión estatal.

3. **TERCERO. Eliminar la unicidad del código corto A2P y la consolidación forzosa** (artículo 6.4.1.4, numeral 6.4.2.2.2 y numeral 19.1.5 del régimen de transición), preservando la pluralidad de códigos como mecanismo de continuidad y diferenciación de servicios.
4. **CUARTO. Eliminar la suspensión y la desconexión unilateral por el PRST** (Parágrafo 4 del artículo 6.1.1.8) y reservar toda medida restrictiva de derechos a la CRC, mediante acto motivado y con garantías de defensa.
5. **QUINTO. Eliminar la autorización previa de plantillas por un esquema de etiquetado**, apoyándose en el sistema de inteligencia compartida y reservando el bloqueo al fraude identificado por orden de autoridad. Eliminar por ende la renovación mensual obligatoria.
6. **SEXTO. Preservar la figura del Integrador Tecnológico y el modelo de agregación**, permitiendo el tráfico en nombre de terceros y la identificación de remitentes internacionales a través del agente local responsable, sin exigir sucursal en Colombia.
7. **SÉPTIMO. Incorporar a los PCA e Integradores Tecnológicos al comité técnico de lucha contra el fraude**, con voz y voto en la revisión de parámetros de detección.
8. **OCTAVO. Publicar, antes de cualquier expedición, un análisis de impacto normativo** que cuantifique los efectos de la unicidad, la consolidación forzosa y las restricciones al SENDER ID sobre los usuarios, el ecosistema y las comunicaciones internacionales, con respuesta motivada a los comentarios recibidos.
9. **NOVENO. Convocar una mesa técnica con la participación de PCA e Integradores Tecnológicos** para la revisión conjunta del articulado, en la que las empresas firmantes manifestamos desde ya nuestra plena disposición a participar y a aportar nuestra experiencia operativa en detección y mitigación de fraude A2P.

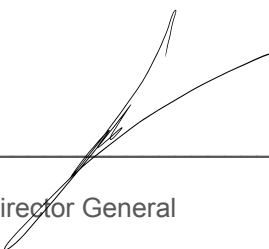
La lucha contra el fraude es una causa que compartimos y en la que hemos invertido capacidades técnicas propias. Por ello insistimos: las medidas eficaces contra el fraude fortalecen la institucionalidad del regulador; las medidas que trasladan el poder del regulador a los agentes dominantes no combaten el fraude, reconfiguran el mercado. Una regulación bajo la cual una empresa formal, con infraestructura construida, empleo sostenido y recursos asignados por la propia Comisión, puede desaparecer operativamente de un día para otro por decisión de su competidor, no es un instrumento de mitigación del fraude: es una fuente de inseguridad jurídica que ningún inversionista, nacional o extranjero, podrá ignorar al evaluar el sector TIC colombiano. Confiamos en que la Comisión, fiel a su mandato de garante del acceso y de la libre competencia, acogerá estas observaciones.

Firmas

En constancia de lo anterior, suscriben el presente documento de observaciones conjuntas:



BLIP-BLIP
Gabriel Díaz — Representante Legal Suplente



INALAMBRIA
Carlos Sierra — Director General



NEXVIA S.A.S.
Representante Legal — Zanya Pineda Molina