

NEXVIA S.A.S.

NIT 902.022.826-3 • PCA e Integrador Tecnológico inscrito en el RPCAI

COMENTARIOS REGULATORIOS AL PROYECTO DE RESOLUCIÓN

«Por la cual se establecen medidas para la prevención y mitigación del fraude a través de redes de servicios móviles y se modifica la Resolución CRC 5050 de 2016»

Análisis técnico-jurídico artículo por artículo, con identificación de disposiciones inconstitucionales cuya eliminación se solicita, propuestas de redacción alternativa y soporte normativo, jurisprudencial y de derecho comparado.

Dirigido a: Comisión de Regulación de Comunicaciones — CRC

Chía, Cundinamarca — Junio de 2026

I. PRESENTACIÓN E INTERÉS LEGÍTIMO

NEXVIA S.A.S., sociedad comercial identificada con NIT 902.022.826-3, inscrita ante la Comisión de Regulación de Comunicaciones en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI) en la doble calidad de Proveedor de Contenidos y Aplicaciones (PCA) e Integrador Tecnológico (IT), presenta dentro del término de participación ciudadana los siguientes comentarios al proyecto de resolución de la referencia.

El Proyecto de Resolución se presenta, según su propio título y considerandos, como un instrumento dirigido a «mitigar el fraude cibernético» y, con ello, a proteger a los usuarios de los servicios de comunicaciones. Sin embargo, un examen detenido de las medidas propuestas revela una paradoja regulatoria de la mayor gravedad: las facultades de suspensión, recuperación, bloqueo y desconexión que la propuesta concede a los Proveedores de Redes y Servicios de Telecomunicaciones (PRST) y al validador centralizado, lejos de proteger al consumidor final, lo exponen a una afectación masiva, automática e indiscriminada de comunicaciones que para él resultan esenciales. La protección al consumidor no puede invocarse como fundamento de una regulación que, en su aplicación práctica, termina sacrificando los derechos de los mismos usuarios que dice tutelar.

Esta observación se formula con fundamento en el artículo 78 de la Constitución Política, que consagra el derecho de los consumidores y usuarios a la protección de su salud, seguridad y adecuado aprovisionamiento; en el artículo 365 superior, que califica los servicios públicos como inherentes a la finalidad social del Estado y obliga a asegurar su prestación eficiente a todos los habitantes del territorio nacional; en la Ley 1341 de 2009, cuyos artículos 2 y 53 erigen la protección de los derechos de los usuarios en principio orientador de todo el sector TIC; en la Ley 2300 de 2023, que reforzó las garantías del consumidor frente a las comunicaciones y servicios de los proveedores; y en la Ley 1581 de 2012, que protege los datos personales de los titulares cuya información circula a través de la mensajería A2P.

1.1. El usuario final es el destinatario silencioso de las comunicaciones que el Proyecto pretende interrumpir

Conviene recordar que la mensajería A2P (Application-to-Person) no constituye un fin en sí misma, sino un medio a través del cual millones de colombianos acceden a servicios indispensables de su vida cotidiana. A través de los códigos cortos y los mensajes de texto cuyo flujo el Proyecto autoriza a suspender, circulan las claves dinámicas de un solo uso (OTP) que permiten el acceso a la banca digital y a las billeteras electrónicas; las alertas inmediatas de

transacciones sospechosas que constituyen la primera línea de defensa del usuario contra el fraude; las confirmaciones de operaciones de comercio electrónico; los recordatorios de citas médicas y de entrega de medicamentos de las entidades del sistema de salud; las notificaciones de las autoridades públicas; y los códigos de verificación que protegen las cuentas personales de los ciudadanos en innumerables plataformas digitales.

De lo anterior se sigue una conclusión ineludible, cada medida de suspensión o desconexión que el Proyecto autoriza no recae únicamente sobre el agente regulado (el Proveedor de Contenidos y Aplicaciones o el Integrador Tecnológico), sino que repercute de manera directa e inmediata sobre una multitud de usuarios finales que son completamente ajenos a la conducta investigada y que jamás tuvieron oportunidad de intervenir en la actuación administrativa correspondiente. El consumidor que no puede recibir el código para ingresar a su cuenta bancaria, el paciente que no es notificado de su cita médica o el comerciante que no logra confirmar una venta, padecen las consecuencias de una decisión en la que no fueron parte y respecto de la cual carecen de todo control.

1.2. La desconexión de un agente produce un efecto en cascada que perjudica a terceros de buena fe

La arquitectura del ecosistema A2P es necesariamente concatenada, el usuario final recibe el mensaje gracias a una cadena que vincula al originador del contenido, al Proveedor de Contenidos y Aplicaciones, al Integrador Tecnológico y, finalmente, al operador de red. Cuando el Proyecto faculta a un PRST para suspender unilateralmente la relación de acceso de un Integrador Tecnológico, o cuando ordena que la recuperación de un código corto produzca efectos sobre la totalidad de los Sender ID vinculados, está habilitando una verdadera sanción por arrastre que se propaga aguas abajo hasta golpear a quienes ninguna responsabilidad tiene en la conducta sancionada.

Un Integrador Tecnológico de tamaño medio puede cursar el tráfico de decenas o centenares de clientes corporativos (entidades financieras, empresas promotoras de salud, plataformas de pago, comercios) que a su vez sirven a millones de usuarios finales. La desconexión de ese único agente, decidida por un operador que es simultáneamente su competidor y su proveedor de infraestructura esencial, interrumpe de manera simultánea la totalidad de esas comunicaciones legítimas. El daño no es marginal ni reparable con facilidad, una vez interrumpido el flujo de claves dinámicas y alertas de seguridad, el usuario queda no solo privado del servicio, sino expuesto al mismo fraude que la regulación dice combatir, pues pierde precisamente los mecanismos de autenticación y notificación que lo protegen.

1.3. La medida desconoce el principio de continuidad de los servicios y afecta de modo desproporcionado a la población más vulnerable

El artículo 365 de la Constitución impone al Estado el deber de asegurar la prestación eficiente y continua de los servicios públicos. La continuidad no es una aspiración programática, sino una garantía exigible, tal como lo ha reconocido reiteradamente la jurisprudencia constitucional al amparar la prestación ininterrumpida de servicios esenciales. Las facultades de suspensión instantánea que el Proyecto contempla, sin período de transición ni régimen de continuidad para las comunicaciones críticas, contrarían frontalmente este mandato.

Esta afectación adquiere una dimensión especialmente grave si se considera que una porción significativa de la población colombiana carece de acceso a internet móvil y depende exclusivamente del mensaje de texto como canal de comunicación con su banco, su EPS y las autoridades. Para estos usuarios (habitualmente los de menores ingresos, mayor edad o residentes en zonas rurales) no existe la alternativa de recurrir a aplicaciones de mensajería basadas en datos. La interrupción del SMS no les representa una incomodidad subsanable por otra vía, sino la pérdida total del único medio de acceso a servicios financieros y de salud, lo que configura una afectación desproporcionada y discriminatoria contraria al artículo 13 de la Constitución y a los principios de acceso universal e igualdad consagrados en la Ley 1341 de 2009.

1.4 El consumidor no fue informado ni consultado, en detrimento de sus derechos a la información y a la participación

La Ley 2300 de 2023 y el Estatuto del Consumidor reconocen al usuario el derecho a recibir información clara, veraz y oportuna sobre los servicios de los que es destinatario. El usuario que confía en recibir la clave de acceso a su banca ignora por completo que la continuidad de ese servicio depende de una cadena de intermediarios susceptible de ser desconectada unilateralmente por un operador, sin aviso previo y sin que medie decisión motivada de la autoridad. El Proyecto, al concentrar en agentes privados la facultad de interrumpir estas comunicaciones, profundiza esa opacidad y deja al consumidor en una situación de absoluta indefensión informativa, pues ni siquiera podrá identificar a quién atribuir la falla del servicio ni ante quién reclamar.

1.5. La protección efectiva del consumidor exige que toda medida restrictiva sea adoptada por la CRC, con debido proceso y salvaguarda de las comunicaciones críticas

Por las razones expuestas, las sociedades suscritas sostienen respetuosamente que la genuina protección del consumidor (invocada como finalidad del Proyecto) no se logra trasladando a los operadores la facultad de interrumpir comunicaciones, sino preservando dicha

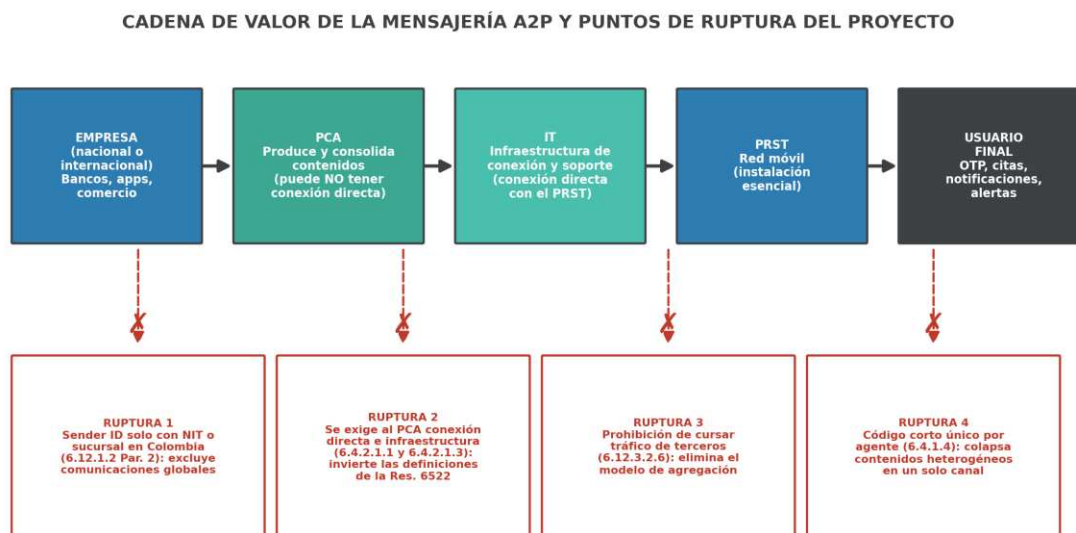
facultad en cabeza de la Comisión de Regulación de Comunicaciones, como autoridad imparcial, y sometiéndola a las garantías del debido proceso. En consecuencia, se solicita que la versión definitiva de la resolución incorpore, como mínimo, las siguientes salvaguardas en favor del usuario final.

Mientras subsista la posibilidad de que las comunicaciones esenciales de millones de usuarios sean interrumpidas como consecuencia automática de una medida dirigida contra un intermediario, y por decisión de un operador que es a la vez juez y parte, la invocación de la protección al usuario operará como un fundamento meramente nominal, desmentido por los efectos reales de la regulación.

II. OBSERVACIONES AL PROYECTO

2.1. La cadena de valor A2P

El proyecto invierte la arquitectura funcional del ecosistema que la propia CRC definió en la Resolución 6522, 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 es responsable de la producción y consolidación de contenidos y «*puede o no*» estar conectado directamente. Exigirle al PCA conexión directa e infraestructura técnica propia, prohibir el tráfico en nombre de terceros y restringir el SENDER ID a titulares con NIT colombiano rompe simultáneamente cuatro eslabones de la cadena de valor, como se ilustra a continuación:



Definiciones de PCA e IT conforme a la Resolución CRC 6522: el IT provee la infraestructura; el PCA puede o no estar conectado directamente.

Figura 1. Cadena de valor de la mensajería A2P y puntos de ruptura introducidos por el proyecto.

La consecuencia práctica no es la mitigación del fraude sino la desintermediación forzosa, las entidades financieras, las plataformas globales (redes sociales, comercio electrónico, transporte) y, en general, cualquier empresa sin sucursal en Colombia quedarían imposibilitadas de entregar comunicaciones transaccionales —incluidos códigos OTP— a los usuarios colombianos, salvo que contraten directamente con el PRST.

2.2. La arquitectura SENDER ID / código corto único: duplicación del NDC 940 y nuevo vector de confusión

Conforme al documento soporte del proyecto, la arquitectura propuesta opera así: el usuario final no ve el código corto sino el SENDER ID alfanumérico que identifica a la empresa (el propio soporte sugiere formatos como «Banco XX – Citas», «Banco XX – Transacciones» o «Banco XX Mercadeo»), mientras que, por detrás, el mensaje se cursa obligatoriamente a través del único código corto A2P asignado al PCA o IT, que actúa como matrícula técnica de trazabilidad. Para que el identificador aparezca en el dispositivo, el SENDER ID debe estar registrado en el Validador Centralizado, vinculado contractualmente a ese código corto y respaldado por una plantilla de contenido aprobada; el tráfico que no cumpla la vinculación no se entrega.

La función de dotar a cada empresa de un identificador unívoco de cara al usuario ya cuenta con un recurso de numeración diseñado exactamente para ese fin: el **NDC 940**. Bastaba ajustar su régimen para incorporar los requisitos de verificación que el proyecto persigue (titularidad de marca o razón social, soporte documental, plantillas de contenido), sin necesidad de crear un recurso alfanumérico paralelo con validador privado, causales de recuperación propias y un régimen de transición que desmonta la numeración existente.

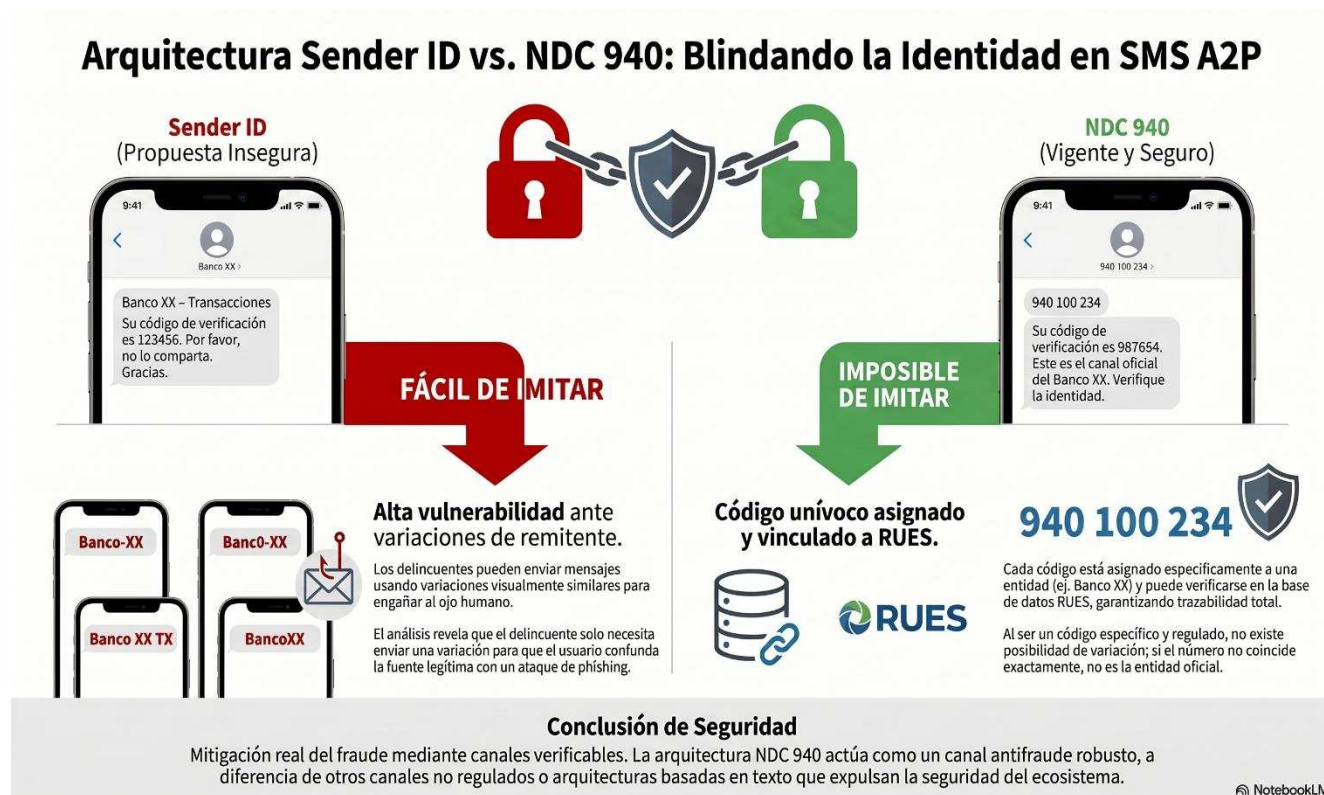


Figura 2. Comparación entre el modelo del proyecto (identificación alfanumérica imitable; código corto único reducido a matrícula técnica invisible) y el recurso preexistente NDC 940 (numeración unívoca por empresa, asignada y administrada por la CRC).

2.3. El conflicto de interés estructural del Validador Centralizado

El proyecto entrega a una persona jurídica privada (seleccionada por los PRSTM conforme a condiciones que ellos mismos elaboran (art. 18 del proyecto), pero financiada por los PCA e IT) la facultad de aprobar o rechazar las plantillas de contenido sin las cuales ningún competidor puede operar, sin recurso administrativo alguno contra sus decisiones.

CONFLICTO DE INTERÉS: PRST como Supervisor de Competidores

Denuncia de la estructura donde operadores dominantes actúan como jueces y partes en el mercado de mensajería A2P, proponiendo una transición hacia una supervisión neutral.

EL PROBLEMA

PRST es JUEZ

PRST es PARTE
(Competidor)

PRST comete FRAUDE
(venta de datos)

La falta de neutralidad permite el uso indebido de información competitiva y debilita la seguridad del SMS verificable.

Riesgo de Fraude y Venta de Datos.



LA SOLUCIÓN REQUERIDA

Validador en CRC

Autoridad reguladora neutral

Supervisión imparcial

Propuesta de trasladar la función de validador a la CRC para garantizar una supervisión imparcial.

Protección de 15,2M de Usuarios: Evita la migración forzada hacia canales sin regulación antifraude.

NotebookLM

Figura 3. Estructura de incentivos del Validador Centralizado, quien selecciona al árbitro compite contra los agentes sometidos a su control.

- **Violación del artículo 209 C.P.** La imparcialidad de la función administrativa delegada se rompe de origen, el validador depende, para su designación y permanencia, de los competidores directos de los sujetos que valida.
- **Violación del artículo 29 C.P.** El rechazo de una plantilla paraliza la operación del PCA/IT sin que el proyecto prevea recurso de reposición ni apelación, por la misma suspensión preventiva.
- **Violación de los artículos 333 y 13 C.P.** El tráfico A2P propio del PRSTM (publicidad de planes, notificaciones de cobro, OTP propios) queda exento de la validación que sí se impone a los independientes, configurando una ventaja competitiva regulatoria injustificada.

2.4. El PRST como juez y parte,

delegación inconstitucional de poder coercitivo

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 corto, y a solicitar la terminación definitiva ante la tercera.

EL PRST COMO JUEZ Y PARTE: RUTA DE DESCONEXIÓN SIN DEBIDO PROCESO

Parágrafo 4 del artículo 6.1.1.8 propuesto (Art. 8 del proyecto)

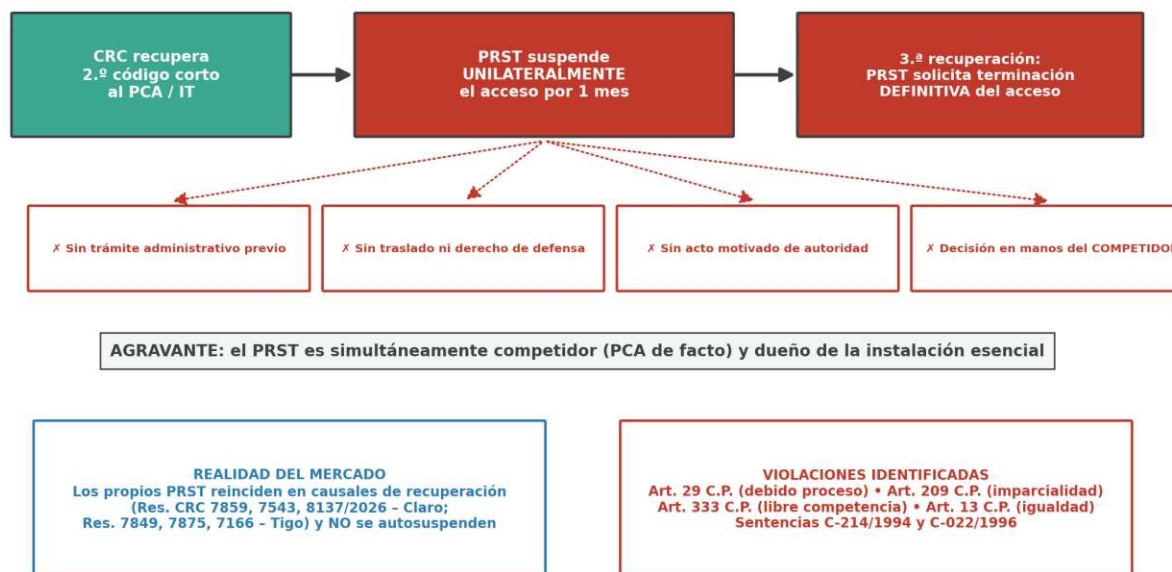


Figura 4. Ruta de desconexión prevista en el Parágrafo 4 del artículo 6.1.1.8 propuesto y garantías ausentes en cada etapa.

La medida es además innecesaria conforme al test de proporcionalidad (Sentencia C-022 de 1996): la propia CRC conserva, en el Parágrafo 3 del mismo artículo, la facultad de suspender preventivamente el recurso. Duplicar esa potestad en manos de un privado interesado no añade protección alguna al usuario; añade únicamente un instrumento de exclusión comercial.

La combinación de esta facultad con la regla de unicidad del artículo 6.4.1.4 produce un escenario que la Comisión debe evaluar, la desaparición operativa de una empresa de un momento a otro. Bajo el proyecto, el código corto único es el corazón técnico de toda la operación; recuperado el código o suspendido el acceso, se produce la invalidación masiva y automática de la totalidad de los SENDER ID vinculados y, en cuestión de segundos, un agente que procesa millones de mensajes bancarios, de salud y de seguridad pierde la capacidad de cursar cualquier tráfico. Para empresas que sostienen nóminas de decenas o centenares de empleados, una suspensión de treinta días equivale a la destrucción del flujo de caja; y como la reinterconexión con un operador puede tardar más de un año —según lo acreditan los procesos de servidumbre tramitados por la propia CRC—, el agente queda en situación de muerte súbita, sin operación comercial posible mientras sus costos fijos continúan corriendo. El proyecto transforma así una sanción administrativa en una sentencia de muerte corporativa, ignorando la realidad de las empresas que han construido infraestructura y empleo formal en Colombia.

2.5. La asimetría regulatoria: los PRST también son PCA y también reinciden

El proyecto descansa sobre la ficción de que los PRST son infraestructura neutral. La realidad documental es otra, los PRST son asignatarios masivos de códigos cortos, compiten en el mercado de contenidos y han sido objeto reiterado de recuperación de recursos de identificación por las mismas causales que el proyecto agrava únicamente para los PCA e IT independientes:

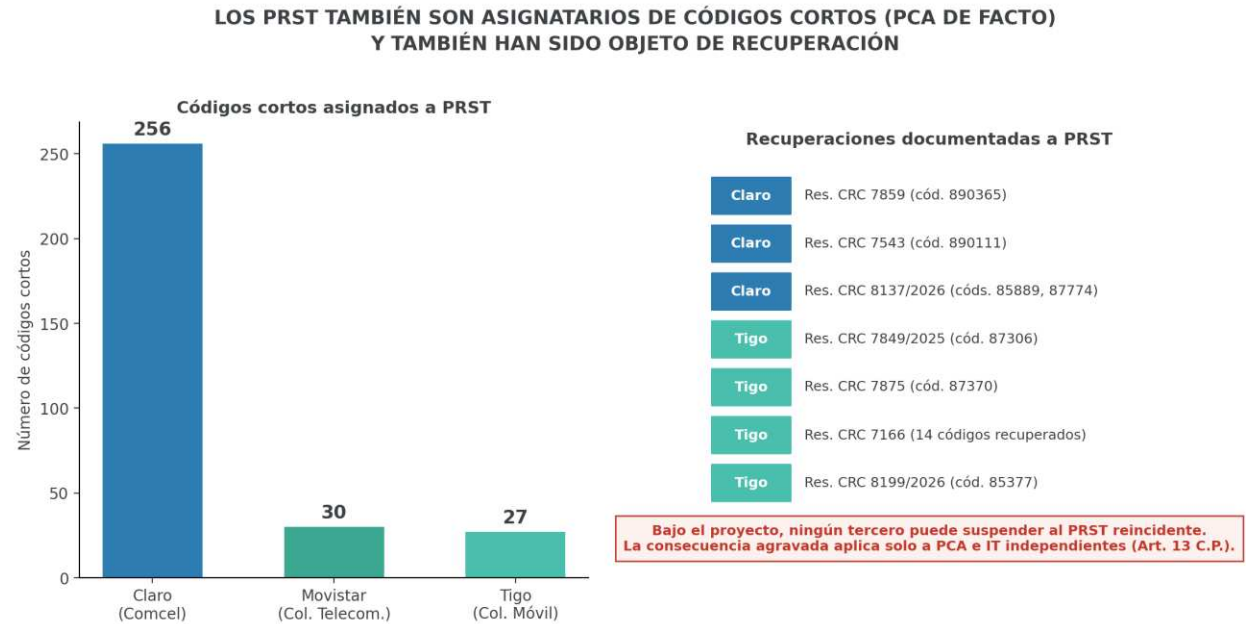


Figura 5. Códigos cortos asignados a los PRST y recuperaciones documentadas. Bajo el proyecto, la consecuencia agravada de la reincidencia (suspensión y desconexión) solo aplica a los PCA e IT independientes.

Tras la integración Tigo–Movistar autorizada en 2026, 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. El documento soporte del proyecto no contiene justificación técnica ni económica alguna para esta asimetría.

Apenas cuatro meses antes de la publicación de este proyecto, la CRC expidió la Resolución 8144 del 13 de febrero de 2026 (en cumplimiento de la sentencia del Consejo de Estado del 21 de noviembre de 2024), cuyo eje es precisamente la corrección regulatoria de las asimetrías entre agentes del mercado. Allí la Comisión reconoció que «la ausencia de estos mecanismos correctivos podría generar efectos negativos, como la afectación desproporcionada a uno de los operadores, lo que llevaría a un desequilibrio económico y competitivo», y que el mecanismo compensatorio es necesario para asegurar que «ningún operador se vea desproporcionadamente afectado por las asimetrías» y para «mantener el equilibrio en las relaciones entre operadores y fomentar una competencia justa». La misma resolución recogió la doctrina del Consejo de Estado conforme a la cual la regulación existe para «preservar o restablecer el equilibrio que debe existir entre aquellos actores que abrigan intereses legítimos

contrapuestos», y reiteró el mandato constitucional de que el Estado «evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante».

Si esa es la vara del regulador cuando las asimetrías se presentan entre PRST (incluidos los agentes de mayor músculo económico del mercado, Comcel y el grupo integrado Colombia Móvil–Colombia Telecomunicaciones), con mayor razón debe serlo cuando la asimetría enfrenta a esos mismos operadores con los PCA e Integradores Tecnológicos independientes, cuya disparidad de tamaño, infraestructura y poder de negociación frente a aquellos es incomparablemente mayor que la que existe entre dos PRST. El presente proyecto hace exactamente lo contrario de lo que la Resolución 8144 predica, en lugar de dotar de mecanismos compensatorios al agente estructuralmente más débil de la relación, amplifica la asimetría entregando al más fuerte facultades coercitivas sobre el más débil. Un regulador no puede sostener simultáneamente ambas doctrinas, o el equilibrio entre actores con intereses contrapuestos es el fin de la regulación, o se abandona ese fin cuando los beneficiarios de la asimetría son los operadores dominantes.

III. ANÁLISIS ARTÍCULOS

3.1. Numeral 4.1.2.6.5 (adición al artículo 4.1.2.6 de la Resolución CRC 5050) — Causal de oposición al acceso por «medidas suficientes»

Texto del proyecto:

~~«Que el hecho de acceder a la solicitud implique otorgarle acceso a un asignatario de códigos cortos, ya sea PCA o IT, respecto del cual la CRC había autorizado la desconexión [...] y que el referido asignatario no haya tomado las medidas suficientes para prevenir el envío de mensajes de contenido fraudulento [...] y las medidas necesarias para demostrar que no volverá a incurrir en las causales de recuperación [...]. En el evento en el que el PRST alegue esta causal, la Comisión le otorgará al PCA/IT asignatario la oportunidad para que, en el respectivo trámite administrativo, demuestre lo contrario.»~~

La disposición introduce un doble estándar indeterminado —«medidas suficientes» y «medidas necesarias para demostrar que no volverá a incurrir»— cuya calificación inicial corresponde al PRST, esto es, al competidor directo del solicitante y titular de la instalación esencial. Ello viola la garantía de legalidad y tipicidad derivada del artículo 29 C.P.: el agente no puede conocer de antemano la regla con la que será juzgado, porque la regla la define, caso a caso, su contraparte comercial.

Adicionalmente, la causal invierte la carga de la prueba en contra del solicitante de acceso («demuestre lo contrario»), exigiéndole acreditar un hecho negativo indefinido, que no volverá a incurrir en conductas futuras.

La disposición es también contraria al artículo 334 y 365 de la carta magna y a la doctrina de instalaciones esenciales, convierte al PRST en árbitro de la entrada al mercado de sus propios competidores, en un sector donde la propia CRC ha debido imponer servidumbres de acceso

(entre otras, en los expedientes promovidos contra Colombia Móvil) precisamente por la negativa y dilación sistemática de los operadores. Entregarles ahora una causal subjetiva de oposición institucionaliza la barrera de entrada que la servidumbre busca remover.

Además, la finalidad de la protección de la competencia tal como la propia Comisión la enunció en la sentencia C-815 de 2001: «*impulsar o promover la existencia de una pluralidad de oferentes que hagan efectivo el derecho a la libre elección de los consumidores*» y «*evitar la conformación de monopolios, las prácticas restrictivas de la competencia o eventuales abusos de posiciones dominantes*». Una causal que habilita al agente dominante para vetar el restablecimiento de oferentes en el mercado produce el efecto exactamente inverso al que la Comisión declara perseguir.

3.2. Parágrafo 4 del artículo 6.1.1.8 (artículo 8 del proyecto) — incisos primero y segundo — Suspensión unilateral y terminación definitiva de la relación de acceso por el PRST

Texto del proyecto:

~~«Los PRST podrán suspender provisionalmente la relación de acceso con los PCA/IT que sean asignatarios de recursos de identificación, en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto [...]. En este escenario, los PRST podrán suspender por un mes dicha relación de acceso en forma unilateral [...]. Una vez superado el referido periodo de suspensión, y en el escenario en el que la CRC recupere por tercera vez un código corto [...], los PRST podrán solicitar a la CRC la autorización para la terminación definitiva de la relación de acceso vigente [...].»~~

Esta es la disposición de mayor gravedad constitucional del proyecto. La suspensión de la relación de acceso es, desde el plano material, una sanción, priva al PCA/IT de su capacidad operativa, le impide cumplir contratos vigentes y le inflige un daño reputacional y económico que puede resultar irreversible, para una empresa del sector, un mes desconectada equivale a la pérdida de su cartera de clientes. Conforme a la Sentencia C-214 de 1994, la naturaleza de una medida se determina por sus efectos, y ninguna sanción puede imponerse sin un procedimiento previo que garantice la defensa.

Ese particular no es un tercero neutral. El PRST es simultáneamente (i) titular de la instalación esencial, (ii) asignatario de códigos cortos y (iii) competidor directo en el mercado A2P. Comcel es asignatario de 256 códigos cortos; Colombia Telecomunicaciones, de 30; Colombia Móvil, de 27. Y los tres han sido objeto de recuperación de códigos por las mismas causales que el proyecto agrava: Resoluciones CRC 7859 (código 890365), 7543 (código 890111) y 8137 de 2026 (códigos 85889 y 87774) respecto de Comcel; Resoluciones 7849 de 2025 (código 87306), 7875 (código 87370), 7166 (catorce códigos) y 8199 de 2026 (código 85377) respecto de Colombia Móvil. ¿quién suspende al PRST reincidente?. El régimen sancionatorio agravado se diseñó para operar en una sola dirección.

El Parágrafo 3 del mismo artículo ya faculta a la CRC para ordenar la suspensión preventiva del recurso durante la actuación administrativa, de modo que la suspensión por el PRST de forma unilateral, no añade protección que la autoridad no pueda brindar directamente. Y no es proporcional en sentido estricto, el costo de destruir empresas formales del ecosistema, que sostienen empleos y han obtenido su acceso, en varios casos, mediante servidumbre impuesta por la propia CRC, supera abiertamente el beneficio marginal de duplicar una facultad preexistente.

Una suspensión de treinta días no es un paréntesis administrativo, para empresas del sector que sostienen nóminas superiores al centenar de empleados, equivale a la destrucción total del flujo de caja, al incumplimiento en cadena de los contratos con clientes corporativos y a la pérdida de una cartera que tardó años en construirse. Y el retorno es inviable en los plazos que el proyecto presupone, la experiencia documentada del sector, incluidos los procesos de servidumbre tramitados por la propia Comisión, demuestra que la interconexión con un PRST puede tardar más de un año, de modo que el agente suspendido, y con mayor razón el desconectado definitivamente, carece de toda vía real para reactivar su operación mientras sus costos fijos continúan corriendo. La «suspensión provisional» del texto proyectado es, en los hechos, una condena de muerte súbita empresarial decretada por el competidor directo del condenado.

La disposición desconoce, la doctrina que la propia Comisión acaba de reiterar en la Resolución 8144 de 2026, la función de la regulación es «*preservar o restablecer el equilibrio que debe existir entre aquellos actores que abrigan intereses legítimos contrapuestos*», y el Estado «*evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional*». Facultar al actor dominante de la relación de acceso, el de mayor músculo económico, frente al cual el PCA/IT carece de todo poder de negociación, para suspender y desconectar al actor dependiente no preserva el equilibrio entre intereses contrapuestos, lo liquida, institucionalizando por vía reglamentaria el abuso de posición que el artículo 333 de la Constitución ordena al Estado evitar y controlar.

Por último, la disposición configura una delegación de poder coercitivo del Estado en particulares interesados, contraria a los artículos 113 y 209 C.P. La CRC fue creada precisamente para arbitrar con imparcialidad las relaciones de acceso, uso e interconexión (artículo 22, Ley 1341 de 2009). Se exhorta respetuosamente a la Comisión a no abdicar de esa función,

aceptar este parágrafo es renunciar, por vía reglamentaria, a la razón de ser institucional del regulador.

3.3. Artículo 6.4.1.1 (aparte final) — Naturaleza del código corto A2P, concentración de todo el tráfico en un único código

Texto del proyecto:

«A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID.»

El aparte final del artículo contradice la naturaleza del recurso definida por la propia Resolución CRC 5050, el código corto fue concebido para el posicionamiento e identificación de un tipo de servicio frente al usuario, informando el tipo de contenido, la modalidad de compra y los costos asociados, y expresamente no para la creación de canales dedicados. Bajo la arquitectura del proyecto, el usuario ya no percibe el código sino el SENDER ID alfanumérico, de modo que el código corto único queda reducido a matrícula técnica invisible, vaciado de la función que define su naturaleza, mientras las modalidades de contenido migran al SENDER ID (parágrafo del artículo 6.12.1.3 propuesto). La metodología de los códigos cortos se reproduce así bajo otro nombre, y el SENDER ID, separado ante el usuario por empresa, con plantillas y modalidades propias, pasa a operar como el canal dedicado por cliente que la doctrina del recurso proscribiera.

La finalidad legítima de identificación unívoca del remitente cuenta, además, con un recurso preexistente y diseñado exactamente para ese fin, la numeración NDC 940, susceptible de incorporar los requisitos de verificación que el proyecto persigue (titularidad del identificador, soporte documental, plantillas), sin vaciar la función del código corto ni crear un recurso alfanumérico paralelo. Ambas funciones, pueden y deben coexistir conforme al régimen vigente.

PROPUESTA DE REDACCIÓN:

«El código corto A2P es el recurso de identificación administrado por la CRC que identifica el tipo de servicio de contenidos y aplicaciones cursado por el agente que, en virtud de una relación contractual o de una servidumbre de acceso, cursa tráfico A2P de mensajería de texto (SMS). A través de los códigos cortos A2P que le sean asignados, el asignatario cursará el tráfico A2P de las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID, conservando la diferenciación de códigos por tipo de servicio, modalidad de contenido y tarifa.»

3.4. Artículo 6.4.1.4 — Unicidad del código corto A2P

Texto del proyecto:

~~«Cada solicitante tendrá derecho a la asignación de un único código corto A2P, el cual lo identificará de manera inequívoca en el ecosistema de mensajería A2P. Un mismo agente no podrá ser titular de más de un código corto A2P asignado simultáneamente.»~~

La identificación inequívoca de agentes en el ecosistema ya cuenta con un recurso de numeración específicamente creado para ese fin, el NDC 940. Reasignarle esa función al código corto desnaturaliza el recurso y duplica innecesariamente instrumentos de identificación.

La unicidad ignora el principio de uso eficiente de los recursos escasos (artículo 2, Ley 1341 de 2009) tal como la propia CRC lo ha aplicado históricamente, los asignatarios cursan tipos de servicio diversos que exigen códigos diferenciados, y la regulación vigente prohíbe que los códigos operen como canales dedicados, lo que presupone pluralidad de códigos por asignatario según el tipo de contenido.

La unicidad convierte además el código corto en punto único de falla de toda la operación. El código es el corazón técnico del agente, su recuperación, produce la invalidación masiva y

automática de la totalidad de los SENDER ID vinculados. Bajo el régimen vigente, la pluralidad de códigos opera como redundancia natural que protege la continuidad del servicio; bajo el proyecto, un solo acto administrativo, o una sola decisión unilateral del PRST conforme al Parágrafo 4 del artículo 6.1.1.8, basta para que una empresa que cursa millones de comunicaciones críticas desaparezca operativamente en segundos. Ningún principio de administración de recursos escasos justifica diseñar deliberadamente un punto único de falla sistémico sobre el cual, además, se asienta la seguridad transaccional de los usuarios.

El efecto práctico, ilustrado en la Figura 2. De un lado, el código corto único, invisible para el usuario bajo la arquitectura del proyecto, pierde toda función frente a este, la identificación inequívoca del agente que el artículo persigue es una función que la numeración NDC 940 ya cumple, sin sacrificar nada a cambio. Del otro, la identificación visible queda confiada a un recurso alfanumérico imitable mediante variaciones tipográficas y homoglifos, elevando el riesgo de suplantación visual frente al usuario, exactamente lo contrario de la finalidad antifraude declarada.

Adicionalmente, el numeral 19.1.5 del régimen de transición revela la magnitud de la afectación, obliga a devolver códigos en operación con millones de usuarios activos, imponiendo migraciones masivas cuyo costo y riesgo el documento soporte ni siquiera cuantifica.

3.5. Numerales 6.4.2.1.1 y 6.4.2.1.3 — Exigencia de conexión directa e infraestructura técnica al PCA

Texto del proyecto:

«6.4.2.1.1. Constancia de inscripción previa en el RPCAI, con indicación de si actúa en calidad de PCA con conexión directa al PRST o de integrador tecnológico. [...] 6.4.2.1.3. Descripción detallada del servicio o función que desempeñará como asignatario del código corto A2P, que incluya como mínimo la descripción de la infraestructura técnica de conexión con el o los PRST, y la identificación de los PRST con quienes mantendrá o mantiene relaciones de acceso.»

Los numerales trasladan al PCA cargas que, por definición regulatoria, corresponden al Integrador Tecnológico. La Resolución CRC 6522 es inequívoca, el PCA *«puede o no estar directamente conectado»* con los PRST, y el IT es el agente *«responsable de la provisión de infraestructura de conexión y de soporte entre los PRST y los PCA sin conexión directa»*. Exigir al PCA la descripción de infraestructura técnica de conexión propia equivale a exigirle convertirse en IT, eliminando por vía de requisitos la categoría regulatoria del PCA sin conexión directa.

La exigencia constituye además un requisito adicional para el ejercicio de una actividad ya reglamentada, en tensión con el artículo 84 C.P., y una barrera de entrada nueva en un mercado donde el acceso ya es históricamente obstaculizado por los operadores, como lo acreditan los procesos de servidumbre tramitados por la propia Comisión.

PROPUESTA DE REDACCIÓN:

«6.4.2.1.1. Constancia de inscripción previa en el RPCAI, con indicación de la calidad en la que actúa el solicitante (PCA, IT, o ambas). 6.4.2.1.3. Descripción detallada del servicio o función que desempeñará como asignatario del código corto A2P. Cuando el solicitante actúe como Integrador Tecnológico o como PCA con conexión directa, incluirá la descripción de la infraestructura técnica de conexión con el o los PRST; cuando actúe como PCA sin conexión directa, indicará el o los Integradores Tecnológicos a través de los cuales cursará su tráfico y las relaciones de acceso de estos con los PRST.»

3.6. Numeral 6.4.2.2.2 — Negación de la asignación por existencia de código corto previo

Texto del proyecto:

~~«Se verificará que el solicitante no tenga un código corto A2P previamente asignado en el SIGRI. Si existe uno previo asignado, se negará la asignación salvo solicitud simultánea de devolución del anterior.»~~

Este numeral es la regla operativa de la unicidad cuya eliminación se solicitó en el punto 3.4; cae por las mismas razones. La negación automática de asignaciones adicionales desconoce que la pluralidad de códigos responde a la diferenciación de servicios exigida por la naturaleza misma del recurso, y convierte la gestión eficiente del recurso escaso, función de la CRC, que debe evaluar caso a caso la justificación del uso.

La «solicitud simultánea de devolución del anterior» agrava el problema, en cuanto a que, fuerza la interrupción de servicios en operación, con usuarios activos, como condición para acceder a un nuevo recurso, sin régimen de continuidad que proteja las comunicaciones en curso.

3.7. Numeral 6.4.3.1.7 — Condicionamiento de todo el tráfico a plantilla aprobada en el validador

Texto del proyecto:

«A través del código corto A2P únicamente podrá cursarse tráfico A2P de personas naturales o jurídicas que cuenten con un SENDER ID previamente asignado y vigente vinculado al mismo, respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado.»

El condicionamiento absoluto del tráfico a la aprobación previa de plantillas, administrada por un validador privado sin recurso contra sus decisiones, instala un régimen de autorización previa de contenidos cuya demora o rechazo paraliza servicios críticos (OTP, alertas transaccionales, citas de salud). En mensajería transaccional, minutos de indisponibilidad generan afectaciones directas al usuario final.

El modelo proporcionado y probado internacionalmente es el de doble vía, análogo al tratamiento del CLI en voz, tráfico con plantilla verificada cursa con plena confianza; tráfico sin verificar cursa con etiquetado que advierte al usuario, sin bloqueo previo. Así se preserva la finalidad antifraude (transparencia frente al usuario) sin instituir un poder de veto privado sobre las comunicaciones.

PROPUESTA DE REDACCIÓN:

«A través del código corto A2P podrá cursarse tráfico A2P de personas naturales o jurídicas que cuenten con un SENDER ID asignado y vigente vinculado al mismo. El tráfico respaldado por una plantilla de contenido verificada y vigente se cursará como tráfico verificado. El tráfico sin plantilla verificada podrá cursarse con la marcación «sin verificar» visible para el usuario receptor, sin perjuicio de las medidas que la CRC ordene dentro de las actuaciones administrativas a que haya lugar.»

3.8. Numeral 6.4.3.2.5 — Causal de recuperación por tráfico sin SENDER ID o sin plantilla**Texto del proyecto:**

«Envío de mensajes de texto (SMS) en nombre de personas naturales o jurídicas que no cuenten con SENDER ID asignado y vigente vinculado al código corto A2P, o envío de mensajes sin respaldo de plantilla de contenido previamente aprobada y vigente en el sistema del validador centralizado.»

Elevar a causal de recuperación del código corto, castiga con la muerte operativa del canal infracciones formales subsanables, sin gradualidad alguna (requerimiento, plan de ajuste, suspensión parcial del SENDER ID involucrado).

El diseño concentra además el riesgo en cabeza equivocada, la conducta reprochable es del titular del SENDER ID o de quien origina el contenido, pero la consecuencia recae sobre el asignatario del código y, por arrastre (Parágrafo 1 del mismo artículo), sobre todos los demás SENDER ID inocentes vinculados al código, incluidas entidades cuyas comunicaciones son críticas para los usuarios.

PROPUESTA DE REDACCIÓN:

«Envío reiterado y deliberado de mensajes de texto (SMS) en nombre de personas que no cuenten con SENDER ID asignado y vigente, previa verificación de que el asignatario del código corto A2P no adoptó las medidas de control a su alcance. La configuración de esta causal exigirá requerimiento previo del Administrador de Recursos de Identificación, otorgamiento de un plazo de ajuste no inferior a diez (10) días hábiles y persistencia de la conducta. El envío de mensajes sin plantilla verificada dará lugar a la marcación del tráfico conforme al numeral 6.4.3.1.7, y solo constituirá causal de recuperación cuando se acredite su utilización para contenido fraudulento.»

3.9. Numeral 6.4.3.2.7 — Recuperación por no presentación del contrato de acceso con el PRST**Texto del proyecto:**

~~«No presentación del contrato de acceso con el PRST dentro del plazo del numeral 6.4.2.1.6 cuando la asignación quedó condicionada a ello.»~~

La causal presupone que todo asignatario de código corto debe sostener un contrato de acceso directo con el PRST, lo que (como se expuso en los puntos 3.5 y en la observación estructural

3.1) invierte la arquitectura del ecosistema, la conexión directa es la función del Integrador Tecnológico, no del PCA.

La causal ignora, además, la realidad contenciosa del acceso, la celebración del contrato no depende solo del solicitante sino de la voluntad del PRST, que históricamente niega y dilata. Un operador puede tardar más de un año en interconectar a un IT, como lo evidencian los procesos de imposición de servidumbre que la propia CRC ha debido tramitar. Sancionar al solicitante con la pérdida del recurso por una demora que el propio régimen reconoce como imputable al operador es trasladar al débil las consecuencias del incumplimiento del fuerte.

Considérese el impacto en territorios donde el mercado es especialmente frágil. Una veterinaria en zona apartada de Colombia, registrada como PCA, puede hoy tercerizar sus comunicaciones transaccionales (citas, recordatorios) a través de un IT local sin cargar con la negociación contractual directa con un PRST. Bajo el proyecto, esa veterinaria debería negociar y contratar directamente con Claro, Movistar o Tigo-Movistar (los únicos PRST del país) un acceso cuyo volumen de tráfico es microscópico comparado con sus operaciones. La solución que la Comisión ofrece a esos agentes es, migren a WhatsApp. Es una admisión implícita de que la regulación no es viable para el pequeño negocio, que es quien más depende del SMS como canal universal de comunicación donde no hay datos.

Si la Comisión estima indispensable verificar la materialización del acceso, la consecuencia proporcionada es la prórroga del plazo cuando la demora obedezca a hechos del PRST, o la activación oficiosa del trámite de solución de controversias, jamás la recuperación del recurso.

3.10. Parágrafos 1 y 2 del artículo 6.4.3.2 (recuperación del código corto A2P) — Efectos de la recuperación sobre los SENDER ID vinculados y suspensión preventiva

Texto del proyecto:

«PARÁGRAFO 1. La recuperación del código corto A2P tiene efectos sobre todos los SENDER ID vinculados. [...] otorgándoles a los asignatarios de SENDER ID treinta (30) días hábiles para acreditar una nueva relación comercial [...]. PARÁGRAFO 2. Cuando la causal de recuperación sea la del numeral 6.4.3.2.5 o la del numeral 6.4.3.2.6, la CRC podrá ordenar, en el acto de apertura de la actuación administrativa, o en cualquier estado de la actuación administrativa, la suspensión temporal del uso del recurso [...]. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses.»

El Parágrafo 1 instituye una sanción por arrastre a terceros inocentes, la recuperación del código de un asignatario priva instantáneamente de canal a todos los SENDER ID vinculados (entidades financieras, prestadores de salud, plataformas) que ninguna conducta reprochable ejecutaron. Mientras esos terceros consiguen, contratan y registran una nueva relación comercial (trámite que en la práctica no se resuelve en días), los usuarios dejan de recibir comunicaciones vitales: códigos OTP, confirmaciones transaccionales, citas médicas. La medida castiga al usuario que dice proteger.

Obsta además a la migración la realidad de la confianza operativa en el sector. La infraestructura técnica, la aprobación de las autoridades internas de riesgo y compliance, y la confianza acumulada de una relación comercial entre una entidad financiera y su proveedor IT no se trasladan de un día para otro. Los bancos no pueden designar arbitrariamente un nuevo IT sin auditoría, sin pruebas de redundancia de sistemas, sin validación de integridad de datos. La Comisión conoce esta realidad porque ha tramitado servidumbres donde los operadores han argumentado precisamente esas restricciones técnicas para dilatar la interconexión. No es coherente reconocer esas restricciones cuando impiden la conexión de nuevos operadores, e ignorarlas cuando obligan la desconexión de operadores existentes

El Parágrafo 2 permite la suspensión del recurso desde el acto de apertura, esto es, antes de cualquier ejercicio del derecho de defensa, hasta por seis meses, una medida materialmente sancionatoria anticipada, de duración equivalente a la liquidación de facto de una empresa del sector, sin las garantías mínimas de la Sentencia C-214 de 1994.

En la práctica, la habilitación del Parágrafo 2 se traduce en la inutilización del recurso en cuestión de horas desde la apertura de la actuación, antes de cualquier traslado o ejercicio del derecho de defensa. Y el término de treinta (30) días hábiles del Parágrafo 1 es técnicamente insuficiente para la migración que presupone, el titular de un SENDER ID afectado (una entidad financiera, por ejemplo) debe identificar un nuevo asignatario de código corto, negociar y suscribir el contrato, registrar la vinculación ante el validador, obtener la aprobación de sus plantillas y reconfigurar sus integraciones técnicas, una secuencia que la operación real no resuelve en ese plazo. Durante el vacío resultante, el usuario queda sin claves OTP, sin confirmaciones transaccionales y sin alertas de seguridad, el riesgo de fraude no se mitiga, se amplifica, porque el defraudador encuentra a un usuario desconectado de los canales legítimos de verificación.

El contraste con la práctica reciente de la propia Comisión es elocuente. En la Resolución 8144 de 2026, la CRC acogió la solicitud de los PRST y amplió la entrada en vigor de las medidas hasta el 1 de julio de 2026, reconociendo expresamente que se trataba de «*un tiempo razonable de aproximadamente cuatro meses y medio*» que otorga «*seguridad jurídica*», y que era necesaria una «*ventana de transición para culminar desarrollos técnicos y adelantar pruebas*» (ello para una adecuación consistente en ajustar sistemas de medición y conciliación de tráfico). No es coherente que el regulador conceda a los operadores más robustos del mercado varios meses para una adecuación de sistemas, y otorgue a terceros inocentes (cuyo canal fue suprimido por conducta ajena) treinta (30) días hábiles para una migración contractual, registral y técnica completa, de la cual dependen las comunicaciones críticas de los usuarios.

El régimen de los treinta (30) días hábiles del Parágrafo 1 presupone, para no interrumpir el servicio, que el asignatario afectado o los demás agentes del mercado disponen de códigos cortos adicionales hacia los cuales reenrutar de inmediato el tráfico de los SENDER ID vinculados. Ese presupuesto existe bajo el régimen vigente (de pluralidad de códigos) y desaparece bajo el propio proyecto, con la unicidad impuesta por el artículo 6.4.1.4, la recuperación del único código del asignatario deja a la totalidad de sus SENDER ID sin canal

alguno desde el primer día, sin posibilidad técnica de reenrutamiento interno. El proyecto destruye en un artículo el mecanismo de continuidad que presupone en otro, y la degradación del servicio recae directamente sobre los millones de usuarios finales que reciben por esos códigos sus comunicaciones críticas.

La continuidad del servicio al usuario debe ser el eje del régimen, la suspensión preventiva debe ser excepcional, motivada en riesgo grave y actual, limitada al SENDER ID o plantilla involucrados en la presunta infracción (no a todo el código), y de duración estrictamente necesaria.

PROPUESTA DE REDACCIÓN:

«PARÁGRAFO 1. La recuperación del código corto A2P no interrumpirá el tráfico de los SENDER ID vinculados ajenos a la causal que la motivó. El Administrador de Recursos de Identificación habilitará un régimen de continuidad transitoria de hasta noventa (90) días hábiles durante el cual dichos SENDER ID podrán seguir cursando tráfico a través del integrador o asignatario que designen, mientras acreditan la nueva relación comercial. PARÁGRAFO 2. La suspensión temporal del recurso solo podrá ordenarse mediante acto motivado, previa valoración de riesgo grave y actual para los usuarios, se limitará al SENDER ID o plantilla presuntamente involucrados, se revisará de oficio cada treinta (30) días y no podrá exceder de tres (3) meses.»

3.11. Parágrafo 1 del artículo 6.12.1.2 — Prohibición de asignar SENDER ID a proveedores de infraestructura**Texto del proyecto:**

~~«Los agentes que únicamente provean infraestructura de conexión para cursar tráfico de mensajes de texto (SMS) de terceros no podrán ser asignatarios de SENDER ID.»~~

La prohibición desconoce que en el mercado colombiano las calidades de PCA e IT concurren de manera habitual y legítima en un mismo agente (inscrito como tal en el RPCAI), y que los Integradores Tecnológicos requieren identificarse frente a sus propios usuarios y clientes (notificaciones de plataforma, alertas de servicio, comunicaciones operativas). Negarles de plano el SENDER ID los excluye de la identificación que el propio proyecto declara universal y obligatoria, creando una categoría de agentes formalmente inscritos, pero funcionalmente invisibles en el nuevo régimen.

3.12. Parágrafo 2 del artículo 6.12.1.2 — Un único SENDER ID por NIT y exigencia de sucursal en Colombia**Texto del proyecto:**

~~«A cada persona natural o jurídica le será asignado un único SENDER ID. La CRC solo asignará un SENDER ID por número de identificación tributaria (NIT) o por cédula de ciudadanía. [...] Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto.»~~

La exigencia de sucursal en Colombia para toda empresa extranjera que pretenda identificarse ante usuarios colombianos clausura las comunicaciones transaccionales globales. Las plataformas internacionales de uso masivo (redes sociales, comercio electrónico, transporte, servicios en la nube) 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 cuyo valor unitario es ínfimo; simplemente dejarán de llegar, o migrarán a canales no regulados, deteriorando la seguridad del usuario (el efecto exactamente inverso al buscado).

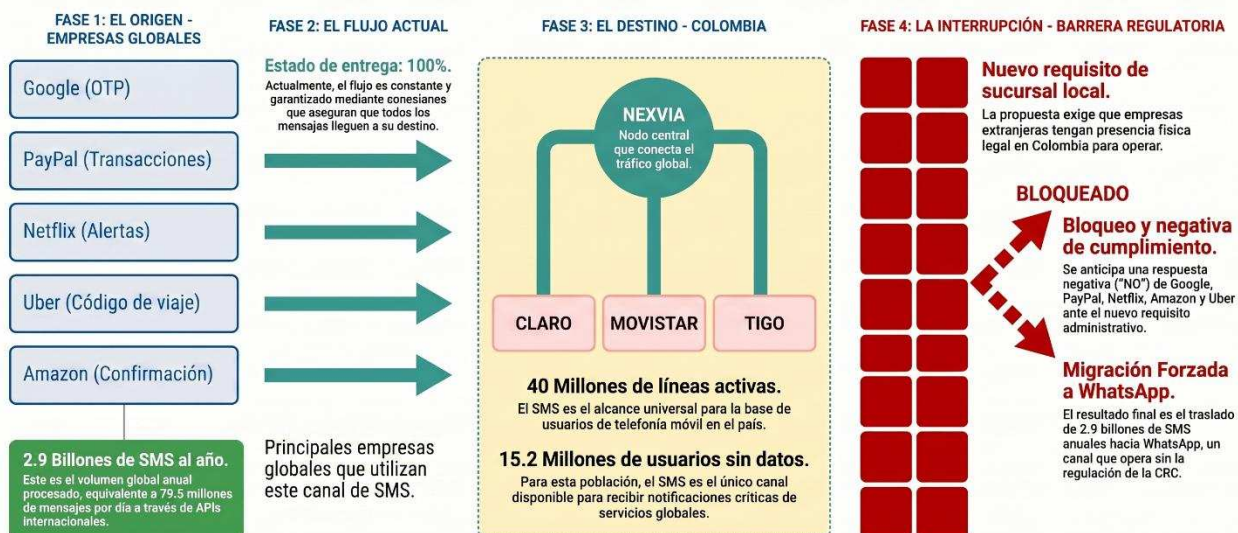
El requisito carece además de conexión con la finalidad antifraude, la trazabilidad del remitente internacional se garantiza mediante el agente local responsable (el PCA o IT que cursa el tráfico y responde por él), modelo bajo el cual el ecosistema ha operado siempre. La prohibición de cursar tráfico de terceros (numeral 6.12.3.2.6, punto 3.16) elimina simultáneamente esa vía, dejando a las comunicaciones internacionales sin ningún cauce lícito.

La regla de un único SENDER ID por NIT desconoce, por su parte, la operación real de grupos empresariales y entidades con múltiples marcas, líneas de negocio o unidades funcionales (una misma entidad financiera opera banca personal, seguros y fiduciaria con identidades comerciales distintas y registradas), forzando la confusión de comunicaciones que el recurso pretende diferenciar.

El Parágrafo 2 contradice, además, el propio documento soporte del proyecto, al ilustrar el funcionamiento del SENDER ID, el soporte sugiere formatos diferenciados por propósito dentro de una misma entidad —«Banco XX – Citas», «Banco XX – Transacciones», «Banco XX Mercadeo»—, diferenciación que el articulado hace imposible al limitar la asignación a un único SENDER ID por NIT. La motivación promete al usuario una granularidad que la norma proyectada prohíbe; la inconsistencia entre el documento soporte y el articulado constituye, en sí misma, un vicio de motivación del acto administrativo de carácter general que la Comisión está obligada a subsanar antes de su expedición.

MERCADO GLOBAL A2P: ¿CÓMO FUNCIONA HOY?

Impacto negativo de una barrera regulatoria propuesta sobre el flujo de mensajes SMS internacionales hacia Colombia, destacando cómo el requisito de una sucursal local bloquea a las empresas globales y desplaza el tráfico hacia canales no regulados



¿El objetivo real de la norma es mitigar el fraude o simplemente desplazar el mercado hacia canales no regulados sin garantías?

Nota: NotebookLM

3.13. Numerales 6.12.2.1.1, 6.12.2.1.5, 6.12.2.2.2 y 6.12.2.2.5 — Requisitos y verificaciones para la asignación del SENDER ID

Texto del proyecto:

~~«6.12.2.1.1. Constancia de inscripción previa del futuro asignatario del SENDER ID en el RPCAI como PCA. Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia [...]. 6.12.2.1.5. Identificación del código corto A2P del agente solicitante, con acreditación de que está asignado e implementado en el SIGRI y que existe contrato vigente entre el asignatario del código corto A2P y el potencial asignatario del SENDER ID. 6.12.2.2.2. Se verificará que el código corto A2P está asignado e implementado, y que el contrato [...] está vigente. 6.12.2.2.5. Se verificará que el solicitante no cuenta con un SENDER ID asignado en el SIGRI bajo el mismo número de identificación tributaria (NIT) o cédula de ciudadanía. Si existe un SENDER ID asignado para ese número de identificación, se negará la asignación.»~~

Estos numerales son las reglas operativas de las restricciones cuya eliminación se solicitó en los puntos 3.11 y 3.12, y caen con ellas: (i) la exigencia de inscripción como PCA y de sucursal nacional excluye a los titulares legítimos de marcas globales; (ii) el encadenamiento del SENDER ID a un código corto específico y a un contrato vigente con su asignatario reproduce, en cada asignación, el riesgo sistémico descrito en el punto 3.10 (recuperado el código, todos los SENDER ID encadenados quedan huérfanos y deben rehacer contratos y registros mientras el usuario deja de recibir comunicaciones); y (iii) la verificación de unicidad por NIT ejecuta la regla de SENDER ID único cuya eliminación se sustentó en el punto 3.12.

El proyecto destruye sin nombrarla la figura del Integrador Tecnológico. El IT es la calidad que requiere inversión en infraestructura, contrato de acceso directo con los PRST y desgaste administrativo frente a los operadores. Al exigir que todos los PCA cuenten con la certificación de conexión directa a un PRST (punto 3.9) y que demuestren contrato vigente (3.11, 3.12), el proyecto equipara funcionalmente a PCA e IT, disolviendo la distinción de roles sobre la cual se estructura el mercado. El regulador no lo enuncia explícitamente, sino que lo ejecuta de hecho mediante requisitos que hacen obsoleta la figura del IT, si el PCA puede (o debe) contratar directamente con el PRST, el intermediario especializado ya no tiene razón de ser. La CRC estaría alterando el mercado no mediante decisión regulatoria abierta, sino mediante una serie de obligaciones que reproduce, en cada asignación de SENDER ID, la lógica que únicamente corresponde al IT.

¿Desconectará la CRC a Colombia Móvil si incurre en causales de recuperación? ¿Desconectará a Claro? ¿Se desconectarán mutuamente en controversias de tráfico o fraude? La respuesta es evidente, no. El duopolio de hecho (Comcel y el grupo integrado Colombia Móvil-Colombia Telecomunicaciones, luego de la integración de Tigo y Movistar) opera bajo una lógica de interdependencia que la regulación respeta. Pero esa lógica no se aplica a quien depende de esos PRST. Hacia abajo, hacia los PCA e IT, el proyecto introduce facultades unilaterales de desconexión que jamás se aplicarían entre operadores. Esa asimetría es la prueba de que no se trata de una regulación neutra del fraude: es una instrumentalización de la facultad sancionadora para excluir competencia hacia el operador dominante.

El efecto sistémico del encadenamiento es la concentración del mercado en los PRST, que son también asignatarios de códigos cortos, recuperado el código de un PCA independiente, los titulares de SENDER ID vinculados (obligados a restablecer su canal en cuestión de días para no interrumpir comunicaciones críticas) migrarán hacia el asignatario que ofrezca continuidad inmediata y riesgo regulatorio mínimo, esto es, hacia el propio PRST, que controla la terminación en su red, dispone de códigos propios y no está expuesto a suspensión por terceros. Cada recuperación a un independiente opera así como una transferencia forzosa de clientela hacia el operador dominante verticalmente integrado, la sanción al PCA se convierte en premio comercial para su competidor. Ese es el diseño de mercado que subyace al articulado, y debe nombrarse como lo que es.

El encadenamiento revela, además, una contradicción interna insalvable con el régimen de desconexión del Parágrafo 4 del artículo 6.1.1.8 propuesto, si cada agente solo puede ser titular de un código corto (artículo 6.4.1.4), la recuperación de ese único código produce por sí misma la desconexión técnica del asignatario (sin código no existe tráfico que cursar), de modo que la suspensión por segunda recuperación y la terminación definitiva por tercera presuponen una pluralidad de códigos que el propio proyecto prohíbe. O el agente tiene un solo código y la primera recuperación lo desconecta de facto desde ese instante, o el régimen de reincidencia del Parágrafo 4 carece de supuesto de hecho posible. Ambas normas no pueden coexistir en el

mismo cuerpo regulatorio, y la incoherencia confirma que el articulado no fue sometido a una prueba de consistencia sistemática antes de su publicación.

El SENDER ID debe asignarse en función de la titularidad legítima del identificador (marca, razón social, denominación oficial) y de la responsabilidad verificable de un agente local que curse el tráfico, sin encadenamiento rígido a un código corto determinado, permitiendo su portabilidad operativa inmediata entre asignatarios de códigos en caso de recuperación, terminación contractual o decisión comercial.

3.14. Numeral 6.12.3.1.5 — Obligación de mantener vigente una relación contractual con un asignatario de código corto

Texto del proyecto:

~~«El asignatario deberá mantener vigente en todo momento al menos una relación contractual con un asignatario de código corto A2P con conexión directa operativa a un PRST, salvo que él mismo sea el asignatario de código corto A2P.»~~

La obligación de vigencia contractual permanente «*en todo momento*» convierte cualquier interrupción contractual ordinaria (terminación, renegociación, recuperación del código del proveedor) en causal automática de pérdida del recurso, sin periodo de gracia. Sumada al requisito de «*conexión directa operativa a un PRST*» del contratista, la regla traslada al titular del SENDER ID las contingencias de relaciones jurídicas ajenas sobre las que no tiene control alguno, en contravía de la responsabilidad subjetiva que rige el derecho administrativo sancionador.

Si la finalidad es asegurar trazabilidad, basta con exigir que el SENDER ID solo curse tráfico a través de agentes inscritos y responsables, con notificación al Administrador del cambio de canal, sin instituir la caducidad automática del recurso por vicisitudes contractuales.

3.15. Numeral 6.12.3.2.6 — Causal de recuperación del SENDER ID por envío de mensajes en nombre de terceros

Texto del proyecto:

~~«Envío de mensajes en nombre de terceros distintos al asignatario.»~~

Esta causal, combinada con la exigencia de NIT o sucursal colombiana (punto 3.12), elimina el modelo de agregación sobre el que opera la totalidad de la mensajería A2P internacional, los PCA colombianos, asignatarios de recursos y responsables ante la CRC, cursan las comunicaciones de empresas globales que no tienen presencia local. Prohibido ese tráfico, las comunicaciones internacionales hacia usuarios colombianos quedan sin cauce lícito alguno.

El efecto debe enunciarse con claridad ante la Comisión y ante los usuarios, bajo esta regla, el ciudadano colombiano que contrata bienes y servicios con empresas del exterior (derecho inherente a una economía abierta) dejará de recibir las comunicaciones asociadas a esos

servicios, incluidos los códigos de verificación que protegen sus propias cuentas. Una resolución de mitigación de fraude que suprime los OTP internacionales incrementa el riesgo del usuario en lugar de reducirlo.

La trazabilidad que la causal pretende ya se obtiene por la vía correcta, el agente local responsable responde por el tráfico que cursa, con identificación del cliente final en los registros del sistema, conforme a las prácticas de diligencia que el propio ecosistema ha implementado.

El efecto de sustitución tampoco puede ignorarse, cerrado 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 con ello la característica diferencial del SMS que justifica precisamente su protección regulatoria, llega a todo usuario con cobertura 2G, 3G, 4G o 5G, sin plan de datos, sin teléfono inteligente y sin aplicación instalada. En las zonas apartadas de Colombia, donde la red móvil básica es el único medio de comunicación disponible y buena parte de la población no contrata canal de datos o ni siquiera dispone de cobertura suficiente para usarlo, el SMS es la vía exclusiva por la que llegan las claves OTP, las citas de salud, las alertas de emergencia y las notificaciones del Estado.

Expulsar el tráfico hacia canales de datos no mitiga el fraude, lo desplaza a un terreno donde la CRC carece de toda herramienta de supervisión y, de paso, excluye de las comunicaciones a los usuarios de menor conectividad, que son los de mayor vulnerabilidad. El resultado es doblemente regresivo, menos control regulatorio y menos inclusión, en contravía directa de los principios de acceso universal y masificación de las TIC de la Ley 1341 de 2009.

3.16. Numerales 6.12.3.2.7 y 6.12.3.2.11 — Causales asociadas al RNE y a la modificación sobrevinida de modalidades

Texto del proyecto:

«6.12.3.2.7. Envío de mensajes a usuarios inscritos en el RNE cuyo envío no haya sido autorizado conforme a la modalidad de contenido de la plantilla previamente aprobada. [...] 6.12.3.2.11. Modificación, por parte del Administrador de Recursos de Identificación, de una modalidad de contenido que haga incompatible el uso del SENDER ID para dicha modalidad.»

Respecto del numeral 6.12.3.2.7: el régimen del RNE ya prevé consecuencias propias ante envíos no autorizados, y el propio proyecto reconoce, acertadamente, en el aparte sobre mensajes transaccionales, que las comunicaciones originadas en una relación de servicio vigente no requieren consentimiento adicional. La causal debe armonizarse expresamente con esa regla, exigiendo dolo o reiteración verificada y excluyendo el tráfico transaccional amparado por el vínculo servicio-usuario, para no reactivar la litigiosidad masiva por quejas individuales que el sector ya conoce.

Respecto del numeral 6.12.3.2.11: la causal hace recaer sobre el asignatario las consecuencias de una decisión sobrevenida del propio Administrador, configurando responsabilidad objetiva por hecho de la administración. La modificación de una modalidad debe operar hacia futuro, con un régimen de transición reglado que otorgue al asignatario un plazo razonable de adecuación antes de cualquier consecuencia sobre el recurso.

PROPUESTA DE REDACCIÓN:

«6.12.3.2.7. Envío deliberado o reiterado de mensajes de contenido comercial o publicitario a usuarios inscritos en el RNE sin autorización vigente, verificado mediante actuación administrativa previa. No configurará esta causal el envío de mensajes transaccionales, informativos o de seguridad amparados por una relación de servicio vigente entre el usuario y el titular del SENDER ID. 6.12.3.2.11. Cuando el Administrador de Recursos de Identificación modifique una modalidad de contenido de manera que resulte incompatible con el uso de un SENDER ID, otorgará al asignatario un plazo de adecuación no inferior a tres (3) meses, durante el cual el uso del recurso conservará plena validez.»

3.17. Numerales 6.13.4.7.2 y 6.13.4.7.4 — Bloqueo previo al enrutamiento y suspensión inmediata por orden del Administrador**Texto del proyecto:**

«6.13.4.7.2. Verificar, previo al enrutamiento de cada mensaje A2P, que cuente con un código corto A2P y un SENDER ID en estado asignado e implementado en el SIGRI, y con una plantilla de contenido aprobada y vigente [...]. En ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, y a elección del PRST, marcarlo con la etiqueta «sin verificar». [...] 6.13.4.7.4. Suspender de manera inmediata el envío de tráfico A2P asociado a un código corto A2P, SENDER ID o plantilla de contenido A2P cuando el Administrador así lo indique [...].»

El numeral 6.13.4.7.2 deja «a elección del PRST» la consecuencia de bloquear o marcar, es decir, entrega al competidor la discrecionalidad de interrumpir o degradar el tráfico de los agentes independientes. Reconocida por el propio proyecto la existencia técnica del etiquetado «sin verificar», la regla proporcionada es el etiquetado como consecuencia general y el bloqueo como excepción reglada, reservada a los supuestos de fraude identificado, nunca a la mera ausencia de plantilla aprobada, cuya demora puede ser imputable al propio validador.

El numeral 6.13.4.7.4 debe condicionarse a que la orden del Administrador provenga de un acto proferido dentro de una actuación administrativa de la CRC, motivado y notificado, con los recursos de ley; de lo contrario instituye una vía de hecho de suspensión inmediata sin control.

PROPUESTA DE REDACCIÓN:

«6.13.4.7.2. Verificar, previo al enrutamiento de cada mensaje A2P, que cuente con un código corto A2P y un SENDER ID en estado asignado e implementado en el SIGRI. El tráfico sin plantilla de contenido verificada será marcado con la etiqueta «sin verificar», visible para el usuario receptor. El bloqueo solo procederá frente a tráfico asociado a códigos cortos, SENDER ID o plantillas objeto de orden de suspensión proferida por la CRC. 6.13.4.7.4. Suspender el envío de tráfico A2P asociado a

un código corto A2P, SENDER ID o plantilla de contenido cuando así lo ordene la CRC mediante acto administrativo motivado, proferido dentro de la actuación correspondiente y notificado al afectado, contra el cual procederán los recursos de ley.»

3.18. Artículos 13, 14 y 18 del proyecto — Validador Centralizado — Selección, gobierno, financiación y régimen de impugnación del Validador Centralizado

Texto del proyecto:

«[Conjunto normativo que instituye el Validador Centralizado como persona jurídica seleccionada por los PRSTM conforme a condiciones elaboradas por estos, financiada por los PCA e IT, con facultad de aprobar o rechazar plantillas de contenido y certificaciones, sin recurso administrativo contra sus decisiones.]»

Por las razones desarrolladas en la observación estructural 3.3, el diseño del Validador vulnera los artículos 13, 29, 209 y 333 de la Constitución, selección por los competidores, financiación por los supervisados, exención del tráfico propio del seleccionador y ausencia total de recursos. No se controvierte la utilidad de una instancia técnica de verificación; se controvierte que su control corresponda a una de las partes del mercado.

La reformulación mínima exigible comprende cinco elementos: (i) selección del Validador mediante proceso público adelantado y decidido por la CRC, con requisitos de independencia verificables respecto de todos los agentes del ecosistema; (ii) gobernanza con participación de todos los actores (PRST, PCA, IT) y supervisión permanente de la Comisión; (iii) sometimiento del tráfico A2P propio de los PRST al mismo régimen de validación aplicable a los demás agentes; (iv) financiación proporcional entre todos los agentes que cursan tráfico, incluidos los PRST; y (v) recurso de reposición ante la CRC contra los rechazos de plantillas y certificaciones, con cinco (5) días hábiles para interponerlo, diez (10) días hábiles para resolverlo y efecto suspensivo (entendiéndose provisionalmente vigente la plantilla) salvo fraude activo comprobado.

Ninguna duda competencial obsta para someter el tráfico propio de los PRST al mismo régimen de validación, como la propia Comisión lo recordó en la Resolución 8144 de 2026, la regulación de la CRC tiene carácter imperativo y *«puede restringir o limitar la autonomía de la voluntad privada y la libertad económica de los PRST»* cuando persigue los fines legales de promover la competencia y evitar el abuso de la posición dominante.

Sin estos elementos, el Validador no es un instrumento de mitigación de fraude sino un mecanismo de administración privada del acceso al mercado por parte del duopolio, esto es, captura regulatoria en sentido estricto.

3.19. Numeral 19.1.5 — Régimen de transición, Fase 4 — Consolidación forzosa de códigos cortos

Texto del proyecto:

~~«Los asignatarios que durante el período de transición tengan múltiples códigos cortos [...] deberán consolidar su numeración hacia el único código corto A2P asignado [...]; elección del código corto a conservar [...]; plan de consolidación con cronograma de devolución de los códigos cortos excedentes; número estimado de usuarios activos afectados por cada código corto a devolver; mecanismo técnico de migración [...]; recuperación de códigos cortos excedentes [...].»~~

El numeral es la ejecución transitoria de la unicidad cuya eliminación se sustentó en los puntos 3.3, 3.4 y 3.6, y debe correr su misma suerte. El propio texto admite la magnitud del daño que ordena, exige estimar el «número de usuarios activos afectados por cada código corto a devolver», esto es, reconoce que la medida afecta servicios en operación con usuarios reales, 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.

La consolidación es además internamente contradictoria con el propio proyecto, tras la migración forzosa, el código único concentrará exactamente la mezcla de contenidos heterogéneos que la naturaleza del recurso prohíbe, y los asignatarios que no acrediten conexión directa (la mayoría de los PCA, conforme a las definiciones vigentes) ni siquiera podrán conservar código alguno, expulsándolos del mercado por vía transitoria.

La propia Comisión fijó el estándar de los regímenes de transición en la Resolución 8144 de 2026, cuando los PRST manifestaron la necesidad técnica de ajustar sus sistemas de medición de tráfico, la CRC amplió la vigencia de las medidas en cuatro meses y medio para otorgar «seguridad jurídica y un tiempo razonable», con una «ventana de transición para culminar desarrollos técnicos y adelantar pruebas» destinada a «asegurar la integridad y confiabilidad de los datos». La consolidación forzosa del numeral 19.1.5, que implica migrar servicios con millones de usuarios activos, devolver recursos en operación, renegociar contratos y reconfigurar plataformas, recibe en cambio plazos perentorios de diez (10) y quince (15) días hábiles para decisiones estructurales, sin ventana de pruebas alguna. La asimetría de trato procedimental entre los operadores y los demás agentes del ecosistema opera, otra vez, como regla no escrita del proyecto.

3.20. Artículos 2.1.10.7.2.2.x — Etiquetado de llamadas por el PRST — Detección, etiquetado y resolución de solicitudes sin verificación independiente

Texto del proyecto:

«Cuando el sistema de monitoreo detecte alguno de estos patrones, el PRST deberá etiquetar las llamadas originadas desde el número o rango de numeración involucrado con la indicación «Alerta de llamada sospechosa» [...]. El etiquetado tendrá carácter temporal y se mantendrá mientras persista el patrón detectado. [...] Una vez recibida la solicitud, el PRST analizará la información aportada por el titular y podrá requerir información adicional dentro de los tres (3) días hábiles siguientes. El plazo total para resolver no podrá exceder de diez (10) días hábiles [...].»

En materia de voz, el proyecto deposita en el PRST la totalidad del ciclo, detección, etiquetado, mantenimiento de la marca y resolución de las reclamaciones del titular afectado, sin prever organismo, auditoría ni reporte alguno que verifique la correcta aplicación de las medidas. La asimetría con el régimen de SMS es notoria, para los mensajes de los agentes independientes se crea un validador, plantillas, registros y causales de recuperación; para las llamadas, gestionadas por los propios operadores, se confía en la autorregulación sin control. Ello pese a que la modalidad de mayor efectividad defraudatoria es precisamente la llamada de suplantación de entidades, frente a la cual el SMS (por su carácter asincrónico y verificable) ofrece al usuario mayor capacidad de reacción.

PROPUESTA DE REDACCIÓN:

«Adiciónese: «El PRST reportará mensualmente a la CRC y al CTLFSM los números y rangos etiquetados, los patrones que motivaron el etiquetado, su duración y las solicitudes de retiro recibidas y su resultado. La CRC podrá auditar en cualquier momento los sistemas de monitoreo y ordenar el retiro de etiquetas impuestas sin justificación. Contra la decisión del PRST que niegue el retiro del etiquetado, el titular podrá acudir ante la CRC, que resolverá de plano en un término máximo de diez (10) días hábiles.»»

3.21. Artículo 2.1.10.7.3 — Comité Técnico de Lucha contra el Fraude (CTLFSM) — Composición del Comité y participación de los agentes del ecosistema**Texto del proyecto:**

«Créase el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles [...] como instancia de intercambio de alertas, identificación de patrones de fraude y espacio de revisión técnica de medidas frente al fraude cibernético [...]. El CTLFSM será liderado y convocado por la CRC [...]. [El artículo 2.1.10.7.2.1.4 impone la participación obligatoria a los PRST.]»

El Comité es una iniciativa valiosa que NEXVIA respalda, la inteligencia compartida en tiempo real es la herramienta antifraude de mayor efectividad comprobada. Precisamente por ello, su composición no puede limitarse a los PRST, los PCA e Integradores Tecnológicos operan la primera línea de detección del fraude A2P, filtrado de contenidos, bloqueo de cuentas, identificación de patrones de suplantación, SIM boxing y SMS pumping, y disponen de información operativa que los operadores de red no ven. Excluirlos del órgano donde se acordarán las mejoras a los parámetros mínimos de detección (artículo 2.1.10.7.2.1.4) significa que las reglas que los obligan se negociarán sin ellos, en contravía del principio de participación del artículo 2 C.P. y del CPACA.

PROPUESTA DE REDACCIÓN:

«Adiciónese al artículo 2.1.10.7.3: «Serán miembros permanentes del CTLFSM, con voz y voto en la revisión técnica de medidas y parámetros de detección, los PCA y los Integradores Tecnológicos

inscritos en el RPCAI que manifiesten su voluntad de participar, así como las autoridades que la CRC convoque. La CRC garantizará la representación equilibrada de todos los segmentos del ecosistema en las decisiones del Comité.»»

VI. MODELO ALTERNATIVO PROPUESTO

Las objeciones precedentes no dejan a la Comisión sin instrumentos. NEXVIA propone un modelo que preserva íntegramente la finalidad antifraude del proyecto, devolviendo la función coercitiva a su titular constitucional:

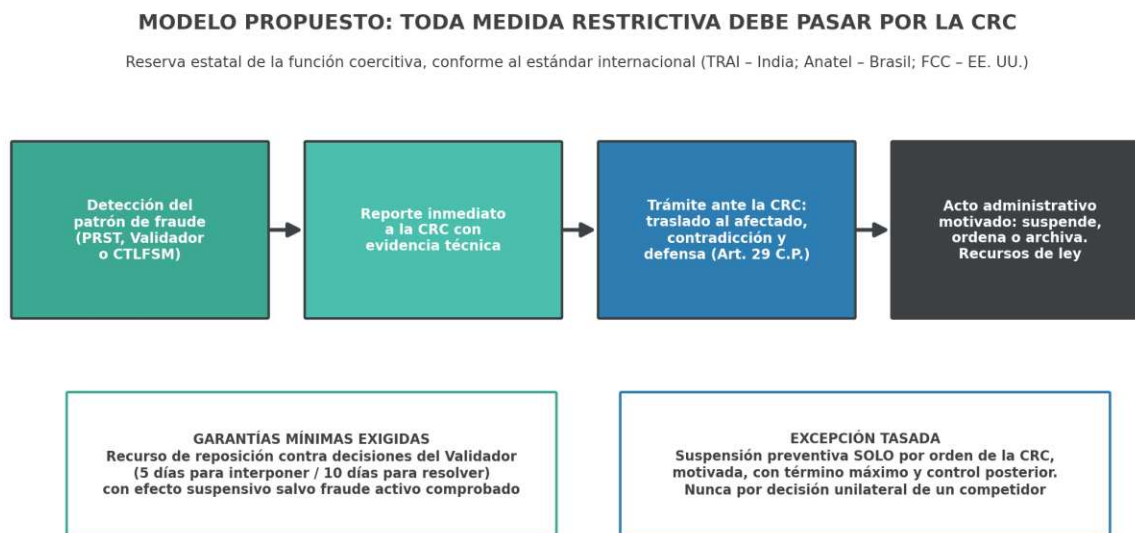


Figura 6. Modelo propuesto: detección distribuida, decisión estatal. Toda medida restrictiva de derechos pasa por la CRC mediante acto motivado, con garantías de contradicción y recursos.

- **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 defensa. Los PRST y el Validador detectan y reportan; no sancionan.
- **Validador independiente bajo control de la CRC.** Selección pública por la Comisión, gobernanza multiactor, validación simétrica del tráfico de todos los agentes, incluidos los PRST, y recurso de reposición con efecto suspensivo contra sus rechazos.
- **Etiquetado sobre bloqueo.** El tráfico sin plantilla verificada se marca «sin verificar», trasladando la información al usuario sin interrumpir comunicaciones; el bloqueo se reserva al fraude identificado mediante orden de autoridad.
- **Continuidad del servicio como principio.** Régimen de portabilidad inmediata del SENDER ID entre asignatarios de códigos y continuidad transitoria del tráfico de terceros

inocentes ante recuperaciones, protegiendo los OTP y comunicaciones críticas de los usuarios.

- **Inteligencia compartida e inclusiva.** CTLFSM con membresía plena de PCA e IT, plataforma de alertas en tiempo real y revisión periódica de parámetros de detección con participación de todos los segmentos.

IV. SOLICITUDES CONCRETAS

Con fundamento en lo expuesto, NEXVIA S.A.S. solicita respetuosamente a la Comisión de Regulación de Comunicaciones:

PRIMERO. ELIMINAR del proyecto el numeral 4.1.2.6.5; los incisos primero y segundo del Parágrafo 4 del artículo 6.1.1.8; el artículo 6.4.1.4; los numerales 6.4.2.2.2, 6.4.3.2.7, 6.12.3.1.5 y 6.12.3.2.6; los Parágrafos 1 y 2 del artículo 6.12.1.2; los numerales 6.12.2.1.1, 6.12.2.1.5, 6.12.2.2.2 y 6.12.2.2.5; y el numeral 19.1.5 del régimen de transición, conforme a la sustentación de la Sección V.

SEGUNDO. MODIFICAR las disposiciones identificadas con modificación en la Sección V, adoptando las redacciones alternativas allí propuestas o aquellas que, preservando su sentido garantista, la Comisión estime técnicamente preferibles.

TERCERO. REFORMULAR estructuralmente el régimen del Validador Centralizado (artículos 13, 14 y 18 del proyecto) conforme a los cinco elementos mínimos señalados en el punto 5.18: selección pública por la CRC, gobernanza multiactor, validación simétrica del tráfico de los PRST, financiación proporcional y recurso de reposición con efecto suspensivo.

CUARTO. INCORPORAR a los PCA e Integradores Tecnológicos como miembros permanentes del CTLFSM, con voz y voto en la revisión técnica de medidas y parámetros de detección.

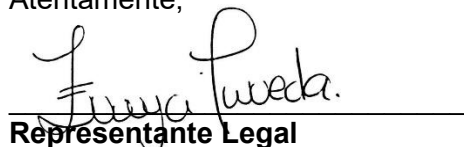
QUINTO. PUBLICAR, antes de la expedición de la resolución definitiva, el análisis de impacto normativo que cuantifique los efectos de la unicidad del código corto, de la consolidación forzosa y de las restricciones al SENDER ID sobre los usuarios, los agentes del ecosistema y las comunicaciones internacionales, con la respuesta motivada a los comentarios recibidos, conforme al deber de motivación de los actos administrativos de carácter general y al estándar que la propia Comisión aplicó en la Resolución 8144 de 2026, en la que evaluó las alternativas regulatorias bajo la metodología de Análisis de Impacto Normativo con cuantificación de los costos administrativos de cada una, adelantó mesas de trabajo con los agentes que formularon observaciones, surtió la abogacía de la competencia ante la SIC conforme al artículo 7 de la Ley 1340 de 2009 y elaboró el documento de respuesta a comentarios exigido por el parágrafo del artículo 2.2.13.3.3 del Decreto 1078 de 2015.

SEXTO. CONVOCAR una mesa técnica con la participación de PCA e Integradores Tecnológicos para la revisión conjunta del articulado, en la que NEXVIA manifiesta desde ya su plena

disposición a participar y a aportar su experiencia operativa en detección y mitigación de fraude A2P.

La lucha contra el fraude es una causa que NEXVIA comparte y en la que ha invertido capacidades técnicas propias. Precisamente por ello insistimos, las medidas eficaces contra el fraude fortalecen la institucionalidad del regulador; las medidas que trasladan el poder del regulador a los regulados 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 legal de garante del acceso y de la libre competencia, acogerá estas observaciones.

Atentamente,



Representante Legal

NEXVIA S.A.S. — NIT 902.022.826-3

Abogada — T.P. 445152 del C.S.J.