

Bogotá D.C., 22 de junio de 2026

Doctor
FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo
Comisión de Regulación de Comunicaciones - CRC
La ciudad

Asunto: Comentarios al *Proyecto de Resolución «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones»*, en lo relativo a las medidas sobre servicios tradicionales de voz; solicitud de abstención respecto del bloqueo de llamadas con CLI nacional.

Respetado Doctor Díaz Suaza:

En condición de proveedor de redes y servicios de telecomunicaciones habilitado para la prestación del servicio de larga distancia internacional (LDI), y por tanto interesado directo en la regulación del tráfico internacional de voz, presentamos dentro del término nuestros comentarios al proyecto de la referencia, circunscritos a las disposiciones sobre prevención del fraude en los servicios tradicionales de voz.

Compartimos plenamente el objetivo del proyecto: combatir el fraude y proteger al usuario. El presente escrito no controvierte ese fin, sino el **medio** elegido para alcanzarlo. Solicitamos respetuosamente que la Comisión **se abstenga de adoptar el bloqueo de las llamadas con identificador de línea llamante (CLI) nacional como regla general**, por las razones de fondo y de procedimiento que se exponen, y adopte en su lugar un mecanismo de verificación y autenticación de origen, que sirve mejor al mismo objetivo.

Adicionalmente, es importante que la CRC haga un análisis jurídico sobre la medida que se quiere adoptar y su impacto sobre la violación al principio de neutralidad de red, principio de origen legal y que su limitación debe estar regido por otra Ley o por orden de autoridad judicial. Asimismo, el bloqueo planteado, afecta a algunos usuarios, que de acuerdo al estudio, no se plantea un mecanismo para evitar vulnerar el derecho de esas personas, ni la forma de restablecerlo; por lo que se solicita una referencia así sea sumaria sobre esos dos puntos.

I. El objetivo es compartido; el problema es la imposibilidad de distinguir el origen

El fraude telefónico es un fenómeno grave que exige acción decidida del Estado, y los operadores son los primeros perjudicados por él. La discusión no está en el fin, sino en cómo alcanzarlo sin causar un daño mayor que el que se quiere evitar.

La raíz del problema es una sola: en la señalización tradicional no es posible distinguir, de forma confiable, el origen real de una llamada que entra del exterior presentando un CLI nacional. Esa imposibilidad afecta por igual a los tres actores del ecosistema:

- **El usuario** no puede saber, al recibir la llamada, si quien lo contacta es realmente su banco o un defraudador que presenta el mismo número; por ello cae en el engaño.

- **El operador de LDI** no puede acreditar ante la red de destino que un tráfico legítimo lo es, ni separarlo del fraudulento, pues la información del originador se diluye en la cadena internacional de intermediarios, y dificulta al operador nacional, así sea de LDI conocer la procedencia completa del tráfico, con el agravante que ese tipo de exigencias a los prestadores internacionales - conectantes – pueden no ser de recibo o simplemente hacen que se tomen medidas de enmascarar mucho antes de que sea entregadas a nosotros.
- **La autoridad y los operadores móviles** no pueden distinguir la llamada legítima de la suplantada, y ante esa ceguera se ven tentados a tratar todo el tráfico por igual.

Esa carencia común tiene un nombre técnico: **falta de trazabilidad y autenticación del origen**. Es la causa estructural. El fraude, el riesgo para el tráfico legítimo y la dificultad regulatoria son manifestaciones de la misma ausencia. Cualquier medida que no ataque esa causa –sino solo uno de sus síntomas– resultará, por definición, ineficaz.

Por qué existe tráfico con CLI nacional cursado por ruta internacional

Conviene precisar, ante todo, por qué una llamada que presenta un número colombiano puede ingresar al país por una ruta internacional, pues de ello depende comprender que no se trata de una anomalía sospechosa, sino de la forma en que operan hoy las comunicaciones empresariales. Según se advirtió en la etapa anterior de este proceso, sin que la observación fuera atendida, las empresas que se comunican con sus clientes –entidades financieras, aseguradoras, aerolíneas, prestadores de salud, comercios– ya no lo hacen, en su mayoría, desde infraestructura física ubicada en Colombia, sino a través de plataformas tecnológicas en la nube (CPaaS/OTT) y de centros de contacto cuya infraestructura se encuentra en el exterior. Cuando esas plataformas cursan una llamada en nombre de la empresa, presentan el número colombiano que legítimamente le pertenece al cliente, aunque la llamada se origine técnicamente en infraestructura internacional. La numeración es real y está asignada al cliente; **lo que es internacional es el medio que la transporta**.

En la práctica, esta operación supone que el titular de la numeración autoriza a la plataforma a presentar su número como identificador de línea llamante cuando cursa comunicaciones en su nombre. Esa autorización ocurre hoy de hecho, pero sin un soporte documental estandarizado ni un mecanismo regulatorio que permita acreditarla; en ningún caso implica cesión ni transferencia del recurso, que permanece asignado al cliente y bajo su responsabilidad. Formalizar y hacer verificable esa cadena de autorización es, precisamente, uno de los objetos del esquema de verificación de origen que más adelante se propone.

Este tráfico no busca ocultar su origen ni eludir obligación alguna: paga el cargo de acceso regulado por su terminación y corresponde a comunicaciones empresariales lícitas –verificaciones, cobranzas autorizadas, atención al cliente y notificaciones transaccionales–, que ascienden a millones de comunicaciones al año. De hecho, constituye hoy la mayor parte del tráfico de larga distancia internacional –estimado en alrededor del 80%, **proporción que la propia Comisión debe verificar**–, como consecuencia de la migración global de las comunicaciones empresariales hacia plataformas en la nube.

Debe distinguirse, por tanto, de la suplantación fraudulenta: ambos pueden presentar un CLI nacional desde el exterior, pero el primero corresponde a un cliente real e identificable que ha autorizado el uso de su número, mientras el segundo oculta deliberadamente su origen. Esa distinción –imposible de establecer

con el solo dato de la nacionalidad del CLI— es precisamente lo que un mecanismo de verificación de origen permitiría acreditar, y lo que el bloqueo indiscriminado ignora.

II. El bloqueo del CLI nacional no supera el test de proporcionalidad

Texto del proyecto (artículo 2.1.10.7.2.2.1, primer inciso):

“Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de tráfico de roaming internacional debidamente identificado como tal por el carrier de origen.”

Toda medida regulatoria que restringe derechos —en este caso, el derecho del usuario a recibir información veraz e imparcial, reconocido como principio orientador en el artículo 2, numeral 7, de la Ley 1341 de 2009 (en desarrollo de los artículos 20 y 15 de la Constitución Política), así como su derecho a la adecuada y eficiente provisión del servicio de comunicaciones, que la CRC está obligada a proteger conforme a los artículos 2.4, 4.1, 7 y 19 de la misma Ley— debe superar el test de proporcionalidad exigido por la jurisprudencia constitucional, además de ajustarse a los principios de mínima intervención y regulación eficiente que enmarcan la actuación de la CRC. El bloqueo del prefijo +57 en la ruta de tráfico internacional suprime de forma indiscriminada llamadas lícitas que el usuario quiere y necesita recibir, interfiriendo el canal de comunicación sin un análisis individualizado de cada llamada. La medida no supera ninguna de las tres gradas del test —idoneidad, necesidad y proporcionalidad en sentido estricto—.

1. No es idóneo (no sirve para el fin)

Qué exige este requisito: una medida solo es válida si efectivamente conduce a lograr el objetivo que persigue.

El bloqueo se condiciona a que el número tenga apariencia colombiana, pero el defraudador evade la medida con solo usar un número de otro país, o trasladándose a aplicaciones de mensajería (OTT), y sigue estafando igual. Una medida que el propio defraudador esquivo con un cambio tan simple no sirve para combatir el fraude: actúa sobre una apariencia —la nacionalidad del número— y no sobre la causa real, que es la imposibilidad de verificar el verdadero origen de la llamada.

Adicionalmente, nosotros los prestadores en Colombia (conexión con el exterior) no podemos adoptar medidas como bloqueos, desconexión provisional, o cuarentenas que ejerzan alguna presión sobre las conectantes internacionales y evitar que se sigan presentando estos eventos, ya que ellos van a seguir entregando tráfico que pueden enmascarar con numeración de otros países similar a la asignada en Colombia. Por ello, el control y la gestión de su tráfico anómalo resultan inocuos, y la medida recae sobre el eslabón equivocado de la cadena: el prestador nacional, que no tiene cómo incidir sobre el verdadero origen del fraude.

2. No es necesario (existe un medio menos lesivo, que la propia resolución ya emplea)

Qué exige este requisito: si hay otra forma de lograr el mismo objetivo causando menos daño, la autoridad está obligada a escoger esa, no la más drástica.

Ese medio menos drástico existe, y la propia resolución lo usa: en el artículo 2.1.10.7.2.2.2 ordena **etiquetar** las llamadas sospechosas con una alerta visible («Alerta de llamada sospechosa»), en lugar de bloquearlas.

Es decir, frente a un riesgo de fraude en voz, la Comisión ya eligió advertir al usuario en vez de cortar la llamada. Si para unos casos basta con etiquetar, no se entiende por qué para el tráfico internacional se acude al bloqueo total, que es la medida más severa. El etiquetado, acompañado de la verificación del origen, permite que la autoridad y el usuario distingan lo legítimo de lo fraudulento sin suprimir comunicaciones lícitas: ataca la causa del problema, no su apariencia. La existencia de este medio menos lesivo e igualmente idóneo, ya adoptado por la propia Comisión para supuestos análogos, basta por sí sola para que la medida no supere el test de proporcionalidad, pues su análisis es secuencial y el fracaso de una sola grada determina su invalidez.

3. No es proporcional en sentido estricto (el daño que causa es mayor que el beneficio que produce)

Qué exige este requisito: el beneficio que se obtiene debe ser mayor que el daño que se causa; si el daño pesa más, la medida no se justifica.

El bloqueo elimina comunicaciones legítimas que el usuario quiere y necesita recibir —la verificación de su banco, la confirmación de una cita médica, el aviso de su aerolínea, la cobranza autorizada—, así como la actividad lícita de las empresas que las realizan. A cambio, obtiene un beneficio parcial y fácilmente evadible: el defraudador lo sortea con un simple cambio de numeración. El usuario no queda más protegido: queda desconectado de servicios que necesita, mientras el estafador lo alcanza por otra vía. El daño es cierto; el beneficio, parcial y evadible. La medida causa más perjuicio que provecho.

Conclusión: el bloqueo restringe derechos sin ser necesario para su fin —existiendo un medio menos lesivo e igualmente eficaz que la propia Comisión ya adopta— y sin superar la proporcionalidad en sentido estricto, con una idoneidad además deficiente por no atacar la causa real del fraude. Vulnera, por ello, el derecho del usuario a recibir información (artículo 2, numeral 7, de la Ley 1341 de 2009 y artículo 20 de la Constitución Política) y los principios de mínima intervención y regulación eficiente que rigen la actuación de la CRC (artículos 2.4, 4.1, 7 y 19 de la Ley 1341 de 2009).

III. El bloqueo distorsiona la competencia sin justificación económica

El bloqueo carece de justificación económica y, además, distorsiona la competencia en perjuicio del sector regulado. No protege ningún ingreso de los operadores —el cargo de acceso por terminación ya está garantizado por la regulación, con independencia del bloqueo— y, en cambio, desplaza tráfico legítimo hacia plataformas que no pagan ese cargo ni están sujetas a la regulación sectorial. Se demuestra en dos pasos.

1. El bloqueo no protege ningún ingreso del operador móvil

Cuando un operador de Larga Distancia Internacional (LDI) entrega una llamada al operador móvil para que la termine, le paga el cargo de acceso, que es un peaje regulado por la propia Comisión. El artículo

4.3.2.8 de la Resolución CRC 5050 de 2016, modificado por la Resolución CRC 7753 de 2025, establece que los proveedores de Larga Distancia Internacional pagan cargos de acceso por origenación y por terminación en las redes móviles.

El operador móvil recibe así su remuneración regulada por terminar la llamada, con independencia de la ruta por la que esta llegue. En consecuencia, no existe ningún ingreso del operador que termina la llamada que el bloqueo venga a proteger: ese ingreso proviene del cargo de acceso ya tasado por la Comisión y no depende de bloquear unas llamadas y permitir otras. La medida carece, por este lado, de toda justificación económica.

2. El bloqueo desplaza tráfico legítimo del sector regulado hacia las plataformas OTT no reguladas

Descartada la protección de ingresos, el bloqueo no resulta neutro sobre la estructura del mercado. Una parte sustancial del tráfico internacional con CLI nacional corresponde a comunicaciones legítimas de empresas hacia sus usuarios –avisos comerciales, gestiones de cobranza, notificaciones de servicio–. Bloqueada la ruta de voz, ese tráfico no desaparece: migra hacia las plataformas OTT –señaladamente WhatsApp, que ya ofrece en Colombia productos pagos de mensajería de negocios y de llamadas comerciales, con tarifas fijadas por Meta según el país de destino del usuario¹–, las cuales terminan la comunicación sobre la red de datos sin pagar cargos de acceso, sin asumir contraprestaciones y sin estar sujetas al régimen de calidad ni a la regulación sectorial de la CRC.

El efecto recae sobre el propio sector regulado, y de manera más aguda sobre los operadores de LDI. Por un lado, los operadores de LDI pierden el transporte de ese tráfico y el margen asociado; el perjuicio es especialmente grave para los operadores de LDI independientes, que carecen de red móvil propia y, a diferencia de los operadores integrados verticalmente, no tienen forma de compensar la pérdida, al punto de que el **bloqueo puede comprometer la viabilidad misma de su línea de negocio**. Por otro lado, los operadores móviles dejan de percibir el cargo de acceso de voz, pues la comunicación se termina como dato a través de la plataforma. El único beneficiario es un actor –Meta, a través de WhatsApp– que no soporta las cargas regulatorias, tributarias ni de calidad que la Comisión impone a sus regulados.

Así, una medida expedida por la CRC para proteger a los usuarios de sus servicios termina trasladando tráfico legítimo –y los ingresos que lo acompañan– desde los operadores que ella regula hacia plataformas que escapan a esa regulación. Esa redistribución no obedece a que los operadores regulados compitan peor, ofrezcan peor precio o menor calidad, sino a una prohibición regulatoria que cierra la ruta de voz y acelera la migración hacia las OTT. Se trata, por tanto, de una distorsión de la competencia por vía administrativa, no por las dinámicas propias del mercado.

En síntesis, el bloqueo no protege ingreso alguno –pues el cargo de acceso ya lo garantiza– y, en cambio, desplaza tráfico legítimo desde los operadores regulados, especialmente los de LDI, hacia las plataformas OTT no reguladas, en perjuicio de la competencia en el sector. Ese efecto sobre la estructura del mercado es precisamente el que debe evaluar la Superintendencia de Industria y Comercio en sede de abogacía de la competencia, conforme se desarrolla en la sección V de este escrito, antes de la adopción de la medida.

¹ WhatsApp Business Platform ofrece productos de mensajería de negocios (categorías marketing, utility y authentication) y de llamadas salientes de negocios (WhatsApp Business Calling). Las llamadas se facturan por minuto, en pulsos de seis segundos y solo cuando el usuario contesta, con tarifa según el código de país del destinatario. Colombia cuenta con rate card propio en pesos colombianos (COP) y fue objeto de actualización tarifaria en mensajería con efecto a partir del 1 de octubre de 2025. Fuente: documentación oficial de precios de WhatsApp Business Platform, Meta (developers.facebook.com).

IV. El Análisis de Impacto Normativo es deficiente: no midió el tráfico legítimo afectado

El documento soporte contiene un Análisis de Impacto Normativo (AIN) con metodología multicriterio y análisis costo-beneficio. No se objeta su existencia, sino su contenido: respecto del bloqueo, el AIN adolece de omisiones concretas y verificables que vician su conclusión.

1. El AIN no cuantificó el tráfico legítimo con CLI nacional cursado por los operadores de LDI

El análisis costo-beneficio del bloqueo (alternativa de prohibición total del enmascaramiento del CLI) presenta dos defectos que operan en la misma dirección:

- El beneficio se estimó por analogía con experiencias internacionales —Irlanda y Australia—, asumiendo porcentajes de reducción del fraude (entre 60% y 90%), y no a partir de datos del tráfico internacional entrante en Colombia. **El AIN no contiene ninguna cifra del volumen de llamadas internacionales entrantes con CLI nacional**, ni de la proporción que de ellas corresponde a fraude frente a comunicaciones legítimas.
- El costo del bloqueo no incluyó el del tráfico legítimo que quedaría suprimido. El análisis de falsos positivos se aplicó únicamente a la alternativa de etiquetado —como argumento en su contra—, pero no a la del bloqueo, pese a que el bloqueo produce el falso positivo más grave: **la eliminación total de la comunicación legítima**, no su simple advertencia.

En consecuencia, el cálculo está estructuralmente sesgado: contabiliza todo el beneficio de bloquear el fraude, pero omite el costo principal de la medida, que es el bloqueo de **millones de comunicaciones empresariales legítimas al año** —verificaciones bancarias, confirmaciones de citas médicas, cobranzas autorizadas, notificaciones transaccionales y atención al cliente— cursadas con CLI nacional real por ruta internacional, que constituyen la mayor parte del tráfico de LDI. Una relación costo-beneficio favorable obtenida sin medir el costo más relevante **no puede sustentar la adopción de la medida**.

Esta omisión se confirma con la propia caracterización empírica del documento soporte, que se basó en información requerida a los operadores móviles sobre tráfico de voz móvil y SMS, **sin incluir a los operadores de LDI ni el tráfico internacional entrante**. El AIN, por tanto, careció de los datos necesarios para valorar el impacto de la medida sobre el tráfico que más afecta.

2. El propio AIN reconoce que el monitoreo con etiquetado es la mejor alternativa en materia de voz

En la evaluación de la temática relativa a la información al usuario sobre las llamadas recibidas, el mismo AIN concluyó que la alternativa de «Lineamientos regulatorios para monitoreo y etiquetado de tráfico de voz, con enfoque general y segmentación empresarial» presenta el mejor desempeño global, por incorporar mecanismos integrales de monitoreo preventivo, etiquetado de llamadas sospechosas y validación de llamadas empresariales. El documento soporte no explica por qué ese enfoque —superior según su propio análisis— no se extendió al tráfico internacional, donde se optó por el bloqueo. Existe así una contradicción interna entre dos partes del mismo AIN.

3. No se evaluó la pertinencia de reglas diferenciales para los operadores de LDI

La evaluación del artículo 31 de la Ley 1978 de 2019 sobre cargas diferenciales se efectuó respecto de los operadores del ecosistema de SMS, A2P y terminación móvil, constatando que superan el umbral de 30.000 accesos. No se analizó el perfil de los operadores de LDI de voz, cuya estructura de accesos y posición en la cadena difieren, de modo que el mandato de evaluar reglas diferenciales no se agotó respecto de esta categoría.

V. El concepto de abogacía de la competencia debe pronunciarse sobre el efecto del bloqueo en el mercado de larga distancia internacional (LDI)

Si bien el numeral 5 del proyecto anuncia el trámite de abogacía de la competencia ante la Superintendencia de Industria y Comercio, conforme al artículo 7 de la Ley 1340 de 2009 y al Capítulo 30 del Título 2 de la Parte 2 del Libro 2 del Decreto 1074 de 2015, dicho trámite debe abordar de manera específica los efectos que el bloqueo de CLI nacional produce sobre la estructura del mercado de larga distancia internacional descritos en la sección III de este escrito. El concepto de la SIC no es vinculante, pero el artículo 7 obliga a la CRC a motivar expresamente, en las consideraciones del acto, las razones por las cuales se aparte de él, y el artículo 2.2.2.30.7 del mismo Decreto 1074 de 2015 le impone dejar constancia del análisis de competencia en la parte considerativa del acto administrativo. La Sala de Consulta y Servicio Civil del Consejo de Estado, en concepto del 4 de julio de 2013, advirtió que la omisión de este trámite, o el apartamiento inmotivado del concepto, puede acarrear la nulidad del acto administrativo por expedición irregular. Por ello, la CRC no debe expedir la resolución sin que el análisis de competencia se haya pronunciado sobre el desplazamiento de tráfico legítimo desde los operadores regulados hacia las plataformas OTT no reguladas que la medida genera, y sin dejar constancia de ese análisis en la parte considerativa.

VI. La alternativa que ataca la causa y sirve a los tres actores

La medida idónea, necesaria y proporcional es la que ataca la causa raíz —la falta de trazabilidad y autenticación del origen— y no su síntoma. Un esquema de verificación de origen sirve, simultáneamente, a los tres actores: el usuario puede confiar en lo que ve, distinguiendo una llamada verificada de una no verificada; el operador de LDI puede acreditar la legitimidad de su tráfico y separarlo del fraudulento; y la autoridad reduce el fraude real sin suprimir comunicaciones lícitas. Sus elementos:

- **Excepción de origen verificado:** junto al roaming, eximir del bloqueo el tráfico con CLI nacional cuyo origen sea certificado por un operador inscrito en un registro ante la CRC.
- **Verificación documental del cliente como condición de la excepción:** acreditación de la identidad del cliente, de la asignación legítima de la numeración presentada y de la autorización del titular para su uso.
- **Etiquetado en lugar de bloqueo para el tráfico verificable,** en coherencia con el artículo 2.1.10.7.2.2.2.
- **Puerto seguro de responsabilidad** para el operador que certifique el origen conforme al estándar, frente a alteraciones producidas en eslabones anteriores de la cadena que no le eran detectables.

- **Mecanismo de impugnación** para el operador y el usuario destinatario afectados por el bloqueo o etiquetado de tráfico legítimo.
- **Implementación gradual**, condicionando los componentes de verificación a la entrada en operación del registro de origen verificado.

VII. Peticiones

Con fundamento en lo expuesto, solicitamos respetuosamente a la Comisión:

1. Abstenerse de adoptar, en el artículo 2.1.10.7.2.2.1, el bloqueo de las llamadas con CLI nacional como regla general, por no superar el test de proporcionalidad.
2. Adoptar en su lugar un esquema de verificación y autenticación de origen, con etiquetado del tráfico no verificado, conforme a la sección VI de este escrito.
3. Completar el Análisis de Impacto Normativo de la medida de bloqueo, cuantificando con datos del tráfico colombiano el volumen y la proporción del tráfico internacional entrante con CLI nacional que corresponde a comunicaciones empresariales legítimas frente al fraudulento, e incorporando el costo del tráfico legítimo que resultaría bloqueado, antes de adoptar la medida.
4. Someter la medida al concepto de abogacía de la competencia de la Superintendencia de Industria y Comercio, por su efecto sobre el mercado de larga distancia internacional (LDI) y el desplazamiento de tráfico legítimo hacia plataformas no reguladas, conforme a las secciones III y V de este escrito.
5. Que, en caso de mantenerse el bloqueo del tráfico con CLI nacional proveniente de la ruta de larga distancia internacional, la obligación de ejecutarlo recaiga sobre el operador propietario de la numeración (operador destino) y no sobre el operador de LDI. El operador destino es el único que conoce en tiempo real el estado de roaming de sus propios abonados y, por tanto, el único en capacidad de distinguir el tráfico de roaming legítimo del que presenta un CLI suplantado. Imponer el bloqueo al operador de LDI —que carece de esa información— produce el bloqueo indiscriminado de comunicaciones legítimas, mientras que asignarlo al operador destino permite bloquear únicamente el tráfico efectivamente fraudulento, preservando el roaming legítimo.
6. De mantenerse alguna forma de bloqueo, incorporar un puerto seguro de responsabilidad: el operador que verifique y certifique el origen conforme al estándar que defina la CRC no responderá por alteraciones del CLI producidas por terceros en eslabones anteriores de la cadena internacional, que no le eran detectables.
7. Extender el procedimiento de revisión previsto en el artículo 2.1.10.7.2.2.2 —hoy limitado al etiquetado y al titular de la línea— para que cubra también los casos de bloqueo de tráfico legítimo y para que pueda ser invocado por el operador de larga distancia internacional y por el usuario destinatario afectados, quienes carecen actualmente de cualquier mecanismo para impugnar el bloqueo de una comunicación lícita.
8. Precisar la fuente, actualización y propagación de la lista DNO (artículo 2.1.10.7.2.2.3) y excluir la responsabilidad por numeración cuya inclusión no era conocible al momento de cursar la llamada.
9. Establecer un plazo de implementación gradual y suficiente para las medidas de prevención de fraude en voz (artículos 2.1.10.7.2.2.4 y 20). En caso de adoptarse el esquema de verificación de

origen propuesto en la sección VI, su exigibilidad debe condicionarse a la entrada en operación previa del registro de origen verificado y a la definición del estándar técnico correspondiente, del mismo modo en que el proyecto condicionó la entrada en vigencia del régimen de mensajería A2P a la previa selección del validador centralizado. En caso de mantenerse el bloqueo, su entrada en vigencia debe diferirse y escalonarse para permitir las adecuaciones técnicas necesarias y las pruebas que eviten la supresión de tráfico legítimo, en lugar de su exigibilidad inmediata conforme al artículo 20.

Agradecemos la atención a los presentes comentarios y reiteramos nuestra disposición para contribuir constructivamente en el perfeccionamiento del proyecto, en torno al objetivo común de proteger al usuario frente al fraude.

Cordialmente,



CARLOS ANDRÉS VARGAS

Representante Legal

Sistemas Satelitales de Colombia S.A. E.S.P.