116751000G-0452

Bogotá D.C., 29 de diciembre 2025.

Doctora
Claudia Ximena Bustamante
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
medidasantifraude@crcom.gov.co
Ciudad

Asunto: Comentarios al proyecto de identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles

Respetada doctora Claudia,

Valoramos y respaldamos la iniciativa de la Comisión de Regulación de Comunicaciones para estructurar una estrategia integral destinada a mitigar el fraude cibernético en los servicios móviles. Coincidimos plenamente con el diagnóstico del regulador respecto a que la confianza digital es un activo crítico que se ha visto erosionado por la sofisticación de delitos como el *smishing*, *vishing* y la suplantación de identidad. Tal como lo hemos manifestado en comunicaciones anteriores, Movistar ha venido implementando de manera proactiva herramientas de detección y bloqueo basadas en inteligencia artificial que han permitido filtrar millones de intentos de contacto fraudulento; sin embargo, compartimos la visión en cuanto a que los esfuerzos aislados son insuficientes y se requiere un marco normativo que cierre las brechas estructurales que hoy aprovechan los delincuentes.

No obstante, para que esta nueva regulación sea efectiva y sostenible, es imperativo que las medidas adoptadas superen un riguroso análisis de viabilidad técnica, proporcionalidad económica y eficiencia operativa. Nos preocupa que algunas de las alternativas planteadas en el documento de consulta parecen trasladar desproporcionadamente la carga operativa y financiera a los proveedores de redes y servicios de telecomunicaciones (PRST), asumiendo que el control de la red equivale al control del origen del fraude, cuando la realidad operativa demuestra que gran parte de la problemática se gesta en eslabones de la cadena de valor que hoy cuentan con una regulación más laxa, como son los agregadores, integradores tecnológicos y generadores de contenido.

Solicitud de habilitación expresa y seguridad jurídica para el bloqueo preventivo

El principal obstáculo que enfrentamos los operadores en la lucha diaria contra el fraude es la asimetría entre la velocidad con la que actúan las estructuras criminales y los tiempos de los procedimientos administrativos vigentes para la suspensión de recursos de numeración. La experiencia nos ha demostrado que, mientras se surte el debido proceso administrativo para recuperar un código corto o bloquear una numeración denunciada, los defraudadores logran masificar sus campañas y afectar a miles de usuarios. Por esta razón, solicitamos a la Comisión que la regulación resultante de este proyecto incluya, como medida prioritaria, una habilitación expresa y un marco de protección jurídica ("puerto seguro") que faculte a los operadores para realizar bloqueos preventivos inmediatos de tráfico,

códigos cortos o numeración internacional ante la detección técnica de patrones anómalos o reportes consistentes de fraude.

Es fundamental que esta facultad quede blindada jurídicamente para que el actuar diligente del operador en defensa de sus usuarios no se configure posteriormente como una infracción por obstrucción al acceso, discriminación o denegación de servicio. La normativa debe permitir actuar con celeridad para detener la conducta lesiva en tiempo real, difiriendo las etapas de revisión de fondo, descargos y eventual reactivación para un momento posterior al bloqueo. Este cambio de paradigma, donde prevalece la protección del usuario sobre la continuidad comercial de un actor bajo sospecha fundada, es la herramienta más efectiva y de menor costo que la Comisión puede otorgar a la industria.

Gobernanza, responsabilidad en la validación y asimetría regulatoria

Frente a las medidas propuestas para la mitigación del fraude en mensajería (SMS), apoyamos el fortalecimiento de los controles de entrada al ecosistema. Sin embargo, somos enfáticos en señalar que las obligaciones de validación de identidad, "Conozca a su Cliente" (KYC) y "Conozca a su Negocio" (KYB) deben recaer de manera directa y estricta sobre los agregadores, integradores tecnológicos y proveedores de contenidos y aplicaciones (PCA). Son estos actores quienes mantienen la relación comercial con el originador del tráfico y quienes se lucran de la comercialización del envío de mensajes; por tanto, no es eficiente ni equitativo pretender que el operador de red, que actúa como transportador, audite la legitimidad de cada marca o campaña que ingresa a través de terceros.

En este sentido, coincidimos plenamente con la visión de la industria sobre la urgencia de implementar un esquema de validación centralizada (KYC) que permita ordenar el mercado de numeración y garantizar la trazabilidad de los remitentes. Reconocemos que un registro unificado es fundamental para eliminar el anonimato y las “zonas grises” que hoy facilitan el fraude. No obstante, para asegurar el éxito de esta iniciativa, consideramos indispensable resolver previamente inquietudes operativas clave relacionadas con la disponibilidad, latencia y seguridad de la información en dicha plataforma central. El modelo debe diseñarse de tal forma que garantice agilidad en la consulta para no afectar el tráfico legítimo, y debe articularse estrictamente con el reordenamiento de los recursos de numeración (Sender ID únicos), asegurando que la validación administrativa se traduzca efectivamente en una limpieza técnica del ecosistema.

Viabilidad técnica en voz: condicionantes para STIR/SHAKEN y redes IP

Respecto a la mitigación del fraude en servicios de voz y el combate al enmascaramiento de llamadas (*CLI Spoofing*), Movistar ratifica su apoyo al objetivo de garantizar la autenticidad del origen de las comunicaciones y erradicar el tráfico internacional con numeración nacional suplantada. Sin embargo, frente a la propuesta de adoptar el estándar de autenticación STIR/SHAKEN y *Rich Call Data* (RCD), es indispensable que la Comisión reconozca una realidad técnica insoslayable: estos protocolos no son una simple actualización de *software*, sino que dependen estructuralmente de que la totalidad de la cadena de interconexión y tránsito curse sobre redes basadas en protocolo IP (SIP).

En el entorno actual de redes en Colombia, donde aún coexisten interconexiones TDM tradicionales y rutas de larga distancia internacional legadas, la "firma digital" o *token* de autenticación que genera STIR/SHAKEN se pierde en el tránsito entre tecnologías, haciendo inefectiva la inversión si no existe

una migración tecnológica previa y coordinada de todo el sector. Por tanto, instamos a la CRC a condicionar la obligatoriedad de estos estándares a un análisis de factibilidad técnica real y a la definición de un cronograma de transición hacia redes "All-IP". Imponer esta obligación sin resolver la brecha de infraestructura implicaría inversiones multimillonarias (CAPEX/OPEX) que no se traducirían en una protección real para el usuario final, encareciendo ineficientemente la prestación del servicio.

Análisis de impacto económico y sostenibilidad de las medidas

Como se ha manifestado desde los gremios y distintos actores de la industria, las tarifas de cargos de acceso para SMS y terminación de voz en Colombia se encuentran entre las más bajas de la región, respondiendo a una política regulatoria orientada a la reducción de costos. En este contexto, la imposición de nuevas obligaciones tecnológicas complejas —como la implementación de *Blockchain* (DLT) para validación de mensajes, sistemas de monitoreo en tiempo real con inteligencia artificial o el despliegue de STIR/SHAKEN— generaría costos de transacción y operación que no son cubiertos por la estructura de ingresos actual de estos servicios.

Solicitamos respetuosamente a la CRC que, previo a la adopción de cualquiera de estas alternativas tecnológicas, se realice un Análisis de Impacto Normativo (AIN) riguroso que cuantifique el costo de implementación para los agentes regulados y lo contraste con el beneficio esperado en reducción del fraude. Existe un riesgo real de que, al elevar artificialmente los costos del canal SMS/Voz legítimo mediante cargas regulatorias excesivas, se termine incentivando el desplazamiento del tráfico corporativo hacia canales OTT (como WhatsApp) que operan fuera del alcance de la regulación nacional y donde la trazabilidad para las autoridades colombianas es aún más limitada. La regulación debe buscar el equilibrio: elevar el estándar de seguridad sin asfixiar económicamente el canal regulado.

Resultaría paradójico imponer cargas económicas desproporcionadas a los operadores de telecomunicaciones, quienes invertimos recursos para detener el tráfico irregular, mientras gran parte de la actividad delictiva migra hacia plataformas digitales y redes sociales que no solo carecen de obligaciones equiparables, sino que incluso monetizan la difusión de estos contenidos. Investigaciones recientes revelan que una fracción significativa de los ingresos publicitarios de estas grandes plataformas proviene de anuncios fraudulentos o de 'alto riesgo'[1], lo que evidencia que la regulación asimétrica no solo es injusta competitivamente, sino ineficaz: asfixiar al operador regulado termina subsidiando el modelo de negocio de las plataformas que se lucran del fraude.

Coordinación interinstitucional y enfoque educativo

Finalmente, frente al componente educativo y de gestión de denuncias, Movistar reitera su compromiso con la pedagogía, evidenciado en nuestras campañas permanentes de sensibilización al usuario. No obstante, consideramos que la creación de sistemas centralizados de trazabilidad de PQR o portales de denuncia administrados por la CRC debe evaluarse con prudencia. Centralizar el detalle

[1] Reuters Investigation. *"Meta is earning a fortune on a deluge of fraudulent ads, documents show"*. Noviembre, 2025. Documentos internos revisados por la agencia proyectaron que aproximadamente el 10% de los ingresos anuales de la plataforma provendrían de anuncios relacionados con estafas o bienes prohibidos. Disponible en: reuters.com/investigations

de las reclamaciones de fraude conlleva riesgos de seguridad de la información y duplicidad de funciones con los canales de atención de los operadores y las entidades financieras.

La lucha contra el fraude trasciende la esfera regulatoria técnica; el bloqueo de un número es una medida de contención, pero no de solución definitiva si no hay judicialización. Por ello, sugerimos que el esfuerzo institucional se enfoque en fortalecer las mesas de trabajo operativas con la Fiscalía General de la Nación, la Policía Nacional y el sector bancario, estableciendo protocolos ágiles para que la evidencia técnica preservada por los operadores pueda ser utilizada eficazmente en la persecución penal de las estructuras delictivas.

Movistar queda a entera disposición de la Comisión para profundizar en los aspectos técnicos aquí expuestos y colaborar en la construcción de un marco regulatorio que proteja eficazmente a los colombianos, bajo premisas de viabilidad técnica y sostenibilidad económica.

Cordialmente,

(Original firmado)
MARIA FERNANDA BERNAL
Directora de Asuntos Públicos y Regulatorios
COLOMBIA TELECOMUNICACIONES S.A. ESP BIC

ANEXO 1: RESPUESTAS AL CUESTIONARIO DE CONSULTA PÚBLICA

9.1 Preguntas generales

— Considerando que la atención coordinada del fraude mediante una estrategia nacional es una necesidad urgente para el país y los usuarios, y que este proyecto regulatorio será un paso de varios en la lucha contra un fenómeno tan dinámico, ¿qué retos técnicos, operativos o regulatorios podrían influir en esos plazos? ¿Qué esquemas de transición o fases intermedias propondría para garantizar una metodología ágil con victorias tempranas que permita atender oportunamente la creciente oleada de comunicaciones fraudulentas?

Respuesta:

Identificamos tres retos estructurales que condicionan los plazos de implementación:

1. **Reto de infraestructura de red (voz):** la implementación de protocolos de autenticación criptográfica como STIR/SHAKEN no es una simple actualización de software; depende de que la cadena de interconexión (nacional e internacional) curse sobre protocolo IP (SIP). Mientras persistan interconexiones TDM o legadas, la "firma" de autenticación se perderá en el tránsito, inutilizando la inversión. Por tanto, el plazo debe estar atado a la evolución natural de las redes hacia *All-IP* y no a mandatos administrativos inmediatos.
2. **Reto de interoperabilidad internacional:** gran parte del *spoofing* proviene de tráfico internacional. Imponer reglas locales estrictas sin acuerdos de interoperabilidad con *carriers* internacionales y de larga distancia (LDI) podría aislar a Colombia o degradar la calidad del servicio de voz legítimo sin detener el fraude.
3. **Reto regulatorio:** actualmente, los operadores enfrentan un riesgo sancionatorio si bloquean tráfico unilateralmente. El reto inmediato es regulatorio, no técnico.

Esquema de Transición Propuesto: Proponemos un enfoque de **"victorias tempranas basadas en facultades"** antes que en **"Obligaciones tecnológicas masivas"**:

- **Fase 1:** habilitación regulatoria expresa ("Puerto Seguro") para que los operadores bloqueen códigos cortos y tráfico internacional con patrones de *spoofing* o reportes de fraude, sin riesgo de sanciones por obstrucción. Saneamiento administrativo de la base de datos de asignatarios de códigos cortos.
- **Fase 2:** implementación de obligaciones de proceso (KYC/KYB) reforzadas para Agregadores y PCAs. Establecimiento de mesas técnicas para definir estándares de intercambio de información (APIs) entre operadores (modelo federado).

— ¿Qué ventajas, desventajas, retos y oportunidades identifica en la implementación por parte de la CRC de mecanismos de evaluación periódica de las medidas adoptadas para mitigar el fraude mediante servicios móviles tradicionales de voz y SMS? ¿Qué criterios, metodologías o frecuencias de evaluación considera más adecuados para asegurar la efectividad y actualización continua de estas medidas?

Respuesta:

- **Ventajas:** permite ajustar la regulación a la mutación del delito, evitando normas obsoletas.
- **Desventajas/riesgos:** existe el riesgo de medir la efectividad basándose únicamente en el volumen bruto de PQR o reportes, lo cual puede ser engañoso (un aumento en reportes puede significar mayor conciencia del usuario, no necesariamente más fraude). Asimismo, evaluaciones excesivamente frecuentes pueden generar una carga administrativa que desvía recursos operativos de la prevención real.
- **Metodología propuesta:** la evaluación debe ser **anual** y basada en indicadores de efectividad técnica (por ejemplo, volumen de tráfico bloqueado preventivamente gracias a las nuevas facultades) y no solo en percepción. Es fundamental que la evaluación distinga entre vulnerabilidades de la red móvil y fraudes de ingeniería social donde la red funcionó correctamente, pero el usuario fue engañado; responsabilizar al operador por la ingeniería social distorsiona la evaluación de las medidas técnicas.

— ¿Cuáles considera que son los principales aciertos y limitaciones de las alternativas propuestas para mitigar el contacto fraudulento a través de servicios tradicionales de voz y mensajes de texto? ¿Qué elementos adicionales o diferentes propondría para mejorar la eficacia de estas medidas?

Respuesta:

- **Aciertos:** valoramos que la CRC reconozca la problemática del *spoofing* y la necesidad de validar la identidad de los remitentes en SMS. Es un acierto proponer el uso de identificadores únicos y exigir mayores controles a la cadena de valor (Agregadores/PCAs).
- **Limitaciones:**
    - **Costos ocultos:** no se evidencia una valoración de los costos de CAPEX/OPEX para los operadores al implementar tecnologías como DLT o STIR/SHAKEN, los cuales no son recuperables vía tarifas actuales.
    - **Internet móvil:** el alcance limitado a SMS y Voz deja por fuera el eslabón final de la cadena de fraude (URLs maliciosas y OTTs como WhatsApp), lo que limita la eficacia integral de la estrategia.
- **Propuesta adicional:** el modelo debe basarse en la **responsabilidad en el origen**. La carga de la prueba, la validación y los costos tecnológicos de autenticación deben recaer sobre quien se lucra del envío del mensaje (el Agregador/PCA), no sobre la red de transporte. Proponemos un modelo donde el operador consulta la validación realizada por el Agregador, bajo un esquema de responsabilidad legal estricta de este último.

— ¿Qué métricas, indicadores o criterios considera que deberían establecerse en la industria para evaluar de manera efectiva la reducción del fraude y el impacto de las alternativas regulatorias propuestas en este documento? ¿Qué variables cuantitativas o cualitativas serían más útiles para medir la evolución del fraude, la protección al usuario y la eficacia de las medidas implementadas, y cómo podrían ser recolectadas y/o reportadas de forma coordinada entre los diferentes actores del sector?

Respuesta: Sugerimos métricas enfocadas en la **gestión preventiva** y no solo en la reactiva:

1. **Tasa de bloqueo preventivo:** volumen de SMS y llamadas bloqueadas por filtros *antispam/antifraud* (muestra la proactividad de la red).
2. **Tiempo de reacción:** tiempo promedio entre la detección/reporte de un patrón de fraude masivo y su bloqueo efectivo (esto mejorará sustancialmente si se otorga el "puerto seguro" legal solicitado).
3. **Tasa de establecimiento de llamadas (csr) anómalo:** Monitoreo de picos de tráfico en rutas internacionales que no corresponden a patrones de tráfico humano (indicador de *robocalling*).

Recolección:
La información debe ser reportada de manera agregada y anonimizada para proteger la privacidad de los usuarios y la estrategia comercial de los operadores. Rechazamos la creación de repositorios centralizados de datos crudos (PQR detallados o CDRs) por los riesgos de ciberseguridad que implican. La coordinación debe darse mediante mesas de trabajo donde se compartan *insights* y patrones (Inteligencia de Amenazas), no bases de datos de clientes.

9.2 Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)
— ¿Qué retos y beneficios identifica en la implementación de un proceso obligatorio de conocimiento del cliente (KYC) para agregadores de SMS? ¿Qué criterios mínimos considera indispensables para que este proceso sea efectivo y no excluyente?

Respuesta:
Consideramos que el principal beneficio es la trazabilidad: permite vincular un mensaje fraudulento con una persona jurídica o natural real, desincentivando el anonimato. Sin embargo, identificamos los siguientes retos:

- **Alcance extraterritorial:** muchos agregadores o clientes finales son empresas extranjeras, lo que dificulta la validación de documentos de constitución y representación legal bajo estándares locales.
- **Costo de implementación:** la verificación exhaustiva manual es costosa y lenta.

Para que el proceso sea efectivo, los criterios mínimos deben ser:
1. verificación de la existencia legal de la empresa y del representante legal;
2. validación de la titularidad de la marca que se pretende usar en el *sender ID* (identificador de remitente);
3. registro de casos de uso (para qué se usará la mensajería).

Es fundamental establecer que la responsabilidad de ejecutar este KYC recae sobre el agregador o integrador que tiene la relación comercial con el cliente, y no sobre el operador de red móvil, quien actúa como transportador.

— Teniendo en cuenta que los agregadores pueden actuar tanto en acuerdos directos como en esquemas donde funcionan como parte de una cadena para terminar tráfico de otros agregadores (normalmente tráfico internacional), ¿qué diferencias, riesgos u oportunidades identifica en la prevención del fraude? ¿Considera pertinente establecer medidas diferenciadas

para cada caso? ¿Qué criterios o mecanismos recomendaría para gestionar de manera más efectiva el tráfico proveniente de cadenas internacionales, especialmente en lo relacionado con la trazabilidad, el monitoreo y la validación de los originadores de contenido?

Respuesta:

El tráfico internacional que pasa por múltiples saltos (*hops*) presenta el mayor riesgo de pérdida de trazabilidad y manipulación de cabeceras. Identificamos como riesgo crítico el "blanqueo" de tráfico, donde un mensaje fraudulento entra a través de una ruta legítima.
No recomendamos medidas diferenciadas que relajen controles, sino un estándar único de entrada a la red nacional:

- **Responsabilidad del último eslabón:** el agregador o *carrier* que entrega el tráfico directamente a Movistar debe ser contractual y legalmente responsable por el contenido que cursa, independientemente de cuántos intermediarios hubo antes.
- **Identificadores inalterables:** se debe exigir que el *sender ID* o código corto no sea modificado en el tránsito.
- **Mandato de bloqueo:** si el agregador no puede certificar el origen del tráfico, el operador debe tener la facultad expresa de rechazar dichos mensajes sin sanciones regulatorias.

— ¿Considera pertinente la implementación de un proceso centralizado o distribuido para la validación de agregadores, marcas y campañas antes de cursar tráfico A2P?

Respuesta:

Consideramos pertinente establecer mecanismos robustos de validación (KYC) para agregadores, marcas y campañas, reconociendo que unificar estos criterios es un paso positivo para sanear el ecosistema. Si bien un modelo centralizado podría aportar orden y estandarización, consideramos fundamental que su diseño contemple la agilidad operativa necesaria para no afectar la entrega de mensajes críticos. Es vital asegurar que la arquitectura elegida no introduzca latencias o puntos únicos de falla que puedan impactar la experiencia del usuario final o la seguridad de la información transaccional.

Respecto a la alternativa de implementación distribuida (basada en tecnologías como DLT o Blockchain), observamos con preocupación que podría implicar costos de inversión y operación desproporcionados frente a la estructura económica actual del servicio de SMS. Por ello, sugerimos priorizar modelos que sean costo-eficientes y sostenibles en el tiempo. En cualquier escenario, es indispensable establecer con claridad que los costos de implementación, gestión y consulta de estas plataformas no deben ser trasladados a los Proveedores de Redes (PRSTM), dado que no somos los generadores del contenido ni quienes gestionan la relación comercial con las marcas.

Finalmente, reiteramos que la responsabilidad operativa de realizar la validación y mantener la información actualizada debe recaer en los Agregadores y PCAs, quienes tienen el vínculo directo con el cliente final. El rol del modelo centralizado debería enfocarse en la estandarización y auditoría de dicha información, evitando que el PRSTM asuma cargas administrativas ajenas a su operación de red. Asimismo, instamos a definir protocolos claros de protección de datos y gobernanza para asegurar

que la información sensible del tráfico se maneje con los más altos estándares de seguridad, independientemente de quién administre la plataforma.

— ¿Cuáles serían, a su juicio, los principales desafíos técnicos, económicos, operativos y de gobernanza para un sistema centralizado de validación de remitentes y campañas? ¿Qué mecanismos de transparencia y auditoría considera necesarios?

Respuesta:

Identificamos los siguientes desafíos críticos:

- **Económicos:** los márgenes del servicio de SMS son estrechos. Crear una entidad centralizada implica costos de administración que no pueden ser trasladados a los operadores de red, cuyas tarifas de acceso ya son bajas.
- **Operativos:** la latencia. Consultar una base de datos central por cada envío masivo (millones de transacciones) puede degradar la calidad del servicio y afectar la entrega de mensajes críticos (como OTPs bancarios).
- **Gobernanza:** definir quién responde cuando el validador central comete un error (falso positivo) y bloquea una campaña legítima de un banco o entidad de salud.

Sería indispensable un mecanismo de auditoría en tiempo real y un SLA (acuerdo de nivel de servicio) estricto, donde el administrador central asuma la responsabilidad por fallas en la validación.

— ¿Qué ventajas y desafíos técnicos, económicos, operativos o de gobernanza identifica en un modelo distribuido de validación basado en DLT? ¿Qué elementos deberían definirse para asegurar la interoperabilidad y la confianza entre los distintos actores?

Respuesta:

- **Ventajas teóricas:** inmutabilidad de los registros y trazabilidad descentralizada.
- **Desafíos reales:** costos y tiempos de transacción. Las tecnologías DLT (*blockchain*) suelen tener costos de escritura y lectura que harían inviable el modelo de negocio del SMS A2P, además de tiempos de confirmación que no se ajustan a la inmediatez requerida.
- **Posición de Movistar:** advertimos que imponer tecnologías complejas como DLT sin un Análisis de Impacto Normativo (AIN) previo que demuestre que el beneficio en reducción de fraude supera los altos costos de implementación (CAPEX/OPEX), podría encarecer el servicio al punto de desplazar el tráfico hacia canales OTT no regulados, anulando el propósito de la medida.

— ¿Qué requerimientos funcionales considera que una solución tecnológica debe tener en cuenta para llevar a cabo de manera efectiva la validación de autenticidad de las URL en el evento que el mensaje corto de texto las contenga?

Respuesta:

Para implementarlo técnicamente sin vulnerar la privacidad, se requiere:

1. Que la validación se realice contra una "lista blanca" de dominios pre-registrados por el cliente corporativo al momento de contratar la campaña;
2. Que el sistema sea automatizado (sin intervención humana);
3. Que exista una exención de responsabilidad legal para el operador por el tratamiento de estos datos con fines de ciberseguridad.

— ¿Qué impactos positivos y negativos prevé en la obligación de bloquear o marcar mensajes que no cuenten con identificadores validados? ¿Cómo se podría garantizar que no se afecte la entrega de mensajes legítimos?

Respuesta:

- **Positivos:** limpieza inmediata del ecosistema y reducción drástica del *smishing*.
- **Negativos:** riesgo de bloquear notificaciones críticas (salud, banca, emergencias) si el proceso de validación falla o es lento.
- **Garantía:** para evitar afectaciones, proponemos una implementación gradual con "listas de confianza" para actores críticos y un canal de soporte 24/7 exclusivo para reactivación de tráfico legítimo bloqueado erróneamente.

— ¿Qué ventajas y riesgos observa en la clasificación obligatoria de los mensajes por tipo de contenido y la articulación con el consentimiento del usuario mediante el RNE? ¿Cómo podría mejorarse la protección de los derechos del usuario a decidir el tipo de contenido que desea recibir? ¿Considera pertinente una clasificación de contenido distinta a la propuesta?

Respuesta:

En cuanto a la clasificación obligatoria de mensajes, identificamos como ventaja principal la capacidad de empoderar al usuario para filtrar selectivamente el tráfico, permitiendo, por ejemplo, bloquear comunicaciones comerciales sin impedir la recepción de mensajes críticos como OTPs o notificaciones bancarias. Sin embargo, el desafío técnico y operativo radica en garantizar la veracidad de dicha clasificación; existe un riesgo latente de que los originadores etiqueten erróneamente mensajes publicitarios como "transaccionales" o "de servicio" para evadir bloqueos. Por ello, consideramos que una clasificación simplificada (por ejemplo, limitándose a "Comercial/Publicitario" y "Servicio/Transaccional") facilitaría la gestión y reduciría las zonas grises, siempre bajo la premisa de que la responsabilidad por el correcto etiquetado recae en el Agregador y no en el operador de red, quien no debe realizar inspección profunda de contenidos por razones de privacidad y eficiencia.

Respecto a la articulación con el Registro de Números Excluidos (RNE), creemos que la protección de los derechos del usuario mejora si se establece la obligación estricta para el Agregador o PCA de consultar y depurar sus bases de datos contra el RNE *antes* de inyectar el tráfico en la red. No resulta viable trasladar al PRSTM la carga de consultar el RNE en tiempo real por cada mensaje recibido, ya que esto impactaría la latencia del servicio. La mejora en la protección del usuario depende de que quien origina el mensaje respete la voluntad de exclusión desde la fuente, integrando la consulta al RNE como un paso previo e ineludible en sus procesos de envío.

Finalmente, es necesario señalar con franqueza que, en la práctica actual, el RNE ha mostrado limitaciones en su eficacia, pues los usuarios inscritos continúan recibiendo tráfico no deseado. Por tanto, cualquier medida que vincule la clasificación de mensajes con este registro será estéril si no viene acompañada de mecanismos de vigilancia y sanción efectivos por parte de las autoridades competentes (SIC/CRC).

— ¿Qué capacidades o características mínimas debería tener el sistema de monitoreo de tráfico por parte de los agregadores para detectar patrones anómalos o sospechosos? ¿Qué salvaguardas deberían definirse para evitar bloqueos injustificados?

Respuesta:

Los sistemas de monitoreo de los agregadores deben tener, como mínimo:

1. Detección de volumen inusual (*rate-limiting*): alertas por picos de tráfico no programados;
2. Análisis de contenido repetitivo: detección de campañas idénticas enviadas desde múltiples orígenes;
3. Validación de *sender ID*: asegurar que el remitente alfanumérico corresponda al autorizado.

Frente a las salvaguardas, reiteramos la necesidad de protocolos claros de "notificación y defensa" *post-bloqueo*, permitiendo al operador actuar primero para proteger al usuario y revisar después.

— ¿Qué beneficios y limitaciones identifica en la alternativa de asignación de códigos alfanuméricos, códigos cortos o números E.164 exclusivos para cada marca? ¿Cómo podría impactar esto en la trazabilidad y la experiencia del usuario?

Respuesta:

Identificamos como principal beneficio el incremento sustancial en la trazabilidad y la confianza del usuario, ya que la asignación exclusiva elimina la ambigüedad que hoy existe con los códigos cortos compartidos, donde un mismo número es utilizado por múltiples empresas, dificultando distinguir una comunicación legítima de una fraudulenta. El uso de identificadores alfanuméricos (*sender ID*) exclusivos refuerza la identidad de marca y facilita al ciudadano reconocer quién le escribe.

Sin embargo, observamos limitaciones técnicas y operativas importantes. La migración masiva a numeración E.164 para aplicaciones comerciales requeriría ajustes profundos en los sistemas de enrutamiento y señalización de las redes móviles, así como en las plataformas de los agregadores. Además, si la asignación no se gestiona con agilidad, podría generar barreras de entrada para pequeñas empresas. En términos de experiencia de usuario, aunque el código alfanumérico es preferible por claridad, este no permite una respuesta directa (doble vía) en la mayoría de los terminales, lo cual limita casos de uso interactivos. Por tanto, sugerimos un esquema híbrido donde la exclusividad sea la norma, pero se permitan modelos compartidos estrictamente controlados para empresas de menor tamaño, siempre bajo la responsabilidad del agregador.

— ¿Qué efectividad considera que tendría la obligatoriedad de usar identificadores alfanuméricos únicos (*sender ID*) en todos los mensajes de texto que reciban los usuarios, de cara a la confianza en el canal y la prevención del fraude?

Respuesta:

Consideramos que esta medida tendría una alta efectividad para mitigar la suplantación de identidad (*spoofing*) en el canal de mensajería empresarial. Al estandarizar el uso de *sender ID* únicos y validados, se reduce drásticamente la superficie de ataque para los delincuentes que aprovechan la falta de estandarización para hacerse pasar por entidades bancarias o gubernamentales.

No obstante, para que esta efectividad sea real y sostenible, la medida debe ir acompañada de procesos de validación rigurosos en el origen (a cargo de los agregadores) que impidan que un actor no autorizado registre un identificador similar al de una marca reconocida (por ejemplo, evitar variantes maliciosas como "Davivienda" vs "Davivienda."). Sin este control previo, la obligatoriedad del identificador alfanumérico podría generar una falsa sensación de seguridad en el usuario.

— ¿Considera que una eventual limitación del uso de *sender ID* alfanumérico a mensajes transaccionales reduciría costos de implementación, o por el contrario contribuiría a desaprovechar la posibilidad de poder generar un mecanismo identificable, de que los usuarios puedan identificar a todos los originadores de contenidos de manera clara?

Respuesta:

Desde nuestra perspectiva técnica y comercial, limitar el uso de identificadores alfanuméricos exclusivamente a mensajes transaccionales sería contraproducente. Lejos de reducir costos, esta fragmentación podría generar confusión en el usuario, quien tendría que aprender a interactuar con dos estándares distintos (alfanuméricos para bancos, numéricos para promociones) dentro de su misma bandeja de entrada, debilitando la percepción de seguridad del canal en su conjunto.

Adicionalmente, restringir esta funcionalidad podría desincentivar el uso del canal SMS legítimo frente a aplicaciones OTT, donde la identificación de marca es estándar. La estrategia más efectiva es permitir y promover el uso generalizado de identificadores claros para todo tipo de tráfico A2P (aplicación a persona), asegurando que el costo de dicha implementación sea asumido por el mercado corporativo que se beneficia de la identidad de marca, y no subsidiado por los operadores de red.

— ¿Qué criterios considera relevantes para definir patrones atípicos en el tráfico SMS P2P? ¿Cómo se podría evitar afectar a usuarios legítimos?

Respuesta:

Basados en la experiencia de nuestros sistemas de monitoreo antifraude actuales, los criterios técnicos más relevantes para detectar tráfico atípico o granjas de SIM (*SIM farms*) incluyen: la dispersión de destinatarios (un solo número enviando a cientos de destinos únicos en un periodo corto), la velocidad de envío (*rate limit*) superior a la capacidad humana de digitación, el uso de

dispositivos con IMEI estáticos asociados a múltiples IMSI (rotación de tarjetas SIM) y la ubicación fija en celdas con comportamiento de tráfico inusual.

Para evitar afectar a usuarios legítimos, es fundamental establecer umbrales dinámicos que se adapten a los perfiles de consumo promedio y no aplicar bloqueos definitivos inmediatos. Proponemos un esquema de suspensión temporal con redirección a un portal cautivo o envío de un mensaje de advertencia, permitiendo al usuario legítimo validar su identidad y reactivar su servicio mediante un proceso de autenticación reforzada.

— ¿Qué ventajas y desventajas identifica en la imposición de un límite máximo de SMS P2P por usuario? ¿Qué umbrales serían razonables?

Respuesta:

La principal ventaja de establecer límites técnicos es la contención inmediata del abuso de planes ilimitados para fines comerciales o fraudulentos, protegiendo la integridad de la red y el modelo económico del servicio. Sin embargo, la desventaja radica en la posible afectación a usuarios con patrones de uso intensivo pero legítimo.

Respecto a los umbrales, consideramos que estos no deben ser fijados de manera rígida por la regulación, ya que los patrones de consumo evolucionan. Sugerimos que la norma faculte a los operadores para definir y actualizar estos límites en sus políticas de uso justo (*fair use policy*), comunicándolos transparentemente en los contratos. Un umbral razonable debería estar basado en el análisis estadístico del percentil 95 o 99 del tráfico de usuarios residenciales, garantizando que la inmensa mayoría de los clientes no se vea impactada.

— ¿Qué mecanismos de colaboración entre agregadores, operadores y autoridades considera que pueden implementarse para que la detección, prevención y judicialización de fraudes sea más efectiva?

Respuesta:

Consideramos que la colaboración debe centrarse en el intercambio ágil de inteligencia de amenazas y no en la centralización burocrática de procesos. Proponemos la creación de mesas de trabajo operativas permanentes donde se compartan, mediante protocolos seguros y automatizados (APIs), los listados de *sender IDs*, URLs y patrones de tráfico identificados como maliciosos.

Es vital que esta colaboración incluya un marco de "puerto seguro" que permita a los operadores compartir evidencias técnicas con las autoridades judiciales (Fiscalía y Policía) de manera expedita para soportar investigaciones penales, sin infringir las normas de protección de datos personales. La efectividad de la judicialización depende de que la evidencia técnica preservada por los operadores pueda ser entregada y procesada con celeridad por los entes investigadores.

9.3 Frente a las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz

— En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en la relación con la prevención y mitigación del fraude? ¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

Respuesta:
Identificamos una diferencia estructural crítica: en el tráfico nacional directo, el operador tiene control contractual sobre el origen y puede aplicar medidas de validación inmediata; el riesgo es bajo y la oportunidad de control es alta mediante cláusulas contractuales. En contraste, el tráfico internacional que llega en cadena presenta el mayor riesgo de fraude y *spoofing* (suplantación), pues la trazabilidad se pierde entre múltiples intermediarios y no existe una relación contractual con el originador real.
Para gestionar esto, consideramos relevante aplicar medidas diferenciadas: para el tráfico nacional, fortalecer la validación contractual; para el tráfico internacional en cadena, es indispensable exigir que el operador de larga distancia internacional (LDI) que entrega la llamada a la red nacional asuma la responsabilidad de garantizar que el CLI (identificador de llamada) no ha sido alterado. Si el *carrier* internacional no puede certificar el origen, el operador nacional debe estar facultado para rechazar dicho tráfico o etiquetarlo como "no verificado".

— ¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

El efecto positivo más relevante sería la eliminación casi inmediata de una gran porción del fraude de suplantación (*vishing*), ya que técnicamente es anómalo que una llamada originada en el exterior presente un número fijo o móvil nacional, salvo en casos muy específicos.

Sin embargo, prevemos un efecto negativo crítico si no se gestionan adecuadamente las excepciones: el bloqueo de usuarios legítimos en situación de *roaming* internacional. Por tanto, es imperativo que la regulación contemple excepciones técnicas claras y automáticas para permitir el tráfico de abonados nacionales que se encuentran viajando y utilizando su línea en el exterior (*roaming*), asegurando que los sistemas de señalización puedan distinguir entre un viajero legítimo y una llamada suplantada.

— ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como “No verificada” o “Probable fraude”? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

Respuesta:

La principal ventaja es empoderar al usuario con información en tiempo real antes de contestar, reduciendo la tasa de éxito del fraude sin bloquear comunicaciones que podrían ser legítimas pero técnicamente no verificables.

No obstante, identificamos retos técnicos y operativos significativos: esta funcionalidad depende de que los terminales (equipos móviles) soporten la visualización de dichas etiquetas y de que la red pueda transmitir esa información de señalización hasta el usuario final. Existe el riesgo de generar "falsos positivos" que etiqueten llamadas legítimas de empresas internacionales como fraude, afectando la operación comercial de clientes corporativos. Además, la implementación requiere inversiones en el núcleo de la red para habilitar estas capacidades de marcado, cuyo costo debe ser evaluado frente al beneficio real.

— ¿Qué oportunidades y retos identifica en la adopción de protocolos de autenticación como STIR/SHAKEN/RCD? ¿Qué condiciones técnicas y regulatorias serían necesarias para su implementación efectiva? ¿Considera que, con la implementación de este protocolo de autenticación, no resulta necesaria la implementación de medidas de filtrado de tráfico o listas de no originación (DNO)?

Respuesta:

Su adopción en Colombia enfrenta un reto estructural insalvable en el corto plazo: este protocolo solo funciona sobre redes basadas enteramente en IP (SIP). Mientras existan interconexiones TDM tradicionales en la red nacional, la "firma digital" de autenticación se perderá en el tránsito, haciendo inefectiva la inversión.

Para su implementación efectiva, se requiere una condición regulatoria previa: un plan de migración tecnológica de todo el sector hacia la interconexión IP. Adicionalmente, consideramos que STIR/SHAKEN no sustituye otras medidas; es una herramienta complementaria. Las listas de no originación (DNO) seguirían siendo útiles para proteger números que nunca deben originar llamadas (como líneas de atención al cliente *inbound*), independientemente del protocolo de señalización usado.

— ¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y análisis de tráfico de voz? ¿Cómo garantizar que no se generen falsos positivos (que terminen afectando el tráfico legítimo), así como la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas?

Respuesta:

Consideramos que los parámetros más adecuados deben basarse en métricas objetivas de comportamiento de red, tales como la Tasa de Establecimiento de Llamadas (CSR - *Call Setup Rate*) y la duración promedio de las llamadas (ACD - *Average Call Duration*). Un volumen masivo de llamadas cortas o intentos fallidos desde un mismo origen es un indicador técnico estándar de *robocalling*.

Para garantizar la minimización de falsos positivos, es crucial que los umbrales de detección no sean estáticos, sino que se ajusten dinámicamente mediante aprendizaje automático (*machine learning*), y

que existan listas blancas para grandes generadores de tráfico legítimo (ej. *call centers* autorizados). La protección de la privacidad se garantiza analizando metadatos de señalización (quién llama a quién y cuánto dura) sin intervenir el contenido de audio de la comunicación.

— ¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para facilitar la identificación y denuncia de fraudes por parte de los usuarios?

Respuesta:

La creación de rangos exclusivos (como un prefijo específico para ventas) presenta la ventaja teórica de facilitar al usuario la identificación de una llamada comercial. Sin embargo, en la práctica, observamos desafíos operativos significativos: implicaría una migración masiva de numeración para miles de empresas, generando costos elevados y confusión inicial.

Además, su efectividad para prevenir el fraude es limitada si no se controla el *spoofing*: los delincuentes podrían simplemente enmascarar sus llamadas usando esos mismos prefijos exclusivos para engañar al usuario. Por tanto, consideramos que es más efectivo enfocar los esfuerzos en la autenticación del origen (validar quién llama) que en la segregación de la numeración (qué número usa).

— ¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

Respuesta:

El etiquetado obligatorio (RCD - *Rich Call Data*) sobre la numeración actual es una alternativa superior a la segregación de rangos, pues permite a las empresas mantener sus números de contacto conocidos. La ventaja es clara: el usuario ve el nombre de la empresa o el motivo de la llamada en su pantalla, aumentando la confianza.

El reto principal es la compatibilidad del parque de terminales: muchos teléfonos antiguos o de gama baja no tienen la capacidad nativa de mostrar esta información enriquecida sin una aplicación adicional. Asimismo, esto requiere que la red soporte la transmisión de datos enriquecidos en la señalización, lo cual nos remite nuevamente a la necesidad de redes IP. Sin una adopción generalizada de *smartphones* compatibles y redes SIP, el impacto de la medida será limitado.

— ¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números de no originación (DNO)? ¿Qué criterios deberían regir su actualización y acceso?

Respuesta:

Identificamos un beneficio claro en la protección de números institucionales que solo deben recibir llamadas (como las líneas 018000 o PBX de atención al cliente), impidiendo que sean suplantados para realizar llamadas salientes fraudulentas. Una lista DNO efectiva bloquearía de raíz el *vishing* que simula ser el banco llamando al cliente.

El riesgo radica en la gestión de la lista: si un número legítimo es incluido por error, la empresa queda incomunicada hacia afuera. Los criterios de actualización deben ser estrictos, permitiendo solo al asignatario del recurso solicitar la inclusión o exclusión, con validación de identidad fuerte. El acceso de consulta debe ser en tiempo real para los operadores que cursan el tráfico, para poder bloquear las llamadas no autorizadas inmediatamente.

— ¿Qué ventajas, retos y posibles impactos identifica en la adopción de un esquema en el que cada PRST mantenga su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC? ¿De qué manera considera que esta medida podría contribuir a la protección contra el fraude y la suplantación en llamadas de voz, y qué desafíos técnicos, operativos o de coordinación deberían ser tenidos en cuenta para asegurar su efectividad y coherencia en Colombia?

Respuesta:

Un esquema donde cada PRST gestiona su propia lista DNO bajo estándares mínimos ofrece la ventaja de la agilidad y la autonomía en la gestión de riesgos de su propia red. Permite a cada operador proteger a sus clientes corporativos de manera directa sin depender de una base centralizada externa.

El desafío es la coherencia: para que la protección sea sistémica, las listas deben estar sincronizadas o ser compartidas. Si Movistar bloquea el uso indebido de un número de su cliente, pero otro operador permite que ese mismo número origine llamadas desde su red (por suplantación), la medida pierde efectividad. Por ello, aunque la lista sea local, debe existir un mecanismo de intercambio o consulta para que el bloqueo de no-originación sea respetado por todas las redes interconectadas.

9.4 Frente a las temáticas enfocadas en la educación de la ciudadanía

Respuesta consolidada:

Respecto al bloque de preguntas sobre estrategias educativas y herramientas de información al usuario, desde Movistar manifestamos nuestro compromiso continuo con la pedagogía, evidenciado en las campañas voluntarias que hemos desplegado en nuestros canales digitales y centros de experiencia para alertar sobre modalidades como *smishing* y *vishing*. Sin embargo, consideramos que la efectividad de estas acciones no puede recaer exclusivamente en los operadores de telecomunicaciones; es imperativo que las obligaciones de divulgación pedagógica se extiendan de manera vinculante a los agregadores, integradores tecnológicos (IT) y proveedores de contenidos y aplicaciones (PCA), dado que gran parte del fraude suplanta a entidades financieras y comercios cuyos servicios son el gancho para el engaño.

Frente a la propuesta de crear un "Portal de la CRC" que centralice listas de números reportados y campañas fraudulentas, valoramos la intención de transparencia, pero advertimos sobre retos operativos críticos para su viabilidad: la actualización de la información debe ser en tiempo real para ser útil, lo cual requiere automatización y no procesos manuales de carga. Asimismo, es fundamental aclarar el modelo de financiación de dicho portal, pues los costos de su desarrollo y mantenimiento no deben ser trasladados a los proveedores de redes.

En cuanto a la creación de un sistema centralizado de trazabilidad de peticiones, quejas y recursos (PQR) administrado por la CRC, expresamos una preocupación técnica y jurídica significativa. Centralizar bases de datos con el detalle de las reclamaciones de fraude de todos los usuarios del país conlleva riesgos elevados de seguridad de la información (creación de un *honeypot* o punto único de falla) y desafíos complejos en materia de protección de datos personales (*habeas data*). Consideramos que la trazabilidad es necesaria, pero esta debe realizarse mediante reportes estandarizados y agregados que los operadores envíen a la autoridad, y no mediante la entrega de la gestión de las PQR a un sistema centralizado, el cual podría burocratizar la atención y exponer la privacidad de los ciudadanos. La métrica de éxito de la estrategia educativa no debe ser solo el volumen de denuncias, sino el alcance efectivo y la reducción de la tasa de éxito de los intentos de fraude, medida a través de encuestas de percepción y análisis de tráfico bloqueado.

9.5 Frente a las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación normativa

Respuesta consolidada:

Respecto a la revisión del régimen de administración de recursos de numeración, Movistar respalda plenamente la adopción de medidas más estrictas para controlar el acceso y uso de los códigos cortos, identificando la reincidencia como el punto crítico a resolver. Consideramos indispensable que la regulación defina criterios objetivos y taxativos para configurar la "reincidencia" (por ejemplo, la comisión reiterada de conductas fraudulentas en un periodo determinado), y que dicha calificación habilite consecuencias contundentes, como la terminación unilateral del contrato de acceso o interconexión y la "muerte comercial" del asignatario para acceder a nuevos recursos de numeración. Actualmente, la simple recuperación del código es insuficiente, pues el actor infractor migra a otro recurso o utiliza un tercero para continuar la práctica; por tanto, la sanción debe recaer sobre la persona jurídica o natural (KYC), impidiéndole operar en el ecosistema, y no solo sobre el número.

Frente a la figura de la suspensión preventiva del tráfico, solicitamos que se otorgue a los operadores una facultad expresa y un "puerto seguro" regulatorio que nos permita bloquear de manera inmediata el tráfico de un código corto ante la detección técnica de patrones anómalos o reportes de fraude consistentes, sin necesidad de agotar un proceso administrativo previo ante la CRC. La protección del usuario requiere acción en tiempo real; esperar a la apertura formal de una investigación por parte del regulador otorga una ventaja temporal inaceptable a los defraudadores. Esta suspensión debe estar acompañada de un protocolo de notificación ágil al asignatario para garantizar su derecho de defensa *a posteriori*, pero priorizando siempre el cese de la afectación al usuario.

En cuanto a la cesión o transferencia de recursos, apoyamos la imposición de restricciones severas. El mercado secundario de códigos cortos sin control ha facilitado que recursos asignados

legítimamente terminen en manos de actores no verificados. Proponemos que toda cesión deba ser notificada y validada nuevamente bajo los mismos estándares de asignación original (KYC reforzado), prohibiendo expresamente la subarriendo o reventa de capacidad de envío a terceros no identificados.

Finalmente, sobre la actualización de la información en el registro, consideramos que es una obligación esencial del asignatario mantener sus datos de contacto y uso vigentes. Proponemos que la falta de actualización o la imposibilidad de contactar al responsable del código sea causal suficiente y autónoma para la recuperación inmediata del recurso por parte de la CRC, saneando así la base de datos de asignaciones "zombis" que suelen ser instrumentalizadas para el fraude. Cualquier medida adicional de simplificación normativa debe tener como límite la trazabilidad: no se debe simplificar requisitos de entrada si ello implica perder la capacidad de identificar quién está detrás de cada mensaje que llega a los colombianos.