



Bogotá, 29 de diciembre de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE OSORIO
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Ciudad.

Asunto: Comentarios al documento: *"IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES. Documento de Alternativas Regulatorias"*

Cordial saludo,

En atención a la publicación para comentarios del documento indicado en el Asunto, COMCEL presenta los siguientes comentarios:

1. COMENTARIOS GENERALES:

1.1. La respuesta dada por la CRC a los comentarios de los diferentes actores:

Con el documento objeto de comentarios, la CRC da respuesta a los comentarios remitidos por los diferentes actores indicando que:

- Se evaluarán ajustes al régimen de numeración y nuevas herramientas regulatorias para prevenir contacto fraudulento (llamadas/SMS) hacia usuarios.
- El enfoque central del proyecto es la protección de los derechos de los usuarios, quienes son los principales afectados por el fraude; sin embargo señala que no es necesario modificar el problema objeto de estudio.
- Define como nuevo problema regulatorio la baja efectividad de las herramientas actuales para prevenir fraude en voz y SMS.
- Considera incluir reincidencia como criterio para administrar o recuperar códigos cortos y aplicar sanciones a PCA/IT y PRST con uso indebido.
- Plantea medidas para evitar que usuarios sean dirigidos a sitios/aplicaciones fraudulentas y proteger poblaciones vulnerables.
- Aunque existen obligaciones antifraude en la regulación vigente, los controles de operadores y asignatarios no han sido efectivos, y se requiere mayor articulación interinstitucional (incluido el sector financiero).
- La adopción de nuevas tecnologías o estándares requerirá análisis de impacto normativo (AIN) para validar viabilidad técnica, económica y legal.



No obstante lo anterior, no da respuesta al comentario expreso realizado por COMCEL con el cual solicitaba autorización para terminar contratos con PCA/IT abiertamente reincidentes.

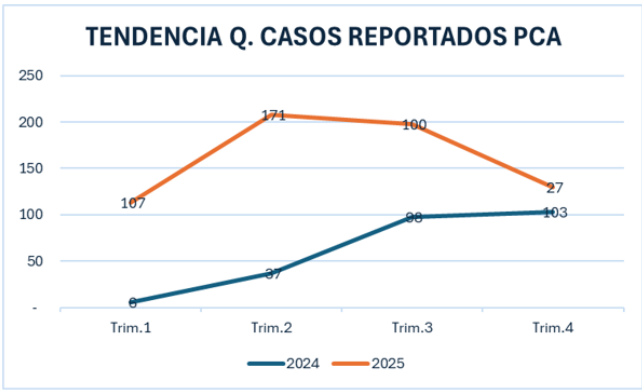
Esta situación ha permitido que los PCA/IT, una vez notificados de la recuperación del código corto, utilicen los demás códigos asignados para enviar a través de dicho código los mensajes fraudulentos, y continuar con el fraude.

1.2. Sobre la ausencia de análisis respecto de la suspensión provisional de códigos cortos al inicio de una actuación administrativa:

No se encuentra un análisis actualizado que revise la medida adelantada por la CRC planteada en el numeral **7.4.3 TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto**, en el marco de una actuación administrativa, dentro del documento objeto de estudio.

Como primera medida, es importante indicar que esta medida se tomó, gracias a la insistencia de los diferentes PRSTM de exigir a la CRC celeridad en su proceso administrativo de recuperación de códigos cortos, pues los tiempos de demora de la misma en este proceso permitían que muchos usuarios recibieran mensajes de texto con contenido presuntamente fraudulento.

Así las cosas, durante el último trimestre de 2025, (fecha a partir de la cual empezó a suspender de manera provisional los códigos cortos al inicio de la actuación administrativa), la CRC ha notificado a COMCEL de la suspensión provisional de 17 códigos cortos, lo cual ha generado una reducción significativa de 73% en el número de casos escalados desde COMCEL a diferentes PCA de la siguiente manera:



Así las cosas, durante el 2024, COMCEL reportó 244 casos de mensajes con contenido presuntamente fraudulento a diferentes PCA.

Durante los tres primeros trimestres del 2025, reportó 378 casos, encontrándose **para el último trimestre que tan solo se reportaron 27 casos**, así:



CASOS REPORTADOS A LOS PCA					
Periodo	Trim.1	Trim.2	Trim.3	Trim.4	TOTAL
2024	6	37	98	103	244
2025	107	171	100	27	405
TOTAL	113	208	198	130	649

Esta simple medida, que con tanta insistencia solicitaban los PRSTM, fue aplicada por la CRC sin que fuera necesaria una modificación regulatoria.

De la misma manera, se encuentra ausente un análisis que determine la viabilidad de terminar los contratos existentes entre PCA y PRSTM cuando al PCA se le han recuperado de manera reiterada códigos cortos por indebido uso de la numeración al remitir mensajes con contenido presuntamente fraudulentos.

Para el caso concreto en el cuadro que se presenta a continuación, se observa que el PCA que a todas luces incumple la normativa, es HABLAME. Esta situación ha sido escala en múltiples oportunidades a la CRC, sin que haya sido posible obtener una respuesta positiva para poder terminar el contrato con este PCA infractor; Obligando a empresas como COMCEL a mantener una relación contractual con un operador que abiertamente incumple la normativa, y que permite con su actuar a miles de colombianos.

ESCALAMIENTOS REALIZADOS A LOS PCA 2024 Y 2025										
PCA/PERIODO	2024				2025				TOTAL	
	Trim.1	Trim.2	Trim.3	Trim.4	Trim.1	Trim.2	Trim.3	Trim.4		
PCA HABLAME COLOMBIA SA ESP. - AZP COLOMBIA SAS			49	81	81	148	91	19	469	
PCA HABLAME COLOMBIA SA ESP. - TELECOM SMS S.A.S	3	16	22						41	
PARTNERS TELECOM COLOMBIA SAS		7		9	7				23	
PCA ATENEA MOBILE S.A.S		1	6	4	4	1	2		18	
PCA ESTRATEC SAS	1	2	3	2	3	2	2		15	
PCA ELIBOM COLOMBIA SAS			1	1	6	2	2		12	
PCA INFOBIP COLOMBIA S.A.S		2	7	1					10	
COLOMBIA TELECOMUNICACIONES SA ESP	2	4		2					8	
PCA HABLAME COLOMBIA LDI SAS ESP		1			3	4			8	
COLOMBIA TELECOMUNICACIONES S.A. E.S.P.				1		6			7	
PCA INALAMBRIA INTERNACIONAL S.A			2			2	2	1	7	
PCA TELECOM SMS SAS								5	5	
PCA ALCASAGAR			2			1			3	
PCA AXESNET S.A.S.			2					1	3	
COLOMBIA TELECOMUNICACIONES S.A. E.S.P.				1			1		2	
PCA Bemobi (Tiara)						2			2	
CYCLELOGIC COLOMBIA LTDA		1	1						2	
PCA AXESNET S.A.S.									2	
PCA HABLAME COLOMBIA SA ESP. - AIRTIME TECHNOLOGIES CHILE SPA						2			2	
PCA SERVICIOS DE APOYO EMPRESARIAL COLOMBIA SAS			1			1			2	
SERVICIOS DE APOYO EMPRESARIAL COLOMBIA SAS				1					1	
HABLAME COLOMBIA LDI SAS ESP		1							1	
INDEFINIDO - SIN ASIGNACION					1				1	
PCA HABLAME COLOMBIA SA ESP								1	1	
PCA HABLAME COLOMBIA SA ESP. - MITTO AG			1						1	
PCA INTICO COLOMBIA SAS.					1				1	
PCA KRONOS MOBILE S.A.S.			1						1	
PCA SIGMA MOVIL S.A.S					1				1	
TOTAL	6	37	98	103	107	171	100	27	649	



Como se puede observar, durante el año 2024 y 2025, HABLAME tuvo los siguientes escalamientos:

- 469 escalamientos, por envío de mensajes de texto con contenido fraudulento con códigos asignados a A2P COLOMBIA SAS.
- 41 escalamientos con códigos asignados a TELECOM SMS S.A.S.
- 9 escalamientos con códigos cortos asignados directamente a HABLAME LDI
- 1 escalamiento sobre un código corto que le fue asignado a HABLAME,
- 1 escalamiento sobre un código corto asignado a la empresa Airtime Technologies Chile
- 1 escalamiento que le fue asignado a la empresa Mitto.

Lo anterior, deja abiertamente en evidencia que HABLAME permite cualquier tipo de tráfico, sin implementar medidas tecnológicas para evitar el envío de SMS con contenido fraudulento.

Los demás operadores reseñados en el cuadro, si bien tuvieron eventos de escalamientos, su frecuencia fue muy inferior, evidenciando un ajuste en sus sistemas tecnológicos.

Así las cosas, es importante indicar que la CRC presenta una propuesta regulatoria para imponer a todos los PRSTM, PCA e IT, cuando el único que no aplica controles a los SMS que envía a través de los operadores móviles es HABLAME, generando con esto cargas administrativas y económicas, sobre actores que se esfuerzan por cumplir su obligación regulatoria y preservar al usuario.

1.3. Sobre la asignación de Códigos cortos:

Sobre la asignación de códigos cortos, es importante indicar que el encargado de asignar la numeración corta es la CRC. En este sentido, la CRC debe hacer una evaluación exhaustiva de los solicitantes de la numeración, en donde constate las calidades, condiciones, y demás requisitos que permitan dar tranquilidad del uso que se va a dar al potencial asignatario de la numeración, y no trasladar con posterioridad el problema a los PRSTM quienes se ven obligados a implementar medidas tecnológicas para evitar el envío de mensajes con contenido fraudulento.

En consecuencia, si la asignación del código corto se hace de manera consciente, a un usuario que la utiliza de manera adecuada, este tipo de problemas no se presenta. Por el contrario, si se evidencia que la numeración no esta siendo bien utilizada, la consecuencia debe ser la recuperación de los códigos cortos mal utilizados, y no volver a asignar hasta tanto demuestre que implementó medidas que evidencien su buen uso.

En este sentido, y solo a título de reflexión, si es la CRC la asignataria de los códigos cortos, y con posterioridad evidencia el mal uso que se le da a los mismos por parte de PCA/IT, de manera reiterada, en necesario que se inicié el proceso de terminación de los acuerdos de acceso con los infractores reincidentes.



1.4. Sobre la ausencia de medidas educativas en cabeza de la CRC:

Finalmente, llama la atención la ausencia de una propuesta que ponga en cabeza de la CRC una obligación de realizar campañas educativas a los ciudadanos para prevenir el fraude a través de mensajes o llamadas.

Consideramos que este es el ente, coordinado con diferentes entidades del Estado el que debe impartir medidas educativas, haciendo consciente al ciudadano del riesgo que se genera por la mala asignación, y de las medidas que tiene para denunciar el mal uso por parte de dichos asignatarios.

2. SOBRE LAS ALTERNATIVAS REGULATORIAS Y SU IMPACTO ECONÓMICO:

La CRC determina como alternativas regulatorias temáticas que comprenden: (i) la mitigación del contacto fraudulento a usuarios a través de los servicios móviles tradicionales de mensajes cortos de texto (SMS); (ii) la mitigación del contacto fraudulento mediante los servicios tradicionales de voz; (iii) el fortalecimiento de la educación y la capacidad de los usuarios para identificar y prevenir prácticas fraudulentas; y (iv) la revisión y simplificación normativa del régimen de administración de los recursos de identificación, con el fin de dotarlo de herramientas que contribuyan a la prevención y control del fraude. Y propone la implementación de las siguientes medidas técnicas:

- **Sistemas de autenticación y validación de identidad.**
- **Trazabilidad y origen de comunicaciones**
- **Controles tecnológicos para mensajes A2P y P2P.**
- **Unificación y estandarización de listas tecnológicas anti-fraude.**
- **Implementar herramientas tecnológicas para administración de recursos de identificación.**
- **Implementar medidas para evitar direccionamiento a sitios fraudulentos.**
- **Utilizar de API y datos de red para validaciones antifraude:** Incentivar el aprovechamiento de API de operadores (validación de titularidad, SIM swap detect, estado de línea, etc.) para fortalecer procesos de autenticación en otros sectores (por ejemplo, financiero).
- **Estándares técnicos obligatorios (previa evaluación AIN).**

Al respecto, es fundamental que la CRC tenga en cuenta las bajas tarifas de cargos de acceso a SMS con los cuales se remunera a los PRSTM por el envío de estos mensajes de texto, son valores que no contemplan ni soportan los costos que se generan por la implementación de estas medidas.

En consecuencia, la adopción de nuevas obligaciones tecnológicas para mitigar el fraude mediante servicios móviles exige un Análisis de Impacto Normativo (AIN) que permita evaluar su viabilidad técnica, económica y jurídica. Este análisis es indispensable para garantizar que las soluciones



regulatorias sean proporcionales, consistentes con el problema identificado y compatibles con los principios de economía, eficiencia, interoperabilidad, trazabilidad y cooperación interinstitucional; máxime como ya se advirtió, se está creando una regulación para poner en cintura a un solo PCA/IT, perjudicando con ello a los demás que si hacen la tarea.

Sin un AIN para cada una de las medidas acá presentadas, se genera el riesgo de imponer cargas regulatorias excesivas o inaplicables, especialmente en áreas donde la tecnología evoluciona rápidamente y requiere validación rigurosa antes de convertirse en mandato obligatorio.

Finalmente, se reitera necesario que la CRC analice con detalle los efectos que ya han tenido las herramientas vigentes, particularmente el bloqueo provisional de mensajes de texto asociados a investigaciones por uso indebido, mecanismo que —según los resultados operativos— ha reducido considerablemente la problemática. Este dato evidencia que medidas focalizadas, basadas en control de numeración y gestión del recurso, pueden generar impactos contundentes sin necesidad inmediata de imponer cargas tecnológicas adicionales. El AIN permitiría determinar si estas acciones existentes deben consolidarse, ajustarse o complementarse, evitando duplicidad de obligaciones o inversiones innecesarias.

Así las cosas, se reitera que es fundamental considerar que muchas de las medidas planteadas implican altos costos de implementación tecnológica, los cuales no se corresponden con la estructura económica del servicio, especialmente cuando se comparan con el bajo valor del cargo de acceso de un SMS. Imponer soluciones costosas en un entorno donde el ingreso por mensaje es mínimo puede generar ineficiencias, distorsiones competitivas e incluso afectar la sostenibilidad del ecosistema A2P/P2P. Un AIN resulta imprescindible para balancear costos y beneficios, estimar impactos sobre operadores, PCA/IT y usuarios, y asegurar que cualquier obligación adicional sea realmente necesaria, proporcional y sostenible.

3. SOBRE LAS PROPUESTAS REALIZADAS:

TEMÁTICA 1: Falta de identificación clara del remitente en SMS A2P

Situación identificada: <i>Los SMS A2P se originan principalmente desde códigos cortos numéricos compartidos entre múltiples marcas y campañas, lo que provoca que el usuario no pueda distinguir fácilmente quién envía el mensaje.</i>	COMENTARIO COMCEL
Alternativa 1. <i>Se conserva el esquema regulatorio actual.</i>	
2. Asignación y uso de código alfanumérico para todos los originadores de contenido (Sender ID).	Para esta alternativa, debe quedar claramente establecido en la regulación, que el encargado de cumplir con este requerimiento es el PCA/IT, quien



	es el dueño del código, y es el que conoce el contenido del mensaje que va a remitir. Desde el momento mismo del envío debe identificar su mensaje con dicho código alfanumérico. Sino queda expreso, los PCA siguen navegando en la ambigüedad y en el incumplimiento.
Alternativa 3 Asignación y uso de código alfanumérico solo para tráfico transaccional. <i>el tráfico promocional continúa identificándose mediante códigos cortos o números E.164, manteniendo la obligación actual de incluir el nombre del originador dentro del texto del mensaje.</i>	Debe quedar claramente establecido en la regulación, que el encargado de cumplir con este requerimiento es el PCA/IT, quien es el dueño del código, y es el que conoce el contenido del mensaje que va a remitir. Sino queda expreso, los PCA siguen navegando en la ambigüedad y en el incumplimiento.

TEMÁTICA 2: Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude

Situación identificada: Debilidades estructurales que obstaculizan la trazabilidad y la asignación de responsabilidades en caso de fraude. Opera un mercado informal con originadores de contenido sin controles homogéneos ni verificaciones previas. Por otra, la cadena de valor carece de puntos de control claros para imputar responsabilidades cuando se perjudica al usuario	COMENTARIO COMCEL:
<i>Alternativa 1 Statu quo.</i>	
Alternativa 2: Proceso de validación centralizado de originadores de contenido. <i>Administrado por un tercero para validar agregadores, marcas y campañas antes de cursar tráfico A2P.</i>	Adicional a ser innecesaria, toda vez que se pretende implementar para todos los PRSTM, PCA/IT, siendo solo uno el que incumple los parámetros regulatorios existentes; por las siguientes razones legales y regulatorias esta medida no es viable: 1. Rol definido en la cadena A2P • El operador actúa como transportador de tráfico, no como generador de contenido. • Según la Resolución CRC 5050 de 2016 y sus modificaciones, el originador (PCA) es



	quien contrata el envío y define el contenido del mensaje. • El operador no tiene facultad para modificar ni validar el contenido, salvo en casos de bloqueo por seguridad o escenarios de fraude (smishing). 2. Principio de neutralidad de red (Ley 1341 de 2009, Art. 22) • El operador debe garantizar la transmisión de datos sin alterar el contenido. • Intervenir en el contenido podría vulnerar este principio y generar riesgos legales. • Es importante reiterar que el PRSTM no puede ser juez y parte en el contenido que se transmite, por lo que es el alojador del contenido quien tiene dicha responsabilidad. 3. Imposibilidad técnica de verificar cada mensaje • El tráfico A2P se envía en volúmenes masivos y en tiempo real. • No es viable aplicar filtros semánticos sin afectar la calidad del servicio y la latencia, lo que podría constituir incumplimiento regulatorio. 4. Responsabilidad contractual del PCA • El PCA es quien contrata el servicio de mensajería y define el remitente, contenido y destinatarios. • El PCA debe garantizar que el contenido cumple con la ley y no induce fraude (Ley 1480 de 2011 – Estatuto del Consumidor). 5. Cumplimiento del operador en trazabilidad mínima • El operador conserva logs de entrega (MSISDN destino, timestamp, ID de mensaje, PCA asociado).
--	---



	• Esto permite identificar el PCA responsable en caso de fraude, cumpliendo con la obligación de colaboración ante autoridades.
Alternativa 3: Proceso de validación distribuido (DLT) de originadores de contenido. <i>Establece un proceso de validación distribuido soportado en tecnología blockchain (DLT), para garantizar inmutabilidad y auditoría descentralizada, a fin de verificar agregadores, marcas y campañas antes de cursar tráfico A2P.</i>	Por las mismas razones indicadas para la alternativa 2, esta medida no es necesaria ni viable.
Alternativa 4: Identificación exclusiva mediante códigos cortos y numeración E.164. <i>Asigna a cada marca un código corto o número E.164 exclusivo (NDC 940) para mejorar la identificación, pero sin validación preventiva.</i>	Se debe controlar la asignación de los códigos alfa numéricos, de tal manera que no se puedan generar códigos que confundan al usuario, cambiando letras, ejemplo BancoXYZ y asignen u código Banc0XYZ. Igual que en las otras alternativas el control debería estar del lado del agregador de contenido, quien origina el tráfico y conoce a sus clientes.

TEMÁTICA 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

Situación identificada: No se contempla un control sobre el tráfico SMS P2P, especialmente en planes que incluyen mensajes ilimitados.	COMENTARIO COMCEL:
Alternativa 1 Statu quo. <i>Se mantiene el esquema actual, sin introducir controles adicionales sobre el tráfico P2P.</i>	
Alternativa 2 Control de patrones de tráfico atípicos. <i>Implementación de mecanismos de detección y bloqueo para identificar comportamientos anómalos en el tráfico SMS P2P, como envíos masivos a números desconocidos o fuera del patrón habitual. Incluye alertas automáticas y bloqueos temporales para prevenir el</i>	Este tipo de controles tiene un pequeño rango de error y puede afectar en un bajo porcentaje a algunos clientes y/o mensajes legítimos. Así las cosas, estos escenarios no debiera interpretarse como una afectación del servicio.



uso fraudulento de planes ilimitados y reducir el mercado secundario.	
Alternativa 3 Alternativa 3: Límite de SMS P2P por usuario. Establecimiento de un tope máximo de mensajes P2P por usuario en un periodo determinado, incluso en planes ilimitados. Una vez alcanzado el límite, se bloquea el envío de nuevos mensajes hasta el siguiente ciclo	Esta medida resulta técnica y jurídicamente desproporcionada. En particular, la medida contraviene el principio de neutralidad tecnológica, al obligar a los proveedores a adoptar configuraciones específicas de red y de control de tráfico que no responden a la arquitectura ni a la evolución natural de sus plataformas, limitando la libertad para gestionar sus redes de manera eficiente. Asimismo, vulnera el principio de intervención mínima y regulación eficiente, dado que introduce una restricción generalizada que impacta a todos los usuarios, incluidos aquellos con usos legítimos, sin demostrar que sea el mecanismo menos intrusivo ni el más eficaz para mitigar el fraude. Adicionalmente, afecta el principio de protección de los derechos de los usuarios, al deteriorar la experiencia del servicio contratado bajo esquemas comerciales ilimitados, generando bloqueos automáticos no asociados a fallas del usuario sino a una restricción regulatoria exógena. Finalmente, la medida desconoce el principio de promoción de la inversión y la innovación, al exigir desarrollos técnicos complejos y costosos en los sistemas de red y facturación, desviando recursos que podrían destinarse a soluciones más focalizadas y efectivas contra el fraude, en contravía del objetivo de eficiencia y sostenibilidad del sector TIC previsto en la Ley 1341.

TEMÁTICA 1: Mecanismos de verificación, autenticación e identificación del originador de la llamada de voz, o limitaciones al enmascaramiento de la identidad de la línea llamante (CLI) 26 (Spoofing)

Situación identificada: No se cuenta con la obligación de implementar mecanismos de verificación, autenticación e identificación del	COMENTARIO COMCEL:
--	----------------------------------



<i>originador de la llamada de voz, y al mismo tiempo no existe una prohibición explícita ni mecanismos robustos para impedir que llamadas internacionales entrantes utilicen números del Plan Nacional de Numeración (PNN) como identificador (CLI).</i> <i>Esta práctica, conocida como CLI masking o enmascaramiento, sin un mecanismo de verificación, autenticación e identificación del originador de la llamada, permite a los delincuentes simular llamadas locales en otros países, o suplantar la identidad de personas o instituciones públicas o privadas, aumentando la efectividad de fraudes como vishing y phishing telefónico, y dificultando posterior identificación de la trazabilidad por parte de las autoridades judiciales en las investigaciones.</i>	
Alternativa 1 <i>Statu quo</i>. Mantiene el marco actual sin controles adicionales sobre el uso de numeración E.164.	
Alternativa 2: Prohibición total del enmascaramiento de la identidad de línea llamante (CLI) <i>Obliga a los operadores a bloquear todas las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número colombiano, salvo excepciones de roaming legítimo, eliminando un canal importante de suplantación.</i>	Esta propuesta debe exigir que todo operador u originador de tráfico de larga distancia, operador de LDI y Carrier internacional cumpla con las recomendaciones de la UIT E.164 respecto a los formatos y longitudes de numeración que corresponden a cada país, respetando los códigos del país donde se origina la llamada, incluyendo la identificación con símbolo (+) de la llamada originante de LDI. Lo anterior apoyara en la identificación del número CLI del usuario que este marcando y el origen de la llamada. Si no se cumple con estos parámetros, la llamada debe bloquearse, so pena de multas para el PRSTM que no bloquee dicho tráfico. Por consiguiente, los operadores LDI y carriers internacionales deberán valerse de herramientas en su red para limitar en lo posible el tráfico con numero A inconsistente o modificado.
Alternativa 3: Permitir enmascaramiento con obligación de identificación y etiquetado de	En la práctica, la evidencia operativa demuestra que las etiquetas o advertencias en



llamadas para el usuario. <i>Permite llamadas internacionales con identificador de línea llamante (CLI) nacional, pero exige que sean identificadas y marcadas como «No verificada» o «Probable fraude» en el dispositivo del usuario, alertando sobre posible riesgo de suplantación.</i>	el dispositivo (“No verificada” o “Probable fraude”) tienen una efectividad limitada, ya que los usuarios tienden a ignorar este tipo de alertas o no comprenden su alcance, por lo que el comportamiento fraudulento persiste. Adicionalmente, desde el punto de vista técnico, no es posible identificar de manera confiable el origen del tráfico para diferenciar llamadas internacionales con CLI nacional, tráfico de clientes en roaming o tráfico cursado desde redes de otros operadores, lo que genera un alto riesgo de falsos positivos y etiquetados erróneos. Esto afecta directamente la experiencia del usuario, quien continuará recibiendo las llamadas no deseadas —ahora acompañadas de alertas confusas— incrementando la molestia y las reclamaciones, sin una reducción real del fraude. En este contexto, la medida carece de una evaluación de impacto normativo que demuestre su proporcionalidad y eficacia, y puede derivar en una carga regulatoria innecesaria, con impactos negativos sobre la calidad del servicio y la confianza del usuario, sin cumplir de manera efectiva el objetivo de protección frente a la suplantación.
Alternativa 4: Implementación de STIR/SHAKEN/RCD para tráfico nacional e Internacional. <i>Requiere que todas las llamadas estén firmadas digitalmente mediante STIR/SHAKEN, incorporando Rich Call Data (RCD) para autenticidad y visualización de información del originador, bloqueando o marcando llamadas no verificadas.</i>	No vemos viable en este momento la implementación de STIR/SHAKEN por las siguientes razones: - Requiere una Inter operatividad muy compleja entre operadores que originen tráfico a Colombia carriers internacionales, operadores de LDI y operadores nacionales, la exigencia de estas condiciones puede afectar significativamente la facilidad de acceso de las comunicaciones a el país. - El costo de implementación y licenciamiento es alto para todos los operadores y carriers que intervienen en la comunicación.



	- Requiere una operación compleja, dado que necesita mantenimiento y soporte para escalamientos de listas de excepciones y/o desbloques. - Las demoras en la implementación, y los rápidos cambios en la forma de los fraudes, podría volver desactualizada la implementación con las nuevas metodologías de fraude. Con un marco regulatorio que exija el cumplimiento de las normas internacionales referentes a la numeración internacional, es suficiente para que los operadores de LDI, pueden trasladar estas exigencias a los carries internacionales y puedan tomar acciones de control al detectar patrones anómalos de tráfico internacional.
--	--

7.2.2 TEMÁTICA 2: Falta de aplicación coordinada de métodos preventivos de filtrado de tráfico de voz

Situación identificada: <i>En Colombia no existe un esquema uniforme que permita a los operadores a aplicar métodos preventivos de filtrado estandarizado en tráfico de voz, lo que dificulta la detección temprana de patrones anómalos asociados a fraude (vishing, llamadas masivas ilegítimas, spoofing). Esta falta de coordinación genera vulnerabilidades y limita la capacidad de respuesta ante incidentes.</i>	COMENTARIO COMCEL:
Alternativa 1: Statu quo: <i>Cada operador aplica controles internos sin lineamientos regulatorios comunes; no existe monitoreo ni filtrado coordinado del tráfico de voz.</i>	
Alternativa 2: Lineamientos regulatorios para monitoreo de tráfico <i>Esta alternativa propone que la CRC establezca lineamientos regulatorios obligatorios para que</i>	Esta iniciativa es viable solo si, el operador de LDI es el que debe hacer el monitoreo basado en comportamientos de tráfico para en lo posible bloquear el tráfico sospechoso de fraude o



<i>todos los operadores implementen mecanismos de monitoreo en tiempo real del tráfico de voz. Esta alternativa propone la creación de una plataforma nacional centralizada, que permita a los operadores reportar en tiempo real patrones sospechosos, incidentes de fraude y llamadas con posible enmascaramiento de la identidad de línea llamante (CLI). La plataforma funcionaría como un hub o puerto de intercambio de alertas y señales de riesgo, facilitando la coordinación entre operadores, la trazabilidad de eventos y la respuesta rápida ante campañas fraudulentas. Esta alternativa propone exigir que todas las llamadas nacionales e internacionales entrantes estén firmadas digitalmente mediante el protocolo STIR/SHAKEN, garantizando la autenticidad del número mostrado al usuario.</i>	enmascaramiento, esta actividad es simple y puede disminuir significativamente la problemática. Debe definirse en la regulación las medidas en caso de que algún operador de LDI incumpla o sea evidente que no realiza de forma eficiente el monitoreo y control de tráfico.
Alternativa 3: Creación de una plataforma de articulación e intercambio de alertas	No es necesaria la implementación de una plataforma centralizada, cada operador de LDI puede tener localmente sus registros de detecciones, en caso de requerir apoyo o notificación a otro operador lo puede realizar vía correo electrónico, como actualmente las áreas de fraude de los diferentes operadores lo realizan.
Alternativa 4: Implementación de STIR/SHAKEN/RCD	Como lo mencionamos en la temática anterior no vemos viable la implementación de STIR/SHAKEN otras alternativas mucho más simples puede disminuir significativamente la problemática. Identificar las llamadas no solucionan la problemática igual la llamada se recibe.

TEMÁTICA 3: Ausencia de diferenciación en rangos de numeración para comunicaciones personales, comerciales y publicitarias

Situación identificada: <i>En Colombia no existe una diferenciación entre los rangos de numeración asignados a comunicaciones</i>	COMENTARIO COMCEL:
---	----------------------------------



personales y aquellos utilizados para fines comerciales (atención al cliente) y/o publicitarios	
Alternativa 1. Consiste en mantener el marco regulatorio y operativo vigente, en el cual no existe distinción entre los rangos de numeración asignados para comunicaciones personales y aquellos utilizados para fines comerciales o publicitarios.	
Alternativa 2: Definición de rangos de numeración exclusivos para comunicaciones comerciales y publicitarias. El objetivo es establecer una diferenciación clara y visible entre las llamadas de carácter personal y aquellas con fines comerciales, facilitando la identificación por parte del usuario mediante el indicativo nacional de destino NDC, y habilitando controles regulatorios y operativos más precisos sobre el tráfico comercial.	La alternativa propuesta no resulta viable ni eficaz para solucionar el problema identificado, en la medida en que parte de un supuesto que no se cumple en la práctica: que el usuario reconoce y entiende la diferenciación de rangos de numeración a partir del NDC. En la experiencia operativa, los usuarios no conocen ni asocian los indicativos de numeración con el carácter comercial o personal de una llamada, por lo que la creación de rangos exclusivos no genera un efecto real de prevención ni de reducción de llamadas no deseadas. Adicionalmente, aunque introduce una carga regulatoria y operativa para los proveedores en la gestión de numeración y enrutamiento, no ataca el problema estructural del fraude y la suplantación, ni garantiza controles efectivos frente al uso indebido de la numeración. Así, la propuesta se limita a una diferenciación formal que carece de impacto práctico en la protección del usuario, resultando desproporcionado frente a los costos y esfuerzos de implementación y sin resolver el problema que pretende mitigar.
Alternativa 3: Etiquetado obligatorio en el identificador de llamadas para contactos comerciales, usando la numeración actual. Todas las llamadas comerciales y publicitarias incluyan un indicador visible en el identificador de llamada (Caller ID), que permita al usuario distinguir el propósito de la comunicación. «Comercial», «Publicidad», «Atención al cliente», etc.) o, cuando la tecnología lo permita, en la implementación de Rich Call Data (RCD) o	En la práctica, la evidencia operativa demuestra que las etiquetas o advertencias en el dispositivo (“No verificada” o “Probable fraude”) tienen una efectividad limitada, ya que los usuarios tienden a ignorar este tipo de alertas o no comprenden su alcance, por lo que el comportamiento fraudulento persiste. Como lo mencionamos en la temática anterior no vemos viable la implementación de



Branded Caller ID bajo la implementación del esquema de STIR/SHAKEN/RCD, mostrando el nombre, logo y motivo de la llamada.	STIR/SHAKEN otras alternativas mucho más simples puede disminuir significativamente la problemática. Por otro lado, Identificar las llamadas no solucionan de fondo los reclamos de los clientes, dado que igual la llamada se recibe.
--	--

TEMÁTICA 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

Situación identificada: ausencia de criterios uniformes y mecanismos coordinados para la aplicación de listas de no originación (DNO por sus siglas en inglés Do Not Originate) entre los operadores ha generado fragmentación y brechas en la protección contra el spoofing y la suplantación de identidad en el canal de voz. Cada operador gestiona sus propias listas razonables de números que no deben ser utilizados para originar llamadas, lo que dificulta la trazabilidad, permite la persistencia de prácticas fraudulentas y limita la eficacia de las medidas preventivas.	
Alternativa 1	Esta alternativa es viable, cada operador de LDI, puede según sus criterios tener localmente el repositorio con sus números de no originación, según sus monitoreos internos. Lo importante es que exista un marco regulatorio en el cual estos monitoreo y bloqueos estén permitidos para el control de fraude o acoso a los usuarios
Alternativa 2: Registro DNO Nacional Único administrado por la CRC: Consiste en mantener el esquema actual de gestión de listas de no originación (DNO) en el canal de voz, en el cual cada operador decide si administra o no de manera independiente sus propias listas de números que no deben ser utilizados para originar llamadas. Bajo este enfoque, no existe un marco regulatorio uniforme ni una coordinación estandarizada para la	No vemos necesario tener un registro único, cada operador puede manejar sus registros localmente de manera efectiva, añadir consultas a fuentes externas complejiza la implementación y puede afectar la velocidad de la detección y control de fraude. De requerirse cada operador puede informar de manera colaborativa, diferentes alarmas vía



definición, actualización o consulta de las listas DNO	correo electrónico entre áreas de fraude, como actualmente se realiza.
Alternativa 3: Estándar Mínimo Obligatorio de DNO con «listas propias» por PRST. <i>Esta alternativa plantea que cada PRST mantenga su propia lista de no originación (DNO), pero bajo la obligación de cumplir con un estándar mínimo uniforme definido por la CRC. El estándar establecería categorías obligatorias de números a incluir como, por ejemplo, números no atribuidos, no asignados, no adjudicados, números comerciales de solo recibo de llamadas, etc.</i>	Esta alternativa es viable, siempre que el estándar mínimo definido no afecte el desempeño de las redes, por consiguiente, la lista de números no debería superar los 10.000 números, que no se requiera actualización dinámica y que la lista pueda configurarse localmente en la red de cada operador.
Alternativa 4: Sustitución funcional de DNO por autenticación del CLI y reglas anti-spoofing internacional STIR/SHAKEN/RCD.	Como lo mencionamos en la temática anterior no vemos viable la implementación de STIR/SHAKEN otras alternativas mucho más simples puede disminuir significativamente la problemática.

Temáticas enfocadas en la educación de la ciudadanía

Situación identificada: <i>Desconocimiento de los usuarios sobre privacidad de la información, modalidades de fraude, técnicas de ingeniería social, acciones de prevención y de mitigación, lo cual facilita la obtención de datos personales con fines fraudulentos por parte de personas inescrupulosas y la comisión de fraudes a través de mensajes de texto y llamadas de voz.</i>	COMENTARIO COMCEL:
Alternativa 1 <i>Mantener la provisión de redes y servicios de telecomunicaciones, así como la provisión de contenidos y aplicaciones y la integración tecnológica, sin obligaciones de socialización o educación a los usuarios finales.</i>	COMCEL dentro de su ejercicio ha realizado campañas educativas a los usuarios, sin hacer evidente su efectividad. En este sentido, se considera necesario mantener el STATU QUO.
Alternativa 2: Pedagogía y lista de campañas más denunciadas. <i>Incluir una obligación de divulgación de información con objetivos pedagógicos y de prevención a los usuarios de servicios móviles, en</i>	Como se indicó anteriormente, COMCEL ha realizado diferentes campañas educativas a sus usuarios sin hacer evidente su efectividad. Los usuarios no tienen el debido cuidado para revisar la página de la CRC, lo que hace



cabeza de los PRST, PCA e IT. Adicionalmente, la CRC creará y administrará un portal que incluya una lista con las campañas más denunciadas ante la CRC e identificadas por esta autoridad de oficio que sean utilizados para contactar usuarios con fines presuntamente fraudulentos.	innecesario la denuncia de las campañas ante la CRC. Esta medida solo trae carga administrativa para los PRTSM, sin evidenciarse un retorno que beneficie al mismo usuario. Medida innecesaria-
Alternativa 3: Sistema de trazabilidad de PQR relacionadas con fraude a través de mensajes de texto o llamadas de voz. Crear e implementar un sistema de trazabilidad de las temáticas objeto de PQR presentadas por los usuarios a la CRC, o a los PRST, PCA e IT, relacionadas con fraudes a través de mensajes de texto o llamadas telefónicas. Este sistema sería administrado por la CRC y alimentado con las PQR presentadas por los usuarios, así como con la información periódica que reporten los PRST, PCA e IT. Adicionalmente, se definiría una estrategia educativa y de prevención de manera conjunta entre los agentes regulados y la CRC, a la cual se invitaría también a otras entidades competentes en estos asuntos	Por las mismas razones indicadas en la alternativa 2, esta medida es innecesaria, por ser ineficaz. Adicionalmente se hace un llamado a la CRC para que haciendo uso de sus posibilidades, a través de los diferentes medios de comunicación haga estas campañas educativas públicas a los usuarios, y no cargue mas a los PRSTM, con estas obligaciones. Como se indicó anteriormente, el código corto es asignado por la CRC. En este sentido, debe tener un mínimo de diligencia frente al asignatario de la misma.

TEMÁTICA 1: Elementos para la mitigación del fraude por medio de la identificación de agentes reincidentes de acciones irregulares mediante el uso de códigos cortos

Situación identificada: En el marco del proceso de recuperación de recursos de identificación, establecido en el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016, se ha identificado el uso indebido de códigos cortos de forma reincidente.	COMENTARIO COMCEL:
<i>Alternativa 1. Mantener el régimen actual de asignación y recuperación de códigos cortos, sin introducir medidas específicas frente a la reincidencia. Se seguiría aplicando la recuperación del recurso por el incumplimiento de</i>	Es necesario implementar consecuencias ante la reincidencia por el indebido uso de códigos cortos.



<i>las obligaciones generales de los asignatarios de los recursos de identificación establecidas en el artículo 6.1.1.6.2.; así como, de las causales del artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, sin obligaciones adicionales para nuevos procesos de asignación y/o recuperación</i>	
Alternativa 2: Establecer obligaciones y consecuencias ante reincidencia. <i>Incorporar al régimen normativo obligaciones y consecuencias específicas relacionadas para los asignatarios reincidentes por recuperación de códigos cortos</i>	Esta acción es fundamental para que realmente las diferentes alternativas planteadas tengan un efecto positivo.

TEMÁTICA 2: Condiciones para la cesión o transferencia de la asignación de recursos de identificación en códigos cortos.

Situación identificada <i>En el marco del proceso de asignación de recursos de identificación, establecido en el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, se ha identificado la posibilidad de transferir o ceder el recurso de identificación cuando se autorice</i>	COMENTARIO COMCEL
Alternativa 1. <i>Mantener el régimen actual, en el cual la cesión o transferencia de recursos de identificación se permite por lo contemplado en el parágrafo del artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, sin condiciones adicionales, siempre que se cumpla con los requisitos de asignación correspondientes</i>	Se debe mantener el STAU QUO. La posibilidad de transferir o ceder recursos de identificación, tal como la propone la CRC, no resulta adecuada en la medida en que termina desvirtuando el objetivo regulatorio de corregir conductas indebidas asociadas al uso de códigos cortos. Permitir la cesión abre la puerta a que los PCA o IT que hayan perdido dichos recursos como consecuencia de incumplimientos o malas prácticas los recuperen indirectamente a través de otros PCA, manteniendo en la práctica la misma capacidad operativa que se pretendía restringir. Esto no solo debilita el efecto disuasivo de la medida, sino que además perpetúa una ventaja injustificada para estos actores frente a quienes sí cumplen las reglas, afectando la equidad competitiva y reduciendo la efectividad de los



	mecanismos de control y sanción definidos por el regulador.
Alternativa 2: Imposición de condiciones para la cesión o transferencia <i>Establecer requisitos específicos para la cesión o transferencia de recursos de identificación, que incluyan, entre otros, la prohibición de cesión a reincidentes, obligación de mantener las condiciones iniciales de asignación, y la trazabilidad del recurso.</i>	Por las razones indicadas para la opción 1, consideramos que no es viable permitir la cesión o transferencia de códigos cortos. Los PCA o IT deben encontrar la necesidad de mantener sus códigos cortos, y esto solamente se logra si la consecuencia de su mal uso es la recuperación y la pérdida de la posibilidad de ser asignatarios de más códigos.

TEMÁTICA 3: Suspensión del tráfico cursado a través de un código corto en el marco de una actuación administrativa.

Situación identificada: <i>En el marco de una actuación administrativa de recuperación de un código corto, se ha identificado que el tráfico presuntamente fraudulento asociado a dicho recurso continúa cursándose hasta que se emita una decisión definitiva.</i>	COMENTARIO COMCEL:
Alternativa 1: <i>Mantener el procedimiento actual de recuperación de recursos de identificación, en el cual se contempla la suspensión del tráfico al inicio del proceso administrativo de recuperación.</i>	Mantener el STAU QUO. Como se ha indicado a lo largo de este documento, la medida aplicada por la CRC durante el último trimestre del 2025, ha permitido que los escalamientos a los PCA se reduzcan en mas de un 70%. Esta situación salvaguarda al usuario, y lo pone como centro de la actuación de la CRC. Esta medida, sin ser una medida regulatoria, da alivio a la problemática planteada, lo que hace evidente que la regulación solo debe imponerse cuando sea necesaria. Para el caso concreto, con solo una medida administrativa por parte de la CRC, se logró en gran medida dar solución a la problemática planteada. Así las cosas, esta medida, sumada a la posibilidad de terminar contrato con operadores



	reincidentes, da solución en su totalidad a la problemática planteada.
<i>Alternativa 2 Incorporar en el régimen la posibilidad de suspender temporalmente el tráfico cursado a través de un código corto en cualquier momento de la actuación administrativa, teniendo en cuenta las quejas y/o reportes de presunto fraude allegados a la Entidad.</i>	Por las razones antes expuestas, no es viable que la medida se imponga en cualquier momento de la actuación administrativa.

TEMÁTICA 4: Condiciones asociadas a la vigencia y obligaciones de actualización de la asignación de recursos de identificación.

Situación identificada.	COMENTARIO COMCEL:
<i>Los asignatarios de los recursos de identificación, en particular los asociados con los códigos cortos no actualizan la información depositada en el RPCAI o en el RUES cuando se presentan novedades en términos de su existencia y representación legal, lo que dificulta el contacto por parte del Administrador de los recursos de identificación en ejercicio de sus funciones, y la trazabilidad de los requerimientos de información en casos de uso indebido.</i>	
<i>Alternativa 1 Mantener el procedimiento de asignación de recursos de identificación establecido en artículo 6.1.1.5 de la Resolución CRC 5050 de 2016.</i>	Es necesario mantener la situación actual. Es una carga operativa muy grande para los asignatarios que si cumplen la regulación. La CRC debe de oficio identificar estos cambios, y proceder con la recuperación de los códigos, sin que este requisito se convierta en una nueva obligación para los asignatarios. La CRC debe recordar que debe imperar la simplificación regulatoria, y NO la imposición de nuevas obligaciones que además, no dan solución a la problemática planteada.
<i>Alternativa 2. Adicionar condiciones al Régimen de Administración de Recursos de Identificación asociadas a una vigencia específica para la asignación del código corto, así como la obligación de actualizar la información del</i>	Es necesario mantener la situación actual. Es una carga operativa muy grande para los asignatarios que si cumplen la regulación. La CRC debe de oficio identificar estos cambios, y proceder con la recuperación de los códigos, sin



<i>asignatario del código corto en el RPCAI y en el RUES de manera periódica</i>	que este requisito se convierta en una nueva obligación para los asignatarios. La CRC debe recordar que debe imperar la simplificación regulatoria, y NO la imposición de nuevas obligaciones que, además, no dan solución a la problemática planteada.
--	--

4. SOBRE LA CONSULTA REALIZADA:

Preguntas generales:

PREGUNTA CRC: *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 tiempos de implementación estima necesarios para cada una de las medidas propuestas, teniendo en cuenta los desarrollos y capacidades actuales de los PRST y agregadores? ¿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 en el país?*

RESPUESTA COMCEL:

a. Frente fraude en SMS:

Antes de definir tiempos de implementación para nuevas medidas, es indispensable que la CRC realice un análisis de necesidad y proporcionalidad sustentado en evidencia reciente. El propio proyecto reconoce que cualquier obligación tecnológica debe pasar por un Análisis de Impacto Normativo (AIN); esto cobra especial relevancia si se considera que la simple adopción de la suspensión provisional de códigos cortos asociados a presunto uso indebido ha generado una disminución superior al 70–90% en los reportes relacionados con mensajes fraudulentos. Esta reducción demuestra que la principal causa del problema estaba en la demora para suspender el envío desde numeración comprometida y que, una vez corregido ese procedimiento, el mercado respondió de manera inmediata y contundente, sin necesidad de imponer nuevas cargas tecnológicas.

En ese sentido, antes de establecer plazos de implementación para medidas adicionales —como autenticación obligatoria, trazabilidad avanzada, plataformas únicas, validación cruzada o estándares técnicos— la CRC debe determinar si realmente persisten brechas operativas que justifiquen inversiones significativas. Varias de las tecnologías sugeridas implican costos muy superiores al ingreso asociado al SMS, cuyo cargo de acceso es extremadamente bajo; exigir desarrollos de alto costo sin evidencia de necesidad podría generar distorsiones económicas, afectar la sostenibilidad del ecosistema A2P y trasladar cargas injustificadas a los PRST y agregadores. El AIN debe evaluar si



los resultados ya obtenidos con la suspensión provisional no hacen innecesaria —o por lo menos postergan— la adopción inmediata de soluciones tecnológicas complejas.

Bajo este enfoque, mientras que la CRC evalúa formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, el país puede continuar obteniendo resultados con medidas de bajo costo, alto impacto y rápida implementación, como el fortalecimiento de procesos de recuperación, reglas claras de reincidencia y mayor articulación sectorial. Solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

Adicionalmente, debe destacarse que, si se permitiera a los operadores bloquear de manera inmediata los mensajes que sus herramientas tecnológicas identifiquen como presuntamente fraudulentos, el fraude a través de SMS se reduciría casi en su totalidad. La experiencia reciente muestra que cuando se habilitan mecanismos ágiles de suspensión o bloqueo, el comportamiento fraudulento cae de forma abrupta. Por tanto, antes de imponer costosos desarrollos tecnológicos, resulta más eficiente y efectivo consolidar y ampliar la capacidad de bloqueo preventivo, que por sí sola podría prácticamente eliminar el fenómeno.

b. Frente a las medidas móviles:

Si se impone como obligación regulatoria el bloqueo de llamadas internacionales enmascaradas, y que no cumplan con los requisitos técnicos y regulatorios de la numeración en Colombia, con consecuencias para los PRSTM que no cumplan con estas medidas, se puede controlar la problemática. En este sentido, esta medida no implica altas inversiones para los PRSTM, y tampoco altos tiempos en su implementación puede ser la solución al problema.

En este sentido, solicitamos a la CRC enfocar su esfuerzo a estas alternativas, evaluar su resultado, y ahí si pensar si es necesario implementar medidas como **STIR/SHAKEN/RCD**, las cuales son altamente costosas.

Medidas como las propuestas generan los siguientes retos:

Técnicos: Integración y coordinación de sistemas de los PRST, agregadores, Carrier y operadores internacionales y entes de control, estandarización de datos y seguridad de la información.

Operativos y financieros: Capacidad de atención y respuesta tanto de recursos humanos, de infraestructura y financieros. En un sector tan decaído, imponer medidas que generen un impacto económico tan fuerte como el propuesto, pone en riesgo la prestación del servicio.

Regulatorios: Definición clara de obligaciones para los involucrados en la cadena de valor.



Tiempos de implementación: las medidas propuestas implican altísimos tiempos en su implementación, poniendo en riesgo la efectividad de las mismas, pues como es sabido, el fraude se perfecciona, cambia, muta con rapidez, pudiendo hacer ver tardía e innecesaria la solución.

PREGUNTA CRC: *¿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 COMCEL: La implementación de mecanismos de evaluación periódica por parte de la CRC ofrece ventajas importantes, siempre que dichas evaluaciones se orienten primero a determinar la necesidad real de nuevas medidas regulatorias. Entre las principales ventajas se destaca la posibilidad de contar con evidencia actualizada sobre la evolución del fraude, identificar tendencias emergentes y ajustar oportunamente los instrumentos existentes sin incurrir en cargas regulatorias innecesarias. También permite mejorar la coordinación interinstitucional y reforzar medidas que ya han mostrado resultados, como la suspensión provisional de códigos cortos, cuya aplicación redujo el fraude por SMS en más del 70–90%, demostrando que herramientas ágiles y focalizadas pueden ser altamente efectivas.

Sin embargo, existen desventajas y retos que deben ser considerados. En primer lugar, una evaluación periódica mal diseñada podría derivar en presión para introducir medidas tecnológicas costosas sin evidencia suficiente, generando cargas desproporcionadas para PRST, PCA e IT, especialmente en un servicio cuyo cargo de acceso es extremadamente bajo y no soporta inversiones de alto costo.

También existe el riesgo de que evaluaciones frecuentes sin metodologías claras generen incertidumbre regulatoria y cambios constantes en los requisitos operativos. Uno de los retos más relevantes es asegurar que la evaluación no se limite a describir el fenómeno, sino que determine si persiste un problema residual que justifique nuevas intervenciones regulatorias, especialmente cuando las medidas recientes ya han demostrado un impacto extraordinariamente positivo.

En cuanto a oportunidades, un sistema de evaluación bien estructurado permitiría consolidar las medidas que ya están funcionando —como la suspensión provisional y el eventual bloqueo de mensajes presuntamente fraudulentos identificados por herramientas tecnológicas— que, de adoptarse plenamente, podrían reducir el fraude por SMS casi en su totalidad.

PREGUNTA CRC: *¿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 COMCEL: Como gran acierto consideramos la implementación de la suspensión provisional de los códigos cortos cuando se este adelantado investigación administrativa por indebido uso. De la misma manera, se considera acertado que se permita el bloqueo del envío de códigos cortos cuando se evidencie que los mismos tienen contenido presuntamente fraudulentos.

Frente a servicios móviles consideramos como acierto la obligatoriedad de bloquear llamadas cuando el numero entrante este enmascarado.

Las demás medidas, adicional a no contar con un ANI, imponen cargas onerosas a los PRSTM, situación que debe analizarse de cara a los bajos valores establecidos en la regulación por cargos de acceso.

Encontramos ausente un análisis que permita la terminación de contratos con PCA/IT reincidentes, una obligación en cabeza de la CRC de realizar campañas educativas a los usuarios, un análisis frente a la metodología utilizada por la CRC para evaluar a los solicitantes de códigos cortos, y con ello prevenir el mal uso de los mismos, un análisis sobre los costos que le implicaría a los PRSTM implementar dichas medidas, sobre todo, teniendo en cuenta los bajos montos establecidos por cargos de acceso.

PREGUNTA CRC: - *¿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 COMCEL: Como primera medida, se debe evaluar el número de casos escalados a los PCA, de la misma manera, se debe tener en cuenta el número de recursos de numeración recuperados por la CRC por indebido uso.

Finalmente, se debe tener en cuenta el tiempo promedio de respuesta ante incidentes por parte de la CRC.

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)

REGUNTA CRC: *¿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 COMCEL: Los retos que a continuación se presentan, vuelven la medida innecesaria.



Retos:

- Costos y complejidad operativa. Máxime cuando hay medidas que se están implementando por la CRC que han dado resultado en la disminución de casos de fraude vía SMS. (suspensión provisional del código corto)
- Agregadores pequeños pueden enfrentar dificultades para cumplir con procesos robustos de verificación, haciendo incumplible la normatividad.
- Protección de datos personales.
- Evasión mediante intermediarios.
- Riesgo de que actores fraudulentos utilicen terceros para eludir controles.
- Necesidad de criterios uniformes entre operadores, PCA e integradores para evitar brechas.
- Tiempo de implementación

Sobre criterios mínimos indispensables para que el KYC sea efectivo y no excluyente, es importante indicar que empresas como COMCEL, anualmente hacen evaluaciones de sus clientes desde el punto de vista jurídico, financiero y otros. Estas evaluaciones en muchos puntos resultan negativos; sin embargo, la regulación obliga a mantener las relaciones de acceso con estos PCA. En virtud de lo anterior, una medida como la propuesta solo tendría cabida si se permite ante evaluaciones negativas terminar contratos de acceso.

PREGUNTA CRC: *Teniendo en cuenta que los agregadores pueden actuar tanto en acuerdos directos (normalmente clientes nacionales como bancos, comercios, entidades de salud o aerolíneas, etc), 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 entre estos dos tipos de tráfico en cuanto al establecimiento de medidas regulatorias para 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 COMCEL: Consideramos que es pertinente establecer medidas diferenciadas entre acuerdos directos e internacionales, porque los riesgos y la capacidad de control varían:

Para tráfico nacional:

- Trazabilidad: exigir que cada intermediario revele el origen real del mensaje o llamada.
- Monitoreo: usar alertas por volúmenes anormales y patrones sospechosos.
- Validación: implementar procesos de registro y verificación para los originadores antes de permitir el envío.
- Cooperación: Una vez realizada denuncia por estos hechos, es necesario que la CRC actúe con rapidez, para evitar que la situación se siga presentando.



Para el tráfico internacional se recomienda exigir validación del originador por parte del primer agregador que entrega tráfico al país, trazabilidad obligatoria de toda la cadena y monitoreo reforzado de patrones. Adicionalmente, que se imponga la medida obligatoria a todos los PRSTM de bloquear tráfico con numeración enmascarada.

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

RESPUESTA COMCEL: No consideramos acertada la propuesta, sin analizar primero si la medida de la suspensión provisional, mientras realiza la actuación administrativa de recuperación del código corto por indebido uso, sumada a otras como permitir el bloqueo de parte de los PRSTM que haciendo uso de herramientas tecnológicas evidencien el envío de SMS con contenido fraudulento, y la terminación de los contratos con PCA/IT (como última alternativa), dan solución a la problemática planteada.

Una vez se evidencie el resultado de la aplicación de estas alternativas, si consideramos necesario analizar si se requiere algún cambio adicional regulatorio.

La regulación debe aplicarse de manera proporcional y únicamente cuando sea necesaria para corregir fallas del mercado, proteger a los usuarios o garantizar condiciones de competencia justa. Una intervención regulatoria excesiva o innecesaria puede generar cargas adicionales a los agentes, distorsionar el funcionamiento del mercado y limitar la innovación, por lo que es fundamental que las medidas se adopten solo cuando exista una justificación clara y un beneficio evidente frente a los costos que implican.

PREGUNTA CRC: *¿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 COMCEL: Como se indicó en el capítulo 3 de este documento, la propuesta presentada es innecesaria. Adicionalmente, esta propuesta trae múltiples desafíos, haciendo que su implementación sea costosa y demorada en el tiempo. En un sector en el cual los delitos se perfeccionan y cambian rápidamente, pensar en medidas que son de tan largo plazo, y costosas, no son garantía de éxito, y si pueden generar una gran carga.

Desafíos técnicos:

- Validar alto volumen de campañas en tiempo real sin afectar la entrega de tráfico.
- Integración con múltiples operadores, agregadores y plataformas internacionales.
- Seguridad y protección de datos.
- Neutralidad tecnológica.



Desafíos económicos:

- Costos de infraestructura
- Implementación y mantenimiento de una plataforma nacional robusta.
- Impacto en actores pequeños
- Riesgo de exclusión si los costos se trasladan a agregadores con menor capacidad.

Desafíos operativos

- Gestión de alto volumen
- Validación simultánea de campañas en picos de tráfico.
- Evitar demoras que afecten la experiencia del usuario final.
- Necesidad de entrenar equipos y garantizar atención 24/7.

Desafíos de gobernanza

- Administración de la plataforma centralizada (CRC, un tercero neutral, o un consorcio)
- Evitar arbitrariedad en aprobaciones o bloqueos.
- Mecanismos claros para supervisión y control por parte de la CRC

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: 1) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, 2) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, 3) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: - *¿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 COMCEL: Como se indicó en los comentarios presentados en el capítulo 3 de este documento, esta propuesta es inviable, presenta múltiples desafíos, haciendo que su implementación sea costosa y demorada en el tiempo. En un sector en el cual los delitos se perfeccionan y cambian



rápidamente, pensar en medidas que son de tan largo plazo, y costosas, no son garantía de éxito, y si pueden generar una gran carga. A su vez, es difícil alinear los criterios entre los diferentes actores, creando vacíos en las responsabilidades de cada parte en el proceso.

Desafíos técnicos:

- Validación de alto volumen de campañas sin afectar el tráfico A2P.
- Integración entre diferentes operadores, agregadores y plataformas internacionales.
- Garantizar seguridad y privacidad del cliente.

Desafíos económicos

- Costos de implementación
- Mantenimiento y actualización, requiere inversión continua en tecnología y capacitación.
- Baja remuneración por envío de SMS. (Cargo de Acceso)

Desafíos operativos

- Definir quién administra la plataforma, cómo se incorporan nuevos actores y cómo se resuelven disputas.
- Evitar demoras en el envío de campañas mientras se hacen las validaciones.

Desafíos de gobernanza

- Establecer roles y responsabilidades precisas
- Mecanismos eficientes para garantizar la seguridad y los protocolos adecuados
- Elementos para asegurar interoperabilidad y confianza
- Políticas de acceso y permisos claras
- Que existan certificaciones digitales para garantizar la autenticidad del que envía

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la



problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿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 COMCEL: Como se indicó anteriormente, la propuesta planteada, presenta múltiples desafíos, haciendo que su implementación sea costosa, demorada en el tiempo e innecesaria. En un sector en el cual los delitos se perfeccionan y cambian rápidamente, pensar en medidas que son de tan largo plazo, y costosas, no son garantía de éxito, y si pueden generar una gran carga.

Es importante indicar que en caso tal de que un mensaje contenga URL, es el dueño del contenido del mensaje el que debe garantizar lo siguiente:

- Verificación en tiempo real
- Comprobar que el dominio existe y no está en listas negras.
- Confirmar que la conexión es segura y el certificado no está caducado ni emitido por una autoridad sospechosa.
- Verificar la reputación del dominio, contrastarlo con listas de sitios maliciosos, detectar patrones de engaño (acortadores o redirecciones sospechosas) y validar la seguridad del sitio. Además, debe integrarse fácilmente con los sistemas de los PRST y operar con tiempos de respuesta adecuados.
- Debería tener una confirmación del dueño de la Marca del portal (URL) que se envía

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿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 COMCEL: Si el proceso previo a el envío de los mensajes se realiza correctamente, y sus remitentes cumplieran con los postulados regulatorios existentes, no debería tener afectación a los mensajes legítimos. No obstante, el bloqueo o marcado de mensajes sin identificadores validados puede generar impactos positivos como negativos.

Positivos:

- Mayor protección al usuario
- Reducción de campañas fraudulentas y fortalecimiento de la trazabilidad del tráfico A2P.

Efectos negativos:

- Bloqueo de mensajes legítimos por errores de validación o fallas en el registro de originadores.

PREGUNTA CRC: *¿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 tipos de contenido distinta a la propuesta?*

RESPUESTA COMCEL: Una medida como la propuesta, genera altas cargas y costos operativos. Asimismo, se podría afectar la experiencia del usuario, si se etiqueta incorrectamente mensajes legítimos, y en consecuencia se bloquea una campaña legítima (ej. implo: Salud, bancos, desastres naturales etc.)

Una clasificación adicional solo sería pertinente si mejora la diferenciación entre mensajes transaccionales, informativos y promocionales sin generar complejidad innecesaria.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.



PREGUNTA 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 COMCEL: El sistema de monitoreo de los agregadores debería contar, como mínimo, con capacidad para analizar volúmenes y frecuencias de envío, identificar variaciones atípicas, detectar remitentes irregulares y validar coincidencias con listas de riesgo.

PREGUNTA CRC: - *¿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: Si bien es cierto los usuarios normalmente no revisan bien el origen del mensaje, (lo que le daría baja eficacia a la propuesta) el hecho de que se asigne un código exclusivo a cada marca permite identificar plenamente al remitente de la información, y señalarlo, cuando la misma es fraudulenta.

Facilita la identificación del remitente y aumenta la confianza del usuario al recibir comunicaciones claramente asociadas a una entidad legítima.

PREGUNTA CRC: *¿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 COMCEL: No obstante ser una medida que puede tener una baja efectividad, podría mejorar la transparencia y la trazabilidad del origen, y la percepción de seguridad en el canal A2P. Es necesario hacer una evaluación de impacto normativo para validar si es viable.

Finalmente, debe quedar claramente establecido en la regulación, que el encargado de cumplir con este requerimiento es el PCA/IT, quien es el dueño del código, y es el que conoce el contenido del mensaje que va a remitir.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la



problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿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 en el que los usuarios puedan identificar a todos los originadores de contenidos de manera clara?*

RESPUESTA COMCEL: Como se ha indicado a lo largo de este documento, hay otras medidas que son de más bajo costo en su implementación que pueden lograr mejores resultados frente a la problemática.

No obstante ser una medida que puede tener una baja efectividad, podría mejorar la transparencia y la trazabilidad del origen, y la percepción de seguridad en el canal A2P. Es necesario hacer una evaluación de impacto normativo para validar si es viable.

Finalmente, debe quedar claramente establecido en la regulación, que el encargado de cumplir con este requerimiento es el PCA/IT, quien es el dueño del código, y es el que conoce el contenido del mensaje que va a remitir.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

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

RESPUESTA COMCEL: Criterios relevantes para determinar patrones atípicos:

- Volumen inusual por unidad de tiempo
- Número de mensajes enviados por línea en intervalos cortos
- Distribución geográfica anómala



- Envíos masivos a destinos internacionales no habituales para el usuario o desde destinos internacionales en caso de entrantes.
- Alto número de destinatarios únicos en un periodo breve.
- Horarios no convencionales
- Picos de envío en horas atípicas

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

RESPUESTA COMCEL: Como se indicó en el capítulo 3 del presente documento, esta medida resulta técnicamente y jurídicamente desproporcionada. En particular, la medida contraviene el principio de neutralidad tecnológica, al obligar a los proveedores a adoptar configuraciones específicas de red y de control de tráfico que no responden a la arquitectura ni a la evolución natural de sus plataformas, limitando la libertad para gestionar sus redes de manera eficiente. Asimismo, vulnera el principio de intervención mínima y regulación eficiente, dado que introduce una restricción generalizada que impacta a todos los usuarios, incluidos aquellos con usos legítimos, sin demostrar que sea el mecanismo menos intrusivo ni el más eficaz para mitigar el fraude. Adicionalmente, afecta el principio de protección de los derechos de los usuarios, al deteriorar la experiencia del servicio contratado bajo esquemas comerciales ilimitados, generando bloqueos automáticos no asociados a fallas del usuario sino a una restricción regulatoria exógena. Finalmente, la medida desconoce el principio de promoción de la inversión y la innovación, al exigir desarrollos técnicos complejos y costosos en los sistemas de red y facturación, desviando recursos que podrían destinarse a soluciones más focalizadas y efectivas contra el fraude, en contravía del objetivo de eficiencia y sostenibilidad del sector TIC previsto en la Ley 1341.

PREGUNTA CRC: - *¿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 COMCEL: La validación en tiempo real referente al contenido del mensaje. Al respecto, se propone como procedimiento a aplicar, que cuando un sistema tecnológico evidencie un posible mensaje fraudulento, solicite la validación del mismo con su remitente, y ponga en copia a la CRC, con el fin de que esta esta alerta a la respuesta del PCA o IT. En caso de que no se presente una respuesta oportuna, dentro de las dos (2) horas siguientes a la validación de la veracidad del contenido) se sugiere que se permita el bloqueo del mismo, y que la CRC inicie actuación administrativa de recuperación del código, con la orden de suspensión provisional del mismo.

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



PREGUNTA CRC: *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 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 COMCEL:

Respecto al tráfico internacional entrante por medio de intermediarios (Carriers) vs clientes nacionales, no existe una norma clara que obligue a la utilización del plan de numeración establecido, lo que da vía libre a manipulación de CLI el cual hoy en día es usado para campañas realizadas por call center y pesquisas con fines fraudulentos.

Como medida se debe primero regulatoriamente establecer el cumplimiento del plan de numeración nacional e internacional para llamadas que ingresen desde el exterior, esto tanto para llamadas que ingresen con country code 57, así como las que vienen con otro CLI de otro país pero que son llamadas con fines fraudulentos.

Y como consecuencia, se debe determinar la obligatoriedad de bloquear de manera inmediata las rutas que incumplen autenticación o trazabilidad.

Frente al tráfico nacional, en términos generales, éste tráfico es fácilmente identificado y puede ser trazado. Así las cosas, la gran problemática la vemos en el tráfico internacional, donde pueden originar tráfico con cualquier número origen y no se tiene forma de trazar o identificar el originador de las llamadas.

PREGUNTA CRC: *¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?*

RESPUESTA COMCEL: Tenemos implementadas herramienta de control con configuraciones específicas, para así mismo proceder con las validaciones con los PCA o IT de los mensajes enviados.

En cuanto a los retos está el cambio constante del número originador que hace el fraude lo que hace que la efectividad no sea del 100%



PREGUNTA CRC: *¿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?*

RESPUESTA COMCEL: Con una medida como la propuesta, se reduciría del fraude por phishing y reclamaciones por wangiri¹, por uso de números en uso por parte de usuarios o por recepción de llamadas para campañas fuera de los horarios establecidos, así mismo se mejoraría en la confianza del usuario en el momento de responder sus llamadas si decide hacerlo.

PREGUNTA CRC: *¿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 COMCEL: En la práctica, la evidencia operativa demuestra que las etiquetas o advertencias en el dispositivo (“No verificada” o “Probable fraude”) tienen una efectividad limitada, ya que los usuarios tienden a ignorar este tipo de alertas o no comprenden su alcance, por lo que el comportamiento fraudulento persiste.

Adicionalmente, desde el punto de vista técnico, no es posible identificar de manera confiable el origen del tráfico para diferenciar llamadas internacionales con CLI nacional, tráfico de clientes en roaming o tráfico cursado desde redes de otros operadores, lo que genera un alto riesgo de falsos positivos y etiquetados erróneos. Esto afecta directamente la experiencia del usuario, quien continuará recibiendo las llamadas no deseadas —ahora acompañadas de alertas confusas— incrementando la molestia y las reclamaciones, sin una reducción real del fraude.

En este contexto, la medida carece de una evaluación de impacto normativo que demuestre su proporcionalidad y eficacia, y puede derivar en una carga regulatoria innecesaria, con impactos negativos sobre la calidad del servicio y la confianza del usuario, sin cumplir de manera efectiva el objetivo de protección frente a la suplantación.

Retos e impactos:

¹ Wangiri: es una estafa telefónica donde delincuentes hacen [llamadas perdidas](#) (un “timbre y corte”) desde números internacionales caros para engañar a la víctima y que devuelva la llamada, generando altos cargos por minuto. Los estafadores ganan comisiones por mantenerse en la línea, usando técnicas como mensajes pregrabados o desvíos a [números premium](#). Para protegerte, **no devuelvas llamadas desconocidas**, investiga números sospechosos y **reporta** estos incidentes a tu operador y autoridades.



- Interoperabilidad tecnológica: Requiere adaptar sistemas SIP/SS7 y equipos de usuario para soportar etiquetas diferenciales.
- Coordinación entre operadores: Unificación de criterios de “falsos positivos” y actualización de estándares.
- Experiencia del usuario: El etiquetado debe ser claro, evitar alarmar sin razón o saturar la interfaz.
- Evitar bloquear llamadas legítimas de empresas internacionales, aliados o servicios críticos.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿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 COMCEL: Como se indicó anteriormente, no vemos viable en este momento la implementación de STIR/SHAKEN por las siguientes razones:

- Requiere una Inter operatividad muy compleja entre operadores que originen tráfico a Colombia carriers internacionales, operadores de LDI y operadores nacionales, la exigencia de estas condiciones puede afectar significativamente la facilidad de acceso de las comunicaciones a el país.
- El costo de implementación y licenciamiento es alto para todos los operadores y carriers que intervienen en la comunicación.
- Requiere una operación compleja, dado que necesita mantenimiento y soporte para escalamientos de listas de excepciones y/o desbloques.



- Las demoras en la implementación, y los rápidos cambios en la forma de los fraudes, podría volver desactualizada la implementación con las nuevas metodologías de fraude.

Con un marco regulatorio que exija el cumplimiento de las normas internacionales referentes a la numeración internacional, es suficiente para que los operadores de LDI, pueden trasladar estas exigencias a los carriers internacionales y puedan tomar acciones de control al detectar patrones anómalos de tráfico internacional.

Como lo mencionamos en a lo largo de este documento, no vemos viable la implementación de STIR/SHAKEN otras alternativas mucho más simples puede disminuir significativamente la problemática.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y filtrado 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 COMCEL: Normalmente los modelos de monitoreo y filtrado tienen igual un muy pequeño rango de falsos positivos; sin embargo estos casos si se gestionan correctamente no debieran afectar de manera significativa a los clientes.

PREGUNTA CRC: *¿Qué actores deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas? ¿Qué mecanismos de gobernanza y protección de datos serían necesarios?*

RESPUESTA COMCEL:

Actores clave:



- Operadores fijos y móviles, CRC, CSIRT nacional.
- Proveedores de soluciones antifraude.
- Empresas con alto volumen de llamadas y proveedores de contenido
- Carriers internacionales

PREGUNTA CRC: *¿Cuáles considera que serían los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado vs un modelo distribuido? ¿Qué mecanismos considera deben ser adoptados y estandarizados para validar la veracidad de una alerta antes de su distribución mediante la plataforma de intercambio?*

RESPUESTA COMCEL: Como se ha indicado a lo largo de este escrito, consideramos que hay medidas más eficaces que la implementación de una plataforma centraliza. Una medida como la propuesta genera altos costos operativos y administrativos.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *¿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 COMCEL: Como se dijo a lo largo de este escrito, estas medidas no generan el impacto esperado, pues el usuario no conoce los rangos de numeración.

Desafíos en su implementación:

- Reservar rangos solo para usos comerciales podría reducir la disponibilidad general de números y requerir una relimitación del plan de numeración.



- Costos. Los operadores, plataformas y usuarios necesitarían ajustar sistemas y procesos para incorporar estos rangos, incluyendo actualizaciones de señalización y registros gubernamentales.
- Necesidad de normativas y controles claros y protocolos de penalización por incumplimiento.
- Riesgo de estafas desde rangos autorizados

A título de conclusión, no se ve una ventaja significativa.

PREGUNTA CRC: *¿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 transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?*

RESPUESTA COMCEL: Como se indicó a lo largo de este escrito, el PCA o IT debería ser el responsable de identificar con el etiquetado cada uno de los mensajes enviados, pues es el que conoce el contenido de cada SMS.

PREGUNTA CRC: *¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?*

RESPUESTA COMCEL: Actualmente ingresa tráfico con millones de números origen diferentes diarios con un perfil de posible fraude, no creemos que un control centralizado sea eficiente, cada operador de LDI, podría tomar sus acciones localmente.

PREGUNTA CRC: - *¿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 COMCEL: Ventajas

- Reducción significativa de fraudes y suplantaciones
- Cada proveedor puede ajustar su lista según su tráfico y contexto, bloqueando números inbound-only o no asignados usados para suplantación.
- Mayor flexibilidad operacional
- Se permite personalización basada en perfiles de tráfico y requisitos locales, sin depender de un único registro central.



No obstante lo anterior, se reitera que los operadores de LDI como dueños del tráfico, deberían tener localmente su propia lista, los operadores de telefonía móvil/fija podrían apoyar reportando casos que se identifiquen.

Frente a las temáticas enfocadas en la educación de la ciudadanía

PREGUNTA CRC: - *¿Qué acciones voluntarias (no regulatorias) adelanta actualmente su organización o conoce usted en el mercado para informar a los usuarios sobre riesgos de fraude? ¿Son efectivas? ¿Tienen métricas de impacto?*

RESPUESTA COMCEL: Se realiza monitoreo y bloqueo de llamadas de forma automática, basado en diferentes comportamientos como:

- Llamadas de corta duración
- Alto volumen de llamadas desde un mismo número A
- Llamadas internacionales con número A usando el country Code de Colombia +57, este bloqueo es parcial para casos de numeración móvil por la afectación que se pueda presentar para usuarios de roaming.
- Para llamadas entrantes internacionales con numeración fija Colombiana está bloqueado al 100%.
- En mensajería existen controles y bloqueos por volúmenes
- Desde el área de fraude y el área de comunicaciones de la compañía se realizan actividades tipo campañas por diferentes canales (Web, mensajería, redes sociales etc.), informando a los usuarios sobre el fraude cibernético.

PREGUNTA CRC: *¿Qué cargas técnicas y económicas representaría para los PRST, los IT y los PCA implementar obligaciones de divulgación pedagógica frente al fraude cibernético?*

RESPUESTA COMCEL: Se presentarían múltiples cargas, tales como la creación de las campañas, ya sean vía SMS o por otros medios, el valor de la transmisión de la misma, más la implementación de los reportes de campañas que la CRC plantea imponer, crear y actualizar contenidos, habilitar canales informativos (web, apps, IVR, SMS) y ajustar sistemas y procesos internos. También requieren recursos humanos para gestión y reporte. Aunque generan una carga moderada, contribuyen a reducir incidentes y fortalecer la confianza del usuario.

En virtud de lo anterior, solicitamos a la CRC que antes de implementar una medida como la propuesta: (i) evalúe formalmente la efectividad de la suspensión provisional y determina si existe un problema residual, (ii) fortalezca procesos de recuperación ágiles, reglas claras de reincidencia y mayor articulación sectorial, (iii) realice un AIN a la propuesta realizada, pues solo si el AIN demuestra que persiste un nivel de fraude que no puede ser contenido con las herramientas ya vigentes tendría



sentido definir fases de implementación para nuevos desarrollos técnicos. Esto garantiza una política pública eficiente, proporcional y basada en evidencia.

En virtud de todos los retos presentados, y del tiempo que una medida como la propuesta requiere para su implementación, consideramos que no es una medida viable para la solución de la problemática, máxime cuando el problema en gran medida se solucionó con la suspensión provisional por parte de la CRC cuando se inicia una actuación administrativa.

PREGUNTA CRC: *Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Qué tipo de contenidos deberían ser obligatorios? (ejemplos reales, guías de prevención, alertas recientes, recomendaciones prácticas, etc.)*

RESPUESTA COMCEL: Consideramos que esta obligación debe estar en cabeza de la CRC y de otras instituciones del estado. Es necesario recordar que el código corto es asignado por la CRC. En este sentido, debe tener un mínimo de diligencia frente al asignatario de la misma.

PREGUNTA CRC: *Frente a la alternativa de divulgación pedagógica por parte de PRST, PCA e IT ¿Cuál considera es el canal más apropiado para esta divulgación? (ejemplo: SMS masivos, mensajes en facturas, Landing pages, Push notifications en apps, etc.)*

RESPUESTA COMCEL: Consideramos que esta obligación debe estar en cabeza de la CRC y de otras instituciones del Estado. Es necesario recordar que el código corto es asignado por la CRC. En este sentido, debe tener un mínimo de diligencia frente al asignatario de la misma. Por tal razón, el medio debería ser definido por la CRC, pero se recomienda: información en su página web, y propagandas en canales abiertos.

PREGUNTA CRC: *Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué nivel de detalle debería tener la información publicada para ser útil sin generar nuevas vulnerabilidades? (ejemplo: números reportados, patrones o modus operandi, ejemplos de mensajes fraudulentos, etc.)*

RESPUESTA COMCEL: Consideramos inútil esta medida. El Usuario no conoce de estas medidas, y no revisa dicha información, y por el contrario, si se cargaría de manera adicional al PRSTM con dichas medidas. Adicionalmente, se generan los siguientes retos:

- Desarrollo y mantenimiento del portal.
- Integración con sistemas internos.
- Actualización periódica de datos y seguridad para evitar vulnerabilidades.
- Costos de infraestructura tecnológica.
- Contratación de personal para administración y soporte.



- Gastos asociados a campañas de divulgación.

PREGUNTA CRC: *Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, ¿Qué beneficios concretos considera que traería este portal para los usuarios y agentes del sector?*

RESPUESTA COMCEL: Como se indicó anteriormente, NINGUNO.

PREGUNTA CRC: *Frente a la alternativa de la implementación de un Portal con las campañas más denunciadas, en caso de que aplique, ¿qué cargas técnicas y económicas representaría para su organización implementar estas obligaciones?*

RESPUESTA COMCEL: Como se indicó anteriormente:

- Desarrollo y mantenimiento del portal.
- Integración con sistemas internos.
- Actualización periódica de datos y seguridad para evitar vulnerabilidades.
- Costos de infraestructura tecnológica.
- Contratación de personal para administración y soporte.
- Gastos asociados a campañas de divulgación.

PREGUNTA CRC: *¿Considera viable técnica y operativamente crear un sistema de trazabilidad centralizado de PQR relacionadas con fraude por mensajes de texto o llamadas? Justifique su respuesta.*

RESPUESTA COMCEL: No. esto solo cargaría más a los PRSTM quienes son los que reciben las PQR de sus usuarios. Lo que se debe implementar es una solicitud de verificación de veracidad de la información contenida en el SMS cuando el PRSTM evidencie de la existencia de un mensaje con contenido presuntamente fraudulento, con copia a la CRC, y con la exigencia de repuesta de manera oportuna (máximo dentro de las dos horas siguientes a su envío). Si el PCA no valida dicho contenido, el PRSTM puede bloquear el envío de los mensajes, y la CRC puede iniciar de oficio una investigación administrativa.

PREGUNTA CRC: *¿Qué variables o campos considera debería contener este sistema de trazabilidad para permitir análisis útiles?*

RESPUESTA COMCEL: Como se indicó anteriormente, no es viable.

PREGUNTA CRC: *¿Qué riesgos de seguridad o privacidad considera deben ser tenidos en cuenta al centralizar la información de PQR relacionadas con fraude?*



RESPUESTA COMCEL: Como se indicó a lo largo de este escrito, la propuesta no es viable, evidenciando múltiples riesgos como:

- Exposición de datos personales por ser PQR centralizadas de varios actores.
- Acceso no autorizado al sistema y robo de información.
- Al centralizar se puede vulnerar los sistemas de los involucrados.
- Debe alinearse con leyes de protección de datos.

PREGUNTA CRC: *¿Qué componentes debería incluir estrategia educativa conjunta entre la CRC, los agentes regulados y otras entidades competentes? (por ejemplo: campañas nacionales, identificación de patrones emergentes, material didáctico para usuarios, indicadores de éxito, etc.)*

RESPUESTA COMCEL: LA CRC debe implementar Campañas nacionales masivas de la siguiente manera:

- Difusión en medios tradicionales y digitales para alertar sobre fraudes.
- Informes periódicos sobre nuevas modalidades de fraude y su afectación en el usuario.
- Material didáctico para usuarios de todas las edades mediante guías prácticas, videos, infografías y simulaciones.
- Capacitación a los actores involucrados, creación de protocolos para atención y prevención.
- Colaboración entre los actores para unificar los tipos de estrategias educativas y que el usuario pueda entender.
- Desarrollo de canales interactivos, portal web, redes sociales y apps para alertas y denuncias.

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

PREGUNTA CRC: *A partir de las temáticas identificadas en el presente documento, y en el marco del proceso de revisión del Régimen de Administración de Recursos de Identificación bajo un enfoque de simplificación regulatoria, resulta pertinente evaluar la pertinencia de ajustes adicionales. En este sentido, se plantean las siguientes preguntas orientadoras:*

Reincidencia en el uso indebido de recursos de identificación para el envío de SMS.

PREGUNTA CRC: *Desde la perspectiva de prevención de contactos fraudulentos a los usuarios, ¿qué elementos del régimen de administración de recursos de identificación para el envío de SMS deberían ser revisados o simplificados para prevenir su uso indebido? Explique detalladamente las razones que justifican dicha revisión.*

RESPUESTA COMCEL: Mecanismos de suspensión preventiva ante indicios de fraude, terminación de contratos por reincidencia, mayor diligencia y la validación de los asignatarios de la numeración.



PREGUNTA CRC: *En relación con la detección de uso indebido del recurso de identificación, ¿qué criterios adicionales a los expuestos considera necesarios para determinar que un asignatario está haciendo un uso indebido del recurso de identificación? Describa y fundamente cada criterio propuesto.*

RESPUESTA COMCEL: Además de los criterios ya previstos, podrían considerarse como indicadores de uso indebido del recurso de identificación como:

- Recurrencia de patrones de tráfico atípicos (altas tasas de envío, horarios inusuales o remitentes no declarados), que sugieren intención de ocultar campañas irregulares;
- Incumplimiento reiterado de solicitudes de información o de requerimientos de trazabilidad, que afecta la capacidad de supervisión y utilización del código por terceros no autorizados, lo que demuestra falta de controles internos del asignatario.
- Concentración de mensajes hacia rangos internacionales inusuales o números aleatorios y así evitar smishing.

PREGUNTA CRC: *Respecto a las medidas correctivas, ¿qué restricciones adicionales a las previstas actualmente, considera pertinente aplicar a los asignatarios que incurren en uso indebido del recurso de identificación para SMS? Explique en detalle las razones de cada restricción sugerida.*

RESPUESTA COMCEL: Como primera medida, es importante indicar que el encargado de asignar la numeración corta es la CRC. En este sentido, la CRC debe hacer una evaluación exhaustiva de los solicitantes de la numeración, en donde constate las calidades, condiciones, y demás requisitos que permitan dar tranquilidad del uso que se va a dar al potencial asignatario de la numeración, y no trasladar con posterioridad el problema a los PRSTM quienes se ven obligados a implementar medidas tecnológicas para evitar el envío de mensajes con contenido fraudulento.

En este sentido, y solo a título de reflexión, si es la CRC la asignataria de los códigos cortos, y con posterioridad evidencia el mal uso que se le da a los mismos por parte de PCA/IT, de manera reiterada, porque no permite la terminación de los acuerdos de acceso con los infractores reincidentes?, es importante reiterar que, si desde el inicio se asigna bien un código corto, este problema no se presenta.

En virtud a lo anterior, la principal restricción opera cuando la CRC no permite la terminación de los contratos o acuerdos de acceso por esta causal.

PREGUNTA CRC: *Con base en su experiencia, ¿cuáles de las medidas actualmente contempladas en la regulación sobre la recuperación de códigos cortos considera efectivas y cuáles no? Por favor sustente su respuesta indicando, cuando sea posible, ejemplos o casos que respalden su argumento.*

RESPUESTA COMCEL:



Falta de criterios claros para reincidencia, en este momento no hay sanciones progresivas, lo que permite que actores reincidan sin consecuencias significativas, y las empresas reincidentes siguen accediendo a nuevos códigos.

Con el incremento de fraudes que se vienen generando la CRC debe buscar mecanismos para dar trámite y respuesta en tiempos más cortos que eviten generar una mayor cantidad de fraudes a los usuarios, Mantener la plataforma del SIGRI y la publicación de Resoluciones actualizada con el fin de poder realizar consultas y validaciones de los recursos asignados y recuperados por la CRC

Cesión o transferencia de recursos

PREGUNTA CRC: *En relación con la cesión o transferencia de recursos de identificación, ¿considera que deberían mantenerse las condiciones iniciales de asignación cuando un recurso de identificación sea cedido o transferido? Por favor, explique las razones que fundamentan su respuesta.*

RESPUESTA COMCEL: como se indicó en el capítulo 3 del presente documento, La posibilidad de transferir o ceder recursos de identificación, tal como la propone la CRC, no resulta adecuada en la medida en que termina desvirtuando el objetivo regulatorio de corregir conductas indebidas asociadas al uso de códigos cortos. Permitir la cesión abre la puerta a que los PCA o IT que hayan perdido dichos recursos como consecuencia de incumplimientos o malas prácticas los recuperen indirectamente a través de otros PCA, manteniendo en la práctica la misma capacidad operativa que se pretendía restringir. Esto no solo debilita el efecto disuasivo de la medida, sino que además perpetúa una ventaja injustificada para estos actores frente a quienes sí cumplen las reglas, afectando la equidad competitiva y reduciendo la efectividad de los mecanismos de control y sanción definidos por el regulador.

PREGUNTA CRC: *Para autorizar la cesión de un código corto, ¿qué tipo de documentación, validación previa o requisitos formales adicionales deberían exigirse a la persona jurídica que recibirá el código corto? Detalle y explique cada elemento propuesto.*

RESPUESTA COMCEL: Como se indicó en la respuesta anterior, no consideramos pertinente la cesión de códigos cortos.

PREGUNTA CRC: *Con base en su experiencia, ¿considera que para códigos cortos debería prohibirse la cesión de estos recursos? ¿Qué aspectos considera que la regulación debe priorizar para mitigar estos riesgos? Justifique su respuesta.*

Sí, debería prohibirse la cesión de códigos cortos. Como se ha indicado a lo largo de este escrito, la cesión aumenta el riesgo de uso indebido y dificulta la trazabilidad del responsable, lo que puede facilitar fraudes.



PREGUNTA CRC: *Respecto a la cesión o transferencia de recursos de identificación, ¿considera que la CRC debe imponer condiciones para mantener la asignación de un código corto, tal como validar el estado o vigencia de la matrícula mercantil de la razón social que solicita un código corto? Por favor, sustente su respuesta.*

RESPUESTA COMCEL: Por las razones ampliamente descritas a lo largo de este documento, consideramos que no se deben imponer condiciones para mantener la asignación del código corto, más allá del cumplimiento de su debido uso.

PREGUNTA CRC: *En relación con la suspensión preventiva del tráfico asociado a un código corto, ¿qué condiciones o supuestos deberían considerarse para habilitar la aplicación de esta medida durante el desarrollo o inicio de la actuación administrativa para la eventual recuperación del recurso? Por favor, explique su respuesta.*

Como se indicó a lo largo de este escrito, la medida adelantada por la CRC de ordenar la suspensión provisional del uso de los mismos por uso presuntamente fraudulento redujo en mas de un 70% el nivel de escalamiento a los PCA o IT por envío de mensajes con contenido fraudulento.

Así las cosas, durante el último trimestre de 2025, La CRC ha solicitado la recuperación de 17 códigos cortos, lo cual ha generado una reducción significativa de 73% en el número de casos escalados desde COMCEL diferentes PCA . Así las cosas, durante el 2024, COMCEL reporto 244 casos de mensajes con contenido presuntamente fraudulento a diferentes PCA, durante los tres primeros trimestres del 2025, reporto 378 casos, encontrándose para el último trimestre que tan solo se reportaron 27 casos, así:

Esta simple medida, que con tanta insistencia solicitaban los PRSTM, disminuyó el envío de mensajes con contenido fraudulento de manera considerable, aplicada por la CRC sin que fuera necesaria una modificación regulatoria.

De la misma manera, se encuentra ausente un análisis que determine la viabilidad de terminar los contratos existentes entre PCA y PRSTM cuando al PCA se le han recuperado de manera reiterada códigos cortos por indebido uso de la numeración al remitir mensajes con contenido presuntamente fraudulentos.

PREGUNTA CRC: *Desde su experiencia, ¿cuáles serían los principales beneficios de aplicar una suspensión preventiva del tráfico en casos de presunto uso indebido vinculados a un código corto? Explique sus razones.*

RESPUESTA COMCEL: Como se ha indicado a lo largo de este documento, son múltiples los beneficios de suspender provisionalmente el tráfico en caso de presunto indebido uso, siendo el más importante que los usuarios no van a volver a recibir mensajes con contenido presuntamente fraudulento. Así mismo, la CRC va a iniciar una actuación administrativa y va a poder recuperar el



código corto, el cual a futuro podrá ser asignado nuevamente a un PCA o IT que cumpla con los requisitos regulatorios sobre SMS.

PREGUNTA CRC: *En cuanto a los posibles impactos, ¿qué riesgos, limitaciones o efectos no deseados podrían derivarse de la aplicación de una suspensión preventiva del tráfico durante el desarrollo o inicio de la actuación administrativa? Detalle y explique los elementos que considere relevantes.*

RESPUESTA COMCEL: El usuario debe ser el enfoque de la regulación, en este sentido, se encuentra acertada la medida de la CRC de suspender provisionalmente el uso del código corto al inicio de una actuación administrativa.

49. PREGUNTA CRC: *Sobre las garantías del debido proceso, ¿qué elementos considera adicionales para establecer la medida de suspensión del tráfico durante el desarrollo o inicio de la actuación administrativa en casos de presunto uso indebido del código corto? Describa y explique los pasos que considere adecuados.*

RESPUESTA COMCEL: Como mínimo se debe contar con una notificación previa al presunto infractor sobre la medida y sus motivos.

Actualización y trazabilidad de información

PREGUNTA CRC: *Sobre la actualización de información, ¿considera que debe incluirse como causal de recuperación de los recursos asignados el incumplimiento en la actualización de los datos en las bases de la CRC, como el RPCAI, conforme al Registro Único Empresarial y Social (RUES) de la sociedad asignataria? Por favor, justifique su respuesta.*

RESPUESTA COMCEL: Como se ha advertido a lo largo de este documento la mejor medida a imponer es la suspensión provisional, sumada a la posibilidad de bloquear por identificar mensajes con contenido presuntamente fraudulentos, cuando los sistemas de alerta evidencien de un posible fraude, y la autorización de parte de la CRC de terminar contratos con PCA/IT reincidentes en la recuperación de códigos cortos por indebido uso – uso fraudulento.

PREGUNTA CRC: *¿Considera que la CRC debería incorporar una causal específica de recuperación de códigos cortos que permita suspender de manera preventiva la autorización de uso cuando el asignatario no actualice la información conforme con el Registro Único Empresarial Social (RUES)? Por favor, justifique su respuesta.*

RESPUESTA COMCEL: Si el PCA/IT asignatario de numeración no ha actualizado su RUES, si se puede impedir la asignación de nuevos códigos cortos. Esta actualización se debe evidenciar al momento de la solicitud.



PREGUNTA CRC: *¿Considera que la CRC debería establecer alguna medida regulatoria adicional en los eventos en los que exista conducta reincidente ante el uso indebido de códigos cortos? Por favor, justifique su respuesta.*

RESPUESTA COMCEL: Sí, la CRC debería permitir la terminación de los acuerdos o contratos con PCA o IT reincidentes. Como se ha indicado a lo largo de este escrito, esta medida sumada con la suspensión temporal del uso de códigos cortos en casos de reincidencia soluciona de raíz la problemática presentada.

PREGUNTA CRC: *¿Qué consecuencias regulatorias adicionales considera adecuadas en caso de que los asignatarios no actualicen su información según lo estipulado? Por favor, justifique su respuesta.*

RESPUESTA COMCEL: como se indicó en el capítulo 3, la propuesta regulatoria no da solución a la problemática planteada, y si impone una carga administrativa y operativa fuerte a los asignatarios de numeración.

Como se ha advertido a lo largo de este documento la mejor medida a imponer es la suspensión provisional, sumada a la posibilidad de bloquear por identificar mensajes con contenido presuntamente fraudulentos, cuando los sistemas de alerta evidencien de un posible fraude, y la autorización de parte de la CRC de terminar contratos con PCA/IT reincidentes en la recuperación de códigos cortos por indebido uso – uso fraudulento.

5. CONCLUSIÓN

De acuerdo con lo manifestado a lo largo de este documento, es necesario que antes de analizar las propuestas regulatorias planteadas, es necesario que la CRC:

- Analice el efecto que generó la suspensión provisional de los códigos cortos al inicio de una actuación administrativa, con el fin de determinar si las demás medidas propuestas son necesarias.
- Permita la terminación de contratos de acceso con PCA/IT reincidentes.
- Implemente procesos más cuidadosos/estrictos frente a los solicitantes de recursos de numeración.
- Permita el bloqueo de SMS/llamadas/nacionales/internacionales, cuando se evidencie posible fraude.



- Una vez analizado el efecto de la suspensión provisional, realice un AIN de las medidas que implican las demás propuestas presentadas.

Esperamos que los comentarios acá remitidos sean tenidos en cuenta.

Cordialmente,

Firmado por:

Maria Teresa Castañeda Guerrero

8F75C896CF544D1...

MARIA TERESA CASTAÑEDA GUERRERO
GERENTE DE REGULACIÓN Y RELACIÓN CON OPERADORES