

Señores Comisión de Regulación de Comunicaciones (CRC):

Atendiendo la invitación para remitir comentarios al Proyecto De Resolución (PR) *“Por la cual se modifica la remuneración de las redes de servicios móviles con ocasión de su utilización a través de mensajes cortos de texto (SMS) de aplicación a persona (A2P) y se dictan otras disposiciones”*, la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria), remite las siguientes observaciones de sus entidades agremiadas con el propósito de contribuir al análisis del esquema de remuneración propuesto y de su articulación con los objetivos regulatorios y la protección de los consumidores financieros y usuarios.

COMENTARIOS GENERALES

Ausencia de responsabilidades diferenciadas como falla del ecosistema A2P.

Se identifica como una de las causas de la baja efectividad de las herramientas regulatorias para la prevención del fraude la ausencia de responsabilidades diferenciadas y trazables entre los originadores, los integradores tecnológicos, los proveedores de contenidos y aplicaciones (PCA), los operadores móviles y los demás actores que participan en el envío de mensajes A2P. Esta situación diluye los incentivos para la prevención y limita la capacidad de reacción del ecosistema. Se sugiere reconocer esta causa en el Análisis de Impacto Normativo, en la medida en que ello fortalecería la coherencia entre el diagnóstico y las medidas que se pretenden establecer mediante el presente PR.

Lo anterior, debe atender especialmente a las funciones de cada participante relacionadas con el monitoreo de anomalías, la detección de campañas, el bloqueo o suspensión, la gestión de incidentes y la conservación de evidencia, así como a la definición de obligaciones frente a la calidad, exactitud, seguridad y oportunidad de la información suministrada, y a las medidas de prevención y mitigación del fraude.

Obligaciones reforzadas de monitoreo, suspensión preventiva y conservación de evidencia.

Se recomienda definir el tratamiento económico del tráfico confirmado como fraudulento, abusivo o no autorizado, y evaluar mecanismos de ajuste, reversión o atribución de costos cuando corresponda. De igual manera, se sugiere tener en cuenta que la conservación de los registros asociados al envío de SMS A2P por un período mínimo de cinco años permitiría contar con una trazabilidad completa de la cadena de envío.

Mecanismos de protección de la información.

Se sugiere establecer mecanismos de protección, integridad, confidencialidad y conservación de la información asociada a los reportes de tráfico, Sender ID y códigos cortos, teniendo en cuenta que la información puede resultar relevante para la investigación y gestión de eventos de fraude. Del mismo modo, se recomienda que los esquemas de reporte asociados a la trazabilidad y supervisión del servicio garanticen el cumplimiento de las disposiciones sobre protección de datos personales y principios de minimización de información.

Alcance de la protección.

El PR regula la metodología de remuneración en la relación entre el operador móvil y el integrador tecnológico, desarrollando una metodología de cálculo circunscrita a dicha relación, sin que el proveedor de contenidos y aplicaciones sea considerado dentro de la metodología, aunque es este quien asume el costo y lo refleja en los servicios que presta a sus clientes. Lo anterior, ocurre en un mercado en el que la propia CRC reconoce la existencia de fallas estructurales de competencia, por lo que la protección regulatoria circunscrita a la relación con el integrador no cubriría la totalidad de la cadena en la que se materializa dicho costo. En consecuencia, se sugiere que los principios de orientación a costos, no discriminación y transparencia se tengan en cuenta también respecto a la relación con el proveedor de contenidos y aplicaciones.

Impacto sobre mensajes de autenticación, seguridad y prevención del fraude.

Los mensajes utilizados para autenticación, validación de identidad, confirmación de transacciones, alertas de fraude y demás comunicaciones asociadas a la gestión del riesgo operacional y la protección del consumidor financiero cumplen una finalidad distinta de la mensajería comercial, sin que el esquema de remuneración propuesto establezca una distinción entre unos y otros. Dicho esquema tendría un impacto presupuestal significativo para las entidades financieras, debido al incremento en la remuneración de los SMS A2P utilizados en mecanismos de autenticación, OTP, alertas transaccionales y notificaciones de seguridad. En la medida en que estos mensajes constituyen controles para la prevención del fraude y la protección del consumidor financiero, la aplicación de una remuneración equivalente a la de la mensajería comercial podría generar un desincentivo para su uso por parte de las entidades financieras, con efectos sobre la gestión de riesgos, la ciberseguridad y la protección de los usuarios.

Considerando lo anterior, se sugiere que la CRC evalúe mecanismos regulatorios que permitan reconocer el carácter esencial de estas comunicaciones dentro del esquema de remuneración, o que contemplen un monitoreo diferenciado del impacto de la medida sobre este tipo de servicios, así como la posibilidad de establecer una remuneración diferenciada para los mensajes asociados a la autenticación, la prevención del fraude y la protección del consumidor financiero.

Evaluaciones Ex post de seguimiento e indicadores.

Se sugiere considerar la realización de evaluaciones periódicas ex post sobre los efectos de la medida en términos de costos, utilización del servicio, evolución de la competencia y uso de comunicaciones críticas por parte de sectores intensivos en mensajería A2P, con el propósito de verificar que los resultados observados sean consistentes con los objetivos regulatorios perseguidos. Además, se recomienda establecer indicadores que permitan medir o evaluar si estas medidas y costos asociados se traducen efectivamente en una reducción de mensajes fraudulentos, suplantación de remitentes y uso indebido de marcas.

COMENTARIOS ESPECÍFICOS

Duplicación de los costos (Artículo 1 - artículo 4.2.7.1).

El costo eficiente de terminación expuesto en el PR parece incorporar las actividades tendientes a la prevención del fraude. No obstante, esas mismas medidas ya se contemplan financiadas por el ecosistema en la primera fase del proyecto (Resolución CRC 8308 de 2026), a través del validador centralizado, el conocimiento del cliente y el régimen de plantillas, lo que advierte el riesgo de que un mismo costo se recupere dos veces. Si bien se comparte que los costos eficientes deben remunerarse, dicha circunstancia debería materializarse por una sola vez, por lo que resulta necesario delimitar de manera expresa los componentes antifraude comprendidos en el costo y acreditar que no concurren con los ya trasladados en la primera fase.

Adicionalmente, se recomienda precisar la articulación entre los diferentes mecanismos de recuperación de costos previstos para el ecosistema A2P, con el propósito de evitar eventuales superposiciones, así como aclarar los criterios de asignación y recuperación de costos considerados dentro de la remuneración propuesta, identificando expresamente qué componentes son reconocidos a través del esquema tarifario y cuáles son cubiertos mediante otros mecanismos, con el fin de evitar incertidumbre respecto a una doble recuperación.

Indicadores y reporte de información (Artículo 1 - artículo 4.2.7.1 parágrafo 4).

La evolución del tráfico constituye un indicador relevante para evaluar el funcionamiento del mercado; sin embargo, no necesariamente refleja la efectividad integral del esquema regulatorio. Por tanto, se considera conveniente complementar los criterios de revisión futura incorporando variables asociadas a resultados regulatorios y operativos, tales como la evolución de indicadores de fraude, el comportamiento de costos para sectores intensivos en mensajería crítica, la efectividad de las comunicaciones de autenticación y las tendencias de migración tecnológica hacia otros mecanismos de interacción con usuarios.

Adicionalmente, se considera necesario separar el reporte trimestral regulatorio previsto en el artículo 6, numeral 6.2, del reporte de incidentes antifraude, y crear un mecanismo de notificación prioritaria para campañas activas, junto con un protocolo de detección, validación, suspensión preventiva, investigación, comunicación, recuperación y cierre. Ante casos inminentes determinados como fraude, debe existir capacidad de reacción y contención oportuna, sin esperar el cierre de la investigación.

Reporte de información de códigos cortos de la Resolución CRC 5050 de 2016 (Artículo 5).

Se considera que la finalidad del reporte se potenciaría si se incorporan nuevos campos que permitan a la CRC medir de manera objetiva si las medidas adoptadas están reduciendo efectivamente el fraude, en la medida en que el esquema actual no contempla indicadores específicos para dicha medición. En particular, se considera positivo incluir rubros como la cantidad de campañas bloqueadas, el número de Sender ID suspendidos, los reportes de smishing recibidos, los incidentes confirmados de fraude, el volumen de

SMS asociados a eventos fraudulentos y el tiempo promedio de bloqueo de campañas sospechosas. Con estos indicadores, la CRC contaría con insumos verificables para evaluar la efectividad de la intervención y calibrar futuros ajustes regulatorios.

De manera complementaria, se sugiere ampliar el esquema de información para permitir reconstruir un incidente de seguridad considerando la siguiente cadena de la comunicación: originador, PCA o integrador, Sender ID o código corto, PRSTM, fecha y hora, tráfico, destino, alerta y acción, con el fin de prever herramientas de conservación, salvaguarda de la integridad, disponibilidad y entrega controlada de evidencia que permitan reconstruir un incidente de seguridad.

Reporte de información de códigos cortos de la Resolución CRC 5050 de 2016 (Artículo 5: 5. ID de cliente: - 7. Sender ID).

Los campos del Formato T.5.2 referidos al Sender ID y al ID Cliente no precisan la responsabilidad del asignatario del Sender ID frente a la autenticidad de la marca representada ni frente a la actualización de la información de identificación y contacto ante la CRC, como tampoco se establecen requisitos de debida diligencia para los titulares de Sender ID, PCA e integradores, ni una validación mínima de conocimiento del cliente en el punto de acceso al ecosistema.

Esta ausencia de precisión y de requisitos mínimos de debida diligencia en el punto de acceso facilita la ocurrencia de suplantaciones, marcas falsas y campañas fraudulentas, y genera zonas grises derivadas de la tercerización relacionadas con quién valida, monitorea, bloquea, informa e investiga. Asimismo, favorece la utilización de empresas de papel o estructuras jurídicas transitorias para el envío de campañas maliciosas, en detrimento de la confianza de los usuarios en las comunicaciones de las entidades con las que tienen contratados servicios o de las que autorizan comunicaciones.

Por lo anterior, se estima pertinente precisar que el asignatario del Sender ID será responsable de garantizar la autenticidad de la marca representada y de actualizar la información de identificación y contacto ante la CRC. Se sugiere, igualmente, establecer requisitos de debida diligencia para los titulares de Sender ID, PCA e integradores, relativos a la existencia y/o representación legal, la actividad económica, el beneficiario final, los antecedentes relevantes y la actualización de información, así como definir claramente quién valida, monitorea, bloquea, informa e investiga.

Quedamos atentos a cualquier inquietud respecto a los comentarios aquí expresados y, de ser necesario, a su disposición para coordinar una reunión que permita su discusión.

Se espera que esta comunicación contribuya al perfeccionamiento de la actividad regulatoria de la Comisión.