

18 de Diciembre de 2025

Doctora
Claudia Ximena Bustamante Osorio
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
Ciudad

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

Respetada Directora,

Reciba un cordial saludo desde Aldeamo - www.aldeamo.com - quien opera en Colombia desde la razón social Axesnet SAS.

A continuación presentamos nuestros comentarios frente a las alternativas regulatorias planteadas en su documento de Noviembre del 2025, y en concreto frente al punto 7.1. **Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS).**

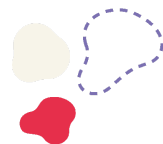
Queremos iniciar agradeciendo esta iniciativa que, esperamos, termine en regulaciones sencillas y concretas que disminuyan el fraude y que balanceen las responsabilidades entre los diferentes actores involucrados en el envío de un mensaje de texto.

En Aldeamo operamos en 12 países de Latinoamérica y nuestras estadísticas muestran que el phishing se intenta mucho más en Colombia que en otros países de la región. Al analizar diferentes factores, consideramos que hay uno que resalta: **el bajo precio regulado de un mensaje de texto en Colombia.**

Este precio, que en el mejor de los casos es **11 veces más económico que el precio de un mensaje de texto en otros países de la región**, hace que cualquier grupo criminal local o extranjero que piense hacer phishing utilizando SMS, intente primero en Colombia.

A continuación una tabla que muestra el comparativo de precio de venta de mensajes de texto de nuestra empresa en algunos países de la región:





Pais	Precio USD	Múltiplo vs Colombia	PVP en COP
Colombia	0.00043		1.66
Costa Rica	0.00494	11.49	19.02
Perú	0.01155	26.86	44.47
Mexico	0.01560	36.28	60.06
Ecuador	0.03532	82.14	135.98
Panamá	0.03822	88.88	147.15
Bolivia	0.06642	154.47	255.72

Los que usan mensajes de texto para fraude son organizaciones complejas que invierten en personal y tecnología para alcanzar sus objetivos y que están en actualización permanente de sus estrategias y sistemas para evitar cualquier obstáculo que se les presente. Si asumimos que cuando hacen un fraude consiguen un millón de pesos colombianos (en dólares US\$ 260 aproximados), y que necesitan, por ejemplo, enviar 50.000 mensajes para que una persona caiga en la trampa, este es el retorno de la inversión para los países mencionados:

Transacciones para 1 fraude		50,000	
Robo x 1 fraude	\$ 260.00		
Pais	Precio USD	50.000 TX	Retorno
Colombia	0.00043	\$ 21.50	12.09
Costa Rica	0.00494	\$ 247.00	1.05
Perú	0.01155	\$ 577.50	0.45
Mexico	0.01560	\$ 780.00	0.33
Ecuador	0.03532	\$ 1,766.00	0.15
Panamá	0.03822	\$ 1,911.00	0.14
Bolivia	0.06642	\$ 3,321.00	0.08

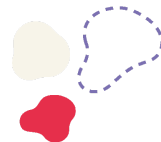
La rentabilidad del fraude en Colombia, con estos datos, es muy superior a la de otros países.

Proponemos que por favor evalúen eliminar la regulación de los precios de mensajes de texto para que estos sean puestos por el mercado.

Consideramos que esta medida:

- Bajará los intentos de fraude en nuestro país
- Generará ingresos extra para la cadena de envío que podrán ser invertidos en mejores herramientas para la prevención de esta práctica

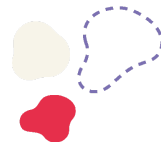




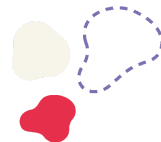
Y esto sin aumentar los **costos totales** para las empresas que utilizan estos servicios y que están siendo suplantadas para realizar fraude. El costo total es el costo de los envíos de mensaje más el costo del fraude.

A continuación presentamos cada una de las temáticas de su documento, con nuestros comentarios frente a las alternativas.

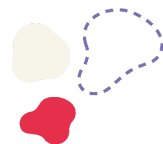
Temática 1	Falta de identificación clara del remitente en SMS A2P
Alternativa preferida	3) Introduce la obligatoriedad de que el Sender ID alfanumérico sea aplicado únicamente a mensajes transaccionales, mientras que el tráfico promocional continúa identificándose mediante códigos cortos o números E.164, manteniendo la obligación actual de incluir el nombre del originador dentro del texto del mensaje.
Comentario sobre quienes usan Sender ID alfanumérico	El envío de mensajes utilizando un Sender ID alfanumérico es una excelente medida de control de phishing. <i>Sin embargo, no debemos confundir el objetivo de disminuir el fraude vía SMS phishing con el de registrar a todos los que envían mensajes de texto.</i> Proponemos que la decisión de adopción de dicha medida no sea consecuencia del tipo de mensaje (transaccional vs promocional) sino que sea a discreción de la entidad que lo desee. Se pueden crear varios niveles: • Entidades que quieran identificarse con Sender ID alfanumérico. (recomendable para aquellas que son suplantadas en los intentos de fraude) • Entidades que quieran tener un código corto exclusivo. (recomendable para entidades que envían muchos mensajes y que no tienen riesgo de fraude. Ej: mensajes de mercadeo) • Entidades que estén dispuestas a compartir un código corto Las entidades más utilizadas para engañar a usuarios (entidades financieras, empresas de servicios públicos, operadores móviles) deberían adoptar los Sender ID alfanuméricos sin volverlos obligatorios para todos.
Comentario sobre el proceso para asignar	Proponemos también un proceso para asignar Sender ID alfanumérico que sea corto, sencillo, coordinado por los operadores



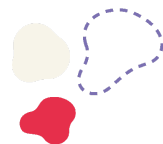
Sender ID alfanumérico	móviles (similar al que ya tienen implementado en otros países de la región y que ya utilizan para algunos de sus envíos de mensajes SMS en Colombia) y que permita fácilmente a una empresa enviar mensajes con un Sender ID alfanumérico.
Posibilidad de tener varios Sender ID alfanuméricos	También proponemos que una empresa pueda configurar varios Sender IDs alfanuméricos para diferenciar su tráfico. Por ejemplo: - Banco XX - Citas - Banco XX - Transacciones - Banco XX - Mercadeo De esta forma cada entidad podrá hacer campañas promocionales que ayuden a sus usuarios y clientes a identificar los mensajes que realmente son originados por ellos. A continuación una imagen de ejemplo de una empresa de seguros en España (Adeslas) que utiliza varios códigos alfanuméricos para sus envíos 



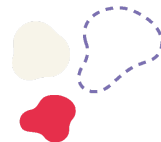
Temática 2	Dificultad para tener una trazabilidad en comunicaciones A2P y falta de controles efectivos para prevenir el fraude
Comentarios sobre los códigos cortos como un bien escaso	En nuestra opinión, los códigos cortos no son un bien escaso. Por el contrario, son muchos y se pueden crear más. La regulación Colombiana decidió que sólo pueden iniciar con el número 8 y tener ciertos dígitos. Esta legislación se creó cuando existían muchos códigos de cobro al usuario final y es una normativa que se podría modificar para incrementar la cantidad de códigos disponibles. En nuestra revisión hay una gran cantidad de códigos cortos que no se están usando, bien sea porque no están asignados o porque han sido recuperados. Todas las medidas de control que se tienen hoy en día parten de una regulación que no funciona bien y en donde todas las entidades participantes, incluyendo a la CRC, gastan recursos importantes para controlar el fraude sin mucho éxito. Algunos ejemplos de la regulación que no funciona son: - Empresas que sufren las consecuencias del fraude (por ejemplo los bancos) y que no se registran ante la CRC como PCA y no obtienen sus propios códigos cortos por no conocer el procedimiento para hacerlo, por no tener claridad en su duración, porque no quieren otra entidad del gobierno que los regule o porque no confían en que, registrándose, van a eliminar el phishing. - Integradores que, para poder prestar servicio, adquieren códigos cortos que son usados por terceros. - Un ente regulador (CRC) que intenta controlar a quienes envían mensajes fraudulentos con un sólo procedimiento que tiene poco éxito: “recuperar el código corto”. Esta medida ha estado en uso por años y el fraude sigue aumentando. Nuestra propuesta es que, además de las alternativas presentadas, se considere modificar la regulación eliminando lo que no funciona y liberando recursos para poder combatir los mensajes de SMS fraudulentos.
Alternativa preferida	2) Proceso de validación centralizado de originadores de contenido
Comentarios sobre Medida 1 de la alternativa 2	Estamos de acuerdo con esta medida, y, para que sea exitosa, nos gustaría proponer las siguientes adiciones:



Conocimiento del cliente (KYC) obligatorio para agregadores	- Los estándares de KYC deben ser definidos en un grupo de trabajo entre las partes interesadas, para evitar procesos muy largos que hagan inviable la adquisición de nuevos clientes. - Los estándares deben ser obligatorios para: - los agregadores - los operadores que ofrecen servicios de SMS como parte de otras soluciones - las empresas de cobranzas - los BPOs Y toda otra entidad que preste servicios a terceros y que utilice mensajes de texto. Esto para evitar que un agregador tenga de cliente a un BPO (por ejemplo) y que el BPO no registre a sus clientes y por allí pase un mensaje de phishing sin el KYC adecuado. - Además, proponemos que se tengan estándares para empresas internacionales que utilizan estos servicios, que también deben presentar los KYC de sus clientes o aceptar las consecuencias de una operación en Colombia con limitaciones por definir entre varias partes.
Comentarios sobre Medida 2 Proceso de validación centralizado (tercero)	Nuestra propuesta es que el ente centralizador sea la CRC. Ya tienen la tarea muy adelantada con la centralización de información de los códigos cortos. Sólo se debe modificar y simplificar para que sea más efectiva. Asignar cualquier otro tercero lleva a preguntarse ¿de dónde salen los recursos para pagarle?, ¿Quién sería este ente validador?, ¿Quién lo selecciona? También consideramos que implementar esta medida de forma equivocada puede incrementar el trabajo de las marcas, de los agregadores, de los PRSTM, y proponemos que se haga una mesa con varios jugadores para definir un procedimiento que le funcione a todos.
Comentarios sobre Medida 3 Bloqueo o marcado por parte del PRSTM de tráfico no autorizado	Partiendo de la base de que las empresas que quieran podrán enviar mensajes con Sender ID alfanumérico y que podrán hacer campañas masivas de educación y prevención (del estilo de: todos los mensajes de texto oficiales de mi empresa llegan desde el remitente EMPRESA XX - todos los demás son intentos de fraude), consideramos que esta medida es innecesaria.



	El mercado operaría así: - Entidades que envían mensajes con Sender ID alfanumérico - Entidades que envían por código corto exclusivo - Entidades que envían por código corto compartido En pocos meses, la gente que reciba un mensaje de texto fraudulento tratando de suplantar a una entidad que usa alfanumérico sabrá que es fraude. Sin embargo, estaríamos dispuestos a considerar el marcado de los mensajes que provengan de call centers, BPOs, empresas de cobranza o empresas internacionales que no cumplan con los estándares de KYC con una etiqueta como “sin verificar”.
Comentarios sobre Medida 4 Categorización del contenido y consentimiento del usuario (articulación con RNE)	Nos parece una buena iniciativa que se debe profundizar. Proponemos que la caracterización del contenido sea realizada por un grupo compuesto por varias entidades, definiendo guías claras de los mensajes que entran en cada categoría.
Comentarios sobre medida 5 Definición de reglas de monitoreo de tráfico por agregadores	Nos parece una buena idea monitorear el tráfico y consideramos que este monitoreo no debe recaer en su totalidad en el eslabón más débil de la cadena: los agregadores. Los operadores móviles, las empresas de cobranza, los BPOs, los call centers y las empresas internacionales también pueden contribuir a este monitoreo. De nuevo nos surge la duda de los recursos para implementar estas medidas, teniendo en cuenta un costo de mensajes regulado. Liberar el precio permitiría a los diferentes eslabones de la cadena cobrar un precio diferencial por los mensajes que cumplen con todo el monitoreo, mientras que los mensajes más económicos podrán ser marcados según lo mencionado en la Medida 3.



Temática 3	Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados
Comentarios sobre la temática	Existen varias herramientas en el mercado para controlar los mensajes SMS P2P que han sido implementadas por muchos operadores en varios países. Algunos operadores deciden hacer una negociación con un tercero (por lo general un agregador de SMS) para que haga este tipo de control. El motivo principal por el que este control no se ha implementado en Colombia es el costo. De nuevo proponemos que se elimine la regulación que controla el precio de los mensajes de texto, para que se generen los recursos necesarios para esta implementación

Terminamos poniéndonos a sus órdenes para conversar sobre este tema. Apoyamos esta iniciativa porque dejará en evidencia a las empresas interesadas en apoyar la tecnología y combatir el fraude y a las que no les interesa el tema.

Esperamos que **las medidas adoptadas sean definidas por mesas en las que diferentes actores participen al mismo tiempo**, de lo contrario, se corre el riesgo de que lo implementado no funcione.

Cordialmente

ALFREDO JOSÉ ÁNGEL SAÑUDO
REPRESENTANTE LEGAL
AXESNET S.A.S

