COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

RESOLUCIÓN No. DE 2026

*«Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones»*

## LA SESIÓN DE COMISIÓN DE COMUNICACIONES DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES

En ejercicio de sus facultades legales, y especialmente las que le confiere los numerales 1, 3 y 12 del artículo 22 de la Ley 1341 de 2009, modificados por la Ley 1978 de 2019, y

## CONSIDERANDO

### 1. ANTECEDENTES NORMATIVOS

Según lo dispuesto en el artículo 334 de la Constitución Política, la dirección general de la economía está a cargo del Estado, el cual intervendrá de manera especial, por mandato de la ley, en los servicios públicos y privados, con el fin de racionalizar la economía, en aras del mejoramiento de la calidad de vida de los habitantes, la distribución equitativa de las oportunidades y los beneficios del desarrollo.

El artículo 365 de la Constitución Política establece que los servicios públicos son inherentes a la finalidad social del Estado, conforme lo disponen los artículos 1 y 2 de la Carta Fundamental y, en consecuencia, le corresponde asegurar su prestación eficiente a todos los habitantes del territorio nacional.

De igual forma, el artículo 365 mencionado establece que los servicios públicos estarán sometidos al régimen jurídico que fije la ley y que, en todo caso, al Estado le corresponde la regulación, el control y la vigilancia de dichos servicios.

Aunado a lo anterior, el numeral 2 del artículo 2° de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, establece que, en virtud del principio de libre competencia, el Estado debe propiciar escenarios de competencia que incentiven la inversión actual y futura en el sector de las Tecnologías de la Información y las Comunicaciones (TIC) y que permitan la concurrencia al mercado, con observancia del régimen de competencia, bajo precios de mercado y en condiciones de igualdad.

En este sentido, el artículo 19 de la Ley 1341 de 2009, modificado por el artículo 15 de la Ley 1978 de 2019, dispone que la Comisión de Regulación de Comunicaciones (CRC o la Comisión) es el órgano encargado de promover la competencia en los mercados y el pluralismo informativo, evitar el abuso de posición dominante, regular los mercados de las redes y los servicios de comunicaciones y garantizar la protección de los derechos de los usuarios, con el fin de que la prestación de los servicios sea económicamente eficiente y refleje altos niveles de calidad.

En el mismo artículo se precisa que la regulación que adopte la CRC deberá promover la inversión, la protección de los usuarios, la calidad de los servicios, la simplificación regulatoria, la neutralidad de la red, así como también incentivar la construcción de un mercado competitivo que desarrolle los principios orientadores de la Ley 1341 de 2009.

Acorde con lo anterior, el numeral 1 del artículo 22 de la Ley 1341 de 2009, modificado por el artículo 19 de la Ley 1978 de 2019, dispone que la CRC debe expedir el régimen de regulación que maximice el bienestar social de los usuarios.

El numeral 3 del artículo 22 de la Ley 1341 de 2009 dispone que la CRC expedirá toda la regulación de carácter general y particular en las materias relacionadas con el régimen de competencia, los aspectos técnicos y económicos relacionados con la obligación de interconexión y el acceso y uso de instalaciones esenciales, recursos físicos y soportes lógicos necesarios para la interconexión. Además, la Comisión podrá expedir la regulación relacionada con la remuneración por el acceso y uso de redes e infraestructura, precios mayoristas, las condiciones de facturación y recaudo; el régimen de acceso y uso de redes; los parámetros de calidad de los servicios; los criterios de eficiencia del sector y la medición de indicadores sectoriales para avanzar en la sociedad de la información; y en materia de solución de controversias.

Por su parte, el numeral 12 del artículo 22 de la Ley 1341 de 2009 dispone que la CRC regulará y administrará los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones y cualquier otro recurso que actualmente o en el futuro identifique redes y usuarios, salvo el nombre de dominio de Internet bajo el código del país correspondiente a Colombia -.co-.

### 1.1. Antecedentes asociados a la administración de los recursos de identificación y el Registro de Números Excluidos (RNE)

De conformidad con el artículo 2 de la Ley 1341 de 2009, las Tecnologías de la Información y las Comunicaciones -TIC son una política del Estado, cuya investigación, fomento y promoción deben contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto de los derechos humanos inherentes y la inclusión social, por lo cual deben servir al interés general y es deber del Estado promover su acceso eficiente y en igualdad de oportunidades, a todos los habitantes del territorio nacional.

En virtud del principio de uso eficiente de la infraestructura y de los recursos escasos, dispuesto en el numeral 3 del artículo 2 de la Ley 1341 de 2009, el Estado se encuentra en la obligación de fomentar el despliegue y uso eficiente de la infraestructura para la provisión de redes de telecomunicaciones y los servicios que sobre ellas se puedan prestar, así como promover el óptimo aprovechamiento de los recursos escasos con el ánimo de generar competencia, calidad y eficiencia, en beneficio de los usuarios.

Los numerales 12, modificado por el artículo 19 de la Ley 1978 de 2019, y 13 del artículo 22 de la Ley 1341 de 2009 se refieren a las competencias de la CRC de regular y administrar los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones y cualquier otro recurso que actualmente o en el futuro identifique redes y usuarios, salvo el nombre de dominio de Internet bajo el código del país correspondiente a Colombia, así como de administrar el uso de los recursos de numeración, identificación de redes de telecomunicaciones y otros recursos escasos utilizados en las telecomunicaciones, diferentes al espectro radioeléctrico.

Mediante la Resolución CRC 5968 de 2020, la CRC consolidó el Régimen Integral de Administración de Recursos de Identificación utilizados en Colombia y administrados por la misma entidad. Así, tomando como base las buenas prácticas nacionales e internacionales que se venían aplicando en esa época, así como la fijación de principios, criterios y procedimientos para la gestión, uso asignación y recuperación de dichos recursos de identificación, el objetivo principal de esta medida regulatoria fue la preservación y garantía de la disponibilidad de los diez recursos de identificación utilizados en el territorio nacional.

Así mismo, se creó el Trámite Único de Recursos de Identificación (TURI) para que los agentes interesados en acceder a los recursos de identificación que administra la CRC realizaran las solicitudes y efectuaran la devolución de forma digital. Entre los recursos contemplados en dicha facilidad digital están los códigos cortos para SMS y USSD y la numeración E.164. Por su parte, también se realizaron nuevas atribuciones para la numeración E.164 dentro de la modalidad no geográfica de servicios, con la intención de atender las necesidades de la industria en cuanto al despliegue de servicios Machine to Machine (M2M) y en general el ecosistema de internet de las cosas (IoT, por sus siglas en inglés), así como atender las necesidades de los diferentes modelos de negocio planteados por los proveedores de servicios de SMS (SMS-SP – SMS Service Providers por sus siglas en inglés).

Mediante Resolución CRC 6522 de 2022, la CRC introdujo modificaciones, principalmente, al régimen de acceso, uso e interconexión de redes de telecomunicaciones contenido en el Título IV de la Resolución CRC 5050 de 2016. Específicamente sobre la numeración de códigos cortos para SMS y USSD se implementaron algunas reglas, por medio de la cual se ajustó el Registro de Números Excluidos (RNE) cuyo objetivo es identificar a todos aquellos usuarios que no desean ser contactados para fines comerciales o publicitarios.

En este contexto, la precitada resolución permitió habilitar a los PCA y a los IT la consulta del RNE, para que estos agentes realicen directamente la actualización de sus bases de datos utilizadas para el envío de SMS o USSD, con fines comerciales o publicitarios. En similar sentido, se estableció la obligación en cabeza de los PRST de integrar o complementar la base de datos de dicho registro con la información que reciben directamente del usuario, a fin de mantener la información actualizada.

En otras palabras, mediante la Resolución CRC 6522 de 2022 se extendieron las obligaciones definidas en el RNE a los Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT), permitiéndoles el acceso a dicho registro con el fin de que estos agentes realicen directamente la actualización de sus propias bases de datos utilizadas para el envío de SMS o USSD, con fines comerciales o publicitarios, tarea que antes era responsabilidad exclusiva de los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM). Así mismo, la mencionada resolución estableció una obligación a los PRSTM de integrar la información contenida en el RNE con la información de solicitudes de exclusión que presenten los usuarios directamente a través de los diferentes medios de atención. Estas disposiciones entraron a regir en julio de 2023.

El 10 de julio de 2023, el Congreso de la República de Colombia expidió la Ley 2300, por medio de la cual se establecen medidas para proteger el derecho a la intimidad de los consumidores. De acuerdo con su artículo 1o, dicha Ley tiene como objetivo proteger el derecho a la intimidad de los consumidores, estableciendo los canales, el horario y la periodicidad en la que estos pueden ser contactados, tanto por las entidades vigiladas por la Superintendencia Financiera, como también por todas las personas naturales y jurídicas que adelanten gestiones de cobranza de forma directa, por medio de terceros o por cesión de la obligación.

El artículo 5 de la Ley 2300 de 2023 ordena que lo dispuesto en ella «se aplicará en los mismos términos a las relaciones comerciales entre los productores y proveedores de bienes y servicios privados o públicos y el consumidor comercial frente al envío de mensajes publicitarios a través de mensajes cortos de texto (SMS), mensajería por aplicaciones o web, correos electrónicos y llamadas telefónicas de carácter comercial o publicitario».

Adicionalmente, el inciso 2 del mismo artículo ordena que «el Gobierno nacional a través del Ministerio de las Tecnologías de la Información y las Comunicaciones coordinará con la Comisión de Regulación de Comunicaciones la implementación de las medidas técnicas necesarias para adaptar el Registro de Números Excluidos conforme lo establecido en la presente ley con un plazo de seis (6) meses». Las anteriores disposiciones legales confieren a los consumidores el derecho a no recibir, mientras se encuentren registrados en el RNE, los mensajes o llamadas telefónicas de naturaleza comercial o publicitaria a que se refiere el citado texto del artículo 5, previa la correspondiente adaptación de tal registro para esos efectos.

Teniendo en cuenta la expedición de la Ley 2300 de 2023, esta Comisión identificó que el RNE, en sus condiciones vigentes para esa época, no contemplaba lo establecido en dicha ley. Lo anterior por cuanto, como se explicó, la Ley 2300 de 2023 amplió el alcance del RNE definido en la regulación general de ese momento, para incluir ya no solo los mensajes de contenido publicitario enviados a través de mensajes cortos (SMS), sino ahora también aquellos enviados a través de aplicaciones o web, correos electrónicos, así como las llamadas telefónicas de carácter comercial o publicitario.

De este modo, entonces, esta Comisión identificó la necesidad de adelantar un proyecto regulatorio con el fin de adaptar, desde el punto de vista técnico, las condiciones operativas del RNE, así como también la necesidad de modificar las disposiciones de la regulación general que así lo ameriten, teniendo en cuenta lo ordenado por la Ley 2300 de 2023. Ese proyecto se materializó con la expedición de la Resolución CRC 7356 de 2024.

### 1.2. Antecedentes asociados a la remuneración de la terminación de mensajes cortos de texto (SMS) en redes móviles

En cumplimiento de lo dispuesto en el Decreto 2870 de 2007, la entonces Comisión de Regulación de Telecomunicaciones expidió la Resolución CRT 2058 de 2009 en la que estableció que el «Mercado Mayorista de terminación de llamadas móvil-móvil en todo el territorio nacional», del que también hacen parte la terminación de mensajes cortos de texto (SMS) y mensajes multimedia (MMS), es un mercado susceptible de regulación ex ante.

Posteriormente, mediante la Resolución CRC 6522 de 2022 se modificó el artículo 4.2.7.1 de la Resolución CRC 5050 de 2016, el cual establece las condiciones de remuneración por parte de los Integradores Tecnológicos (IT) y los Proveedores de Contenidos y Aplicaciones (PCA) a los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) por la terminación de SMS. Con dicha modificación, estos agentes pueden establecer de mutuo acuerdo con los PRSTM esquemas de remuneración distintos, siempre y cuando tales acuerdos se ajusten a las obligaciones y principios regulatorios y no superen los topes establecidos para este tipo de remuneración.

En tal sentido se estipuló que, cuando a petición del PCA o del IT se apliquen condiciones diferenciales en el tratamiento de determinadas porciones de tráfico de SMS, no se aplicarán los topes tarifarios establecidos en la regulación. Adicionalmente, la prestación de tales condiciones diferenciales se someterá a las siguientes reglas: i) su ofrecimiento por parte del PRST será facultativo, y se prestarán en condiciones no discriminatorias a los PCA o IT que los soliciten, sujeto a la capacidad técnica de la red del PRST; (ii) se prestarán respecto de porciones de tráfico específicas que determine el PCA o IT. Este pacto, no supondrá que todo el tráfico a ser cursado en la relación de acceso migre a este esquema, salvo que el PCA o IT así lo requiera; (iii) las condiciones de remuneración de estos servicios adicionales dentro de la relación de acceso serán definidas de manera negociada por las partes para dicho tráfico; (iv) la implementación de estos servicios implicará un aumento en la capacidad o el dimensionamiento previamente acordados en la relación de acceso mientras así lo requiera el PCA o IT, y (v) en ningún caso estos acuerdos podrán suponer una degradación del servicio o servicios no sujetos al esquema de servicios adicionales.

En esa misma oportunidad, se incluyó, dentro de las obligaciones de los PRST, el deber de garantizar los volúmenes de tráfico requeridos por los PCA o IT en las proyecciones presentadas, siempre que sea técnica y económicamente viable, en concordancia con lo señalado en el numeral 4.2.2.1.2 del artículo 4.2.2.1 de la Resolución CRC 5050 de 2016. Adicionalmente, el PRST debe velar por una adecuada gestión del tráfico de los mensajes de texto a ser enviados, teniendo en cuenta la implementación de colas para dicho tráfico, entre otras medidas, para evitar el rechazo de estos.

En paralelo, entre 2021 y 2022 la Comisión desarrolló el proyecto regulatorio «Revisión de los esquemas de remuneración móvil», el cual concluyó con la expedición de la Resolución CRC 7007 de 2022, mediante la cual se: (i) actualizaron los valores de los cargos de acceso a redes móviles; (ii) actualizaron los valores de la remuneración de Roaming Automático Nacional (RAN); (iii) modificó la regla de remuneración mayorista de la operación móvil virtual; (iv) estableció el esquema Sender Keeps All (SKA) para remunerar la interconexión en dos vías aplicable a la terminación de llamadas y SMS en redes móviles.

Es de señalar que la terminación de SMS en redes móviles no solo se encontraba regulada mediante un tope tarifario aplicable al intercambio de tráfico entre operadores móviles, sino que dicho tope también resulta aplicable a la provisión del servicio de acceso a la red mediante SMS por parte de los PRSTM a los IT y a los PCA.

Mediante Resolución CRC 8183 de 2026, la Comisión modificó las condiciones de remuneración de los servicios móviles definidas en el Título IV de la Resolución CRC 5050 de 2016 y dictó otras disposiciones. En relación con el proyecto que se materializa por vía del presente acto administrativo, en la Resolución CRC 8183 de 2026 la Comisión advirtió lo siguiente:

> «En cuanto al servicio de SMS A2P, la Comisión decidió mantener el esquema tarifario vigente, de manera que la remuneración por la terminación de mensajes corresponda al cargo actualizado aplicable, equivalente a $1 por SMS en pesos constantes de 2022, lo cual quedará consignado en la modificación del artículo 4.2.7.1 de la Resolución CRC 5050 de 201614. Este mismo valor seguirá

siendo aplicable a la terminación de mensajes cortos de texto (SMS) asociada al tráfico A2P y P2P de larga distancia internacional, condición que se incorporará mediante la adición del artículo 4.3.2.11 a la citada resolución. Lo anterior, **mientras la CRC adelanta una revisión integral de estos segmentos del mercado, en el marco del proyecto regulatorio orientado a la mitigación del fraude cibernético y al análisis de las responsabilidades e incentivos de los distintos agentes que participan en la cadena de valor**» (SNFT).

Con el fin de atender esa revisión integral relacionada con la remuneración de los SMS A2P y con el fin de evaluar las alternativas relacionadas con la temática de remuneración, la CRC consideró adecuado y necesario que el presente proyecto regulatorio fuera dividido en dos fases.

La primera fase de este proyecto abarcará de manera integral las distintas alternativas y medidas orientadas a la mitigación del fraude cibernético asociado a los servicios tradicionales de voz y SMS contenidas en este acto administrativo.

En la segunda fase la Comisión evaluará todos los aspectos asociados a la remuneración del servicio de SMS en el ecosistema A2P. Por lo tanto, será en el marco de esa fase donde se responderán de manera detallada los comentarios de los agentes relacionados con remuneración y, además, se evaluarán las respectivas alternativas. Por lo tanto, las medidas técnicas contenidas en esta resolución, que tienen relación directa con la mensajería A2P, quedarán condicionadas en su entrada en vigencia a la publicación en el Diario Oficial del acto administrativo por medio del cual la Comisión defina la nueva remuneración que aplicará en el ecosistema A2P (Fase II), en los estrictos términos de la parte resolutiva de este acto administrativo.

## 2. EVOLUCIÓN DEL PROYECTO REGULATORIO

El 4 de julio de 2025, la CRC publicó para conocimiento y participación de los interesados el documento con la formulación del problema del proyecto regulatorio denominado: «Identificación de medidas para mitigar el fraude cibernético por medio de servicios tradicionales de voz y mensajes de texto». En esa oportunidad se recibieron múltiples comentarios en relación con el documento de formulación del problema.

El 21 de noviembre de 2025, la CRC publicó el documento de Alternativas Regulatorias en el cual se presentaron las respuestas de la CRC a cada comentario recibido respecto de la formulación del problema, fundamentadas en un análisis técnico que da respuesta a las inquietudes planteadas por los interesados. Teniendo en cuenta la metodología de Análisis de Impacto Normativo -AIN, en esa oportunidad la CRC socializó con los agentes interesados las alternativas regulatorias identificadas para abordar las causas asociadas al problema definido en el marco del proyecto regulatorio «Identificación de medidas para mitigar el fraude cibernético por medio de servicios tradicionales de voz y mensajes de texto». Con el objetivo de orientar esa consulta, se solicitó a los agentes interesados que contestaran unas preguntas al momento de realizar sus comentarios, los cuales se recibieron hasta el 22 de diciembre de 2025.

De conformidad con la publicación del documento de alternativas de solución mencionado anteriormente, la CRC recibió comentarios, observaciones y sugerencias de los siguientes agentes interesados:

| **REMITENTE** | **ABREVIATURA** |
|---|---|
| ANDESCO | ANDESCO |
| ASOCIACIÓN BANCARIA Y DE ENTIDADES FINANCIERAS DE COLOMBIA | ASOBANCARIA |
| ASOMÓVIL | ASOMÓVIL |
| AXESNET S.A.S. | ALDEAMO |
| CÁMARA COLOMBIANA DE COMERCIO ELECTRÓNICO | CCE |
| CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES | CCIT |
| CÁMARA DE LA INDUSTRIA DIGITAL Y SERVICIOS | ANDI |
| COLOMBIA MÓVIL S.A. E.S.P. | TIGO |
| COLOMBIA TELECOMUNICACIONES S.A. ESP BIC | TELEFÓNICA |
| COMUNICACIÓN CELULAR S. A. COMCEL S. A | COMCEL |
| HABLAME COLOMBIA S.A. E.S.P. | HABLAME |
| INALAMBRIA | INALAMBRIA |

| | |
|---|---|
| PARTNERS TELECOM COLOMBIA S.A.S. | PTC |
| SISTEMAS SATELITALES DE COLOMBIA S.A. E.S.P. | SSC |
| SUPERINTENDENCIA FINANCIERA DE COLOMBIA | SFC |
| UNIVERSIDAD EXTERNADO DE COLOMBIA | U. EXTERNADO |
| ZANYA PINEDA MOLINA | ZANYA PINEDA |

En el documento soporte que se publicó junto con el proyecto de resolución se dio respuesta a cada uno de los comentarios presentados.

En el marco de la aplicación de la metodología de Análisis de Impacto Normativo (AIN) se elaboró el árbol del problema del proyecto regulatorio, cuya premisa central fue la siguiente: «Baja efectividad de las herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto».

A su vez, se detectaron como posibles causas del problema las siguientes:

(i) Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso

(ii) Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes

(iii) Dificultad en la identificación y rastreo de ataques cibernéticos

(iv) El enfoque regulatorio actual no diferencia entre los tipos de mensajería corta de texto P2P y A2P.

(v) Ausencia de articulación de una estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

En aplicación del ciclo de política regulatoria, se identificaron las siguientes consecuencias vinculadas al problema antes mencionado:

(i) Aumento de casos de uso indebido de códigos cortos con fines fraudulentos

(ii) Transgresión de los derechos de los usuarios de los servicios de telecomunicaciones

(iii) Afectaciones a empresas y organismos públicos

(iv) Pérdida de confianza en los servicios de telecomunicaciones

(v) Desconocimiento de los usuarios respecto de la privacidad de la información, de las modalidades de ataque y de sus posibles acciones de prevención y mitigación; facilita la obtención de datos personales con fines fraudulentos.

A partir del árbol de problema descrito, la Comisión definió como objetivo del proyecto «Diseñar la estrategia de la CRC para la prevención y mitigación del contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto».

## 3. RESULTADO DE LA EVALUACIÓN DE ALTERNATIVAS REGULATORIAS

Frente a la problemática identificada, la CRC propuso y evaluó múltiples alternativas que dividió con base en las siguientes temáticas:

a) Temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)

b) Temáticas enfocadas en mitigar el contacto a los usuarios con fines fraudulentos mediante los servicios tradicionales de voz

c) Temáticas enfocadas en la educación a la ciudadanía

d) Temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación.

Cada uno de los ejes temáticos fue dividido en sub – temáticas, las cuales a su vez estaban compuestas de diferentes alternativas con medidas claramente determinadas en el documento soporte que se publicó con el respectivo proyecto de resolución. La CRC evaluó las alternativas regulatorias referidas a las temáticas antes enunciadas, para lo cual utilizó las siguientes metodologías:

a) Multicriterio, aplicada para evaluar las alternativas regulatorias propuestas para las siguientes temáticas:

**(i) Eje de temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios móviles tradicionales de mensajes cortos de texto (SMS)**

- Temática 1: Falta de identificación clara del remitente en SMS A2P
- Temática 3: Falta de control en SMS P2P y riesgos asociados a planes con SMS ilimitados

**(ii) Eje de temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz**

- Temática 2: Falta de una instancia de coordinación para la articulación y el intercambio de alertas
- Temática 3: Falta de lineamientos específicos para monitoreo y etiquetado de tráfico
- Temática 4: Falta de estandarización en la aplicación de listas de no originación (DNO)

**(iii) Eje de temáticas enfocadas en la educación de la ciudadanía**

- Temática 1: Acciones educativas que aumenten el conocimiento de los usuarios

b) Costo – Beneficio, aplicada para evaluar las alternativas regulatorias propuestas en la «**¡Error! No se encuentra el origen de la referencia.**» correspondiente al eje del servicio SMS y la «**¡Error! No se encuentra el origen de la referencia.**» del eje del servicio de voz.

c) Costos Administrativos, empleada para evaluar aquel paquete de medidas que resultare de evaluar cada una de las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz, con el fin de contrastar el costo total acumulado frente al costo que implicaría la adopción del método STIR/SHAKEN/RCD.

d) Enfoque de simplificación normativa, aplicada a las «**¡Error! No se encuentra el origen de la referencia.**».

Como resultado de la evaluación de alternativas derivada de los análisis realizados, la cual consta de manera expresa en el documento soporte publicado con el proyecto de resolución, la CRC estructuró una propuesta regulatoria que incluyó las siguientes medidas:

**a) En relación con las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de SMS**:

(i) Crear un nuevo recurso de identificación denominado SENDER ID el cual corresponde a un código alfanumérico para todos los originadores de contenido.

(ii) Crear un sistema de validación centralizada que funcionará por medio de una persona jurídica que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de

contenido que participan en el ecosistema de tráfico A2P. Sus funciones comprenden la verificación del proceso de conocimiento del cliente adelantado por los asignatarios del código corto A2P (se subrogará el Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 para cambiar la forma en la que funcionan los códigos cortos) respecto de los potenciales asignatarios del SENDER ID, la aprobación de las plantillas de contenido A2P, y la emisión de las certificaciones requeridas en el proceso de asignación de los recursos de identificación código corto A2P y SENDER ID.

(iii) Se establecerán una serie de medidas técnicas mínimas para el control de patrones de tráfico atípicos en la mensajería P2P.

**b) En relación con las temáticas enfocadas en mitigar el contacto a usuarios con fines fraudulentos mediante los servicios tradicionales de voz**:

(i) Prohibición total del enmascaramiento de la identidad de la línea llamante (CLI).

(ii) Creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, como instancia permanente de coordinación para el intercambio de alertas, la identificación de patrones de fraude y la actualización de medidas técnicas frente al fraude cibernético a través de los servicios de voz móvil y mensajes cortos de texto (SMS). Este comité será liderado y convocado por la CRC, con base en las reglas de funcionamiento y administración que se definen en este acto administrativo.

(iii) Se crean medidas técnicas mínimas de monitoreo y etiquetado de tráfico de voz con el objetivo de detectar y prevenir la suplantación y otras actividades sospechosas en llamadas, así como etiquetar las llamadas con fines publicitarios.

(iv) Medidas enfocadas a que cada PRST mantenga su propia lista de no originación (DNO), 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 o institucionales de solo recibo de llamadas, etc.

**c) En relación con las temáticas enfocadas en la educación a la ciudadanía**:

(i) Creación de una serie de medidas que se materializan en obligaciones a nivel pedagógico y de prevención en beneficio de los usuarios de servicios móviles, las cuales estarán en cabeza de los PRST, PCA, IT, pero también a cargo de la CRC. Estas medidas tienen como base la coordinación y liderazgo entre los distintos agentes involucrados y el sector, de manera que se definen con claridad las responsabilidades específicas asociadas a las acciones de educación y prevención. Además, las medidas están divididas entre aquellas que son comunes para servicios SMS y voz, y otras independientes para SMS y voz respectivamente.

**d) En relación con las temáticas objeto de revisión asociadas al Régimen de Administración de Recursos de Identificación bajo el enfoque de simplificación:**

(i) Se creó la posibilidad de que los PRST puedan suspender provisionalmente la relación de acceso con los PCA/IT en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto por unas causales en particular. Ante una nueva reincidencia –tercera recuperación de código corto por parte de la Comisión–, el PRST con quien dicho PCA/IT tiene una relación de acceso podría iniciar un trámite de desconexión definitiva ante la CRC con el fin de que esta

Comisión autorice tal terminación. Esta medida se complementa con la inclusión de dos nuevas causales de oposición a ser invocadas por los PRST ante una solicitud de acceso por parte de PCA/IT a quienes se les haya previamente terminado una relación de acceso con ocasión de la constatada reincidencia en materia de recuperación de códigos cortos.

(ii) Precisión de los requisitos al momento de la asignación de códigos cortos, así como de las obligaciones de los asignatarios.

(iii) Prohibición de la cesión o transferencia de códigos cortos.

(iv) Modificación de la prerrogativa de suspensión provisional del tráfico de un código corto en el marco de una actuación administrativa, para que pueda ser ordenada en cualquier momento.

(v) Posibilidad de que la SIC pueda solicitar información a la CRC y al validador centralizado para que sea utilizada en el marco de las competencias de la SIC respecto de la vigilancia del RNE.

(vi) Precisión en las obligaciones relacionadas con la vigencia y actualizaciones de los registros asociados a la asignación de recursos de identificación.

## 4. ETAPA DE PARTICIPACIÓN SECTORIAL

Con fundamento en los artículos 2.2.13.3.2 y 2.2.13.3.3 del Decreto 1078 de 2015 y en el numeral 8 del artículo 8 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA), entre el 5 al 23 de junio de 2026, la CRC publicó el proyecto de resolución «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones» y el documento soporte correspondiente. Lo anterior, con el fin de garantizar la participación de todos los agentes interesados en el proceso de regulación de la iniciativa mencionada.

Dentro del plazo establecido, se recibieron comentarios, observaciones o sugerencias por parte de los siguientes agentes: _____.

En atención a los comentarios recibidos durante el proceso de consulta pública, la CRC llevó a cabo una revisión detallada de los argumentos presentados por los agentes del sector.

## 5. ABOGACÍA DE LA COMPETENCIA

De conformidad con lo establecido en el artículo 2.2.2.30.5. del Decreto 1074 de 2015, esta Comisión diligenció el cuestionario expedido por la Superintendencia de Industria y Comercio (SIC) mediante el artículo 5 de la Resolución SIC 44649 de 2010, con el fin de verificar si las disposiciones contempladas en la propuesta regulatoria publicada para comentarios del sector tienen efectos en la competencia.

En observancia de lo definido en el artículo 7 de la Ley 1340 de 2009, el artículo 2.2.2.30.8. del Decreto 1074 de 2015 y la Resolución SIC 44649 de 2010, el XX de XX de 2026 la CRC envió a la SIC el proyecto regulatorio publicado con su respectivo documento soporte, y anexó el cuestionario dispuesto por tal entidad para proyectos regulatorios de carácter general, así como, los diferentes comentarios a la propuesta regulatoria que fueron recibidos durante el plazo establecido[1].

La Superintendencia, en sede del mencionado procedimiento de abogacía de la competencia, mediante comunicación identificada con el radicado SIC XXXXX del XX de XX de 2026, emitió su concepto sobre la propuesta regulatoria publicada, a propósito de lo cual planteó las siguientes recomendaciones:

«(…)»

[1] Estos documentos fueron recibidos en la mencionada superintendencia bajo radicado con el No. XXXXXX.

Esta Comisión procedió a evaluar cada una de las observaciones y recomendaciones plasmadas en el citado concepto, con el siguiente resultado: XXX

## 6. IMPLEMENTACIÓN NORMATIVA DE LA DECISIÓN ADOPTADA

A partir del análisis de los comentarios recibidos en la etapa de socialización de la propuesta regulatoria, la CRC identificó (XXXXX)

Una vez atendidas las observaciones recibidas durante todo el proceso de discusión del presente proyecto, se elaboró el documento que contiene las razones por las cuales se aceptan o rechazan los planteamientos expuestos, el cual fue puesto a consideración del Comité de Comisionados de Comunicaciones según consta en el Acta No. XXX del XX de XXX de 2026 y de los miembros de la Sesión de Comisión de Comunicaciones el XXX de XXX de 2026 y aprobados en dicha instancia, según consta en el Acta No. XXX.

En virtud de lo expuesto,

## RESUELVE

**ARTÍCULO 1.** Adiciónense las siguientes definiciones al TÍTULO I de la Resolución CRC 5050 de 2016:

«(…)

**CONOCIMIENTO DEL CLIENTE — KYC (KNOW YOUR CUSTOMER):** Proceso de debida diligencia mediante el cual los asignatarios del código corto A2P verifican la identidad, legitimidad y perfil de riesgo de los agentes con quienes celebran contratos para cursar el tráfico de mensajería A2P, con el propósito de prevenir el uso indebido de los recursos de identificación para la comisión de fraudes mediante mensajes cortos de texto (SMS). El proceso de KYC comprende como mínimo la verificación de la existencia jurídica y representación legal del agente, la identificación del beneficiario final de la relación contractual, la acreditación del objeto social compatible con el servicio a prestar, la evaluación del perfil de riesgo del solicitante y el monitoreo continuo de la relación contractual durante su vigencia, conforme a las obligaciones establecidas en el Capítulo 13 del TÍTULO VI de la presente resolución.

**LISTA DNO (DO NOT ORIGINATE):** Lista de numeración E.164 nacional que no debe ser utilizada como identificador de línea llamante (CLI) en la originación de llamadas de voz, por tratarse de numeración no atribuida, no asignada, no adjudicada por la CRC, o reservada exclusivamente para la recepción de llamadas. Los PRST deberán implementar en sus redes mecanismos para bloquear las llamadas originadas desde números incluidos en la lista DNO, conforme a las condiciones establecidas en el artículo 2.1.10.7.2.2.3 de la presente resolución y en concordancia con la Recomendación UIT-T E.164.

**PLANTILLA DE CONTENIDO A2P (TEMPLATE ID):** Estructura base del mensaje corto de texto (SMS) que un asignatario del SENDER ID somete a aprobación del validador centralizado antes de cursarla a los usuarios finales, y que define el contenido fijo y los campos variables autorizados del mensaje, la modalidad de contenido aplicable, las condiciones de consentimiento requeridas y, cuando corresponda, las URLs o dominios de destino autorizados. Si bien la plantilla de contenido A2P se debería asociar con un número único denominado TEMPLATE ID, dicho número no es un recurso de identificación administrado por la CRC. El mal uso de la plantilla por parte del asignatario del SENDER ID o del asignatario del código corto A2P constituye causal de recuperación del respectivo recurso de identificación conforme a las reglas de atribución de responsabilidad establecidas en el Capítulo 13 del TÍTULO VI de la presente resolución. Ningún mensaje A2P podrá ser cursado a través de las redes de los PRST si no está respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

**SENDER ID:** Recurso de identificación administrado por la CRC, que identifica de manera única e inequívoca a la persona natural o jurídica responsable directa por la producción y generación de contenidos o aplicaciones enviados a través de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD).

El SENDER ID es visible para el usuario final en el encabezado del mensaje recibido y permite la identificación clara e inmediata del originador del contenido. A cada persona natural o jurídica le será asignado un único SENDER ID. El SENDER ID podrá utilizarse para una o varias de las modalidades de contenido establecidas en el artículo 6.12.1.3 del Capítulo 12 del TÍTULO VI. El tráfico A2P identificado con el SENDER ID se cursa a través del código corto A2P del agente intermediario con quien el asignatario del SENDER ID mantiene relación contractual. La asignación del SENDER ID confiere exclusivamente el derecho de uso del recurso de identificación, pero no otorga derecho de propiedad sobre el mismo, ni tendrá costo alguno para el asignatario. El régimen de administración del SENDER ID se encuentra establecido en el Capítulo 12 del TÍTULO VI de la presente resolución.

**TRÁFICO A2P (APPLICATION TO PERSON):** Modalidad de tráfico de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD) en la que el mensaje es originado por una aplicación, plataforma o sistema automatizado y tiene como destinatario a un usuario final de un servicio de telecomunicaciones móviles. Para efectos del régimen de administración de recursos de identificación establecido en el TÍTULO VI de la presente resolución, el tráfico A2P es aquel cursado mediante la utilización de un código corto A2P y un SENDER ID debidamente asignados por la CRC, respaldado por una plantilla de contenido aprobada por el validador centralizado conforme al Capítulo 13 del TÍTULO VI de la presente resolución.

**TRÁFICO P2P (PERSON TO PERSON):** Modalidad de tráfico de mensajes cortos de texto (SMS) en la que el mensaje es originado y recibido por usuarios finales de servicios de telecomunicaciones móviles, utilizando la numeración E.164 no geográfica de redes para la comunicación directa entre personas. El tráfico P2P está sujeto a las condiciones de monitoreo y control establecidas en el artículo 2.1.10.7.2.1 de la presente resolución.

**VALIDADOR CENTRALIZADO:** Persona jurídica que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico A2P. Sus funciones comprenden la verificación del proceso de KYC adelantado por los asignatarios del código corto A2P respecto de los potenciales asignatarios del SENDER ID, la aprobación de las plantillas de contenido A2P, y la emisión de las certificaciones requeridas en el proceso de asignación de los recursos de identificación código corto A2P y SENDER ID. La actuación del validador centralizado se enmarca dentro de los lineamientos regulatorios que para el efecto expida la CRC y bajo la supervisión permanente del Administrador de los Recursos de Identificación.

(…)».

**ARTÍCULO 2.** Modifíquese las siguientes definiciones del TÍTULO I de la Resolución CRC 5050 de 2016, las cuales quedarán así:

«(…)

**CÓDIGO CORTO A2P:** ~~Tipo de numeración asignada por la CRC para la prestación de servicios de contenidos y aplicaciones basados en el envío o recepción de mensajes cortos de texto (SMS) y mensajes a través del Servicio Suplementario de Datos no Estructurados (USSD). La naturaleza de esta numeración está circunscrita al posicionamiento e identificación de un tipo de servicio de contenidos y aplicaciones para los usuarios, a través de un código numérico que informe claramente el tipo de servicio, el contenido, la modalidad de compra y los costos asociados, y no para la creación de un canal de comunicación dedicado de SMS entre los usuarios finales del servicio de telefonía móvil y sus clientes~~. Recurso de identificación administrado por la CRC que corresponde a un código corto asignado de manera exclusiva e individual a cada agente que, en virtud de una relación contractual con un PRST, tiene conexión directa con este para cursar tráfico A2P de mensajería de texto (SMS). A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID. El régimen de administración del código corto A2P se encuentra establecido en el Capítulo 4 del TÍTULO VI de la presente resolución.

**INTEGRADOR TECNOLÓGICO (IT):** Agente responsable de la provisión de infraestructura de conexión y de soporte técnico entre los PRST y los PCA (asignatarios de SENDER ID) sin conexión directa con los PRST, a través de una relación contractual de acceso directo con al menos un PRST. En su calidad de responsable de la infraestructura de conexión, el IT es el asignatario del recurso de identificación denominado código corto A2P conforme al Capítulo 4 del TÍTULO VI de la presente resolución. Cuando el IT sea también responsable directo por la producción o generación de contenidos o aplicaciones propios que curse a través de su propia infraestructura de conexión, deberá ser asignatario tanto del código corto A2P, así como del recurso de identificación denominado SENDER ID conforme al Capítulo 12 del TÍTULO VI de la presente resolución, en su calidad de PCA.

**PROVEEDOR DE CONTENIDOS Y APLICACIONES (PCA):** Agente~~s~~ responsable~~s~~ directo~~s~~ por la producción o generación ~~o consolidación~~ de contenidos o aplicaciones cursados a través de redes de telecomunicaciones hacia usuarios finales de servicios de telecomunicaciones móviles. En su calidad de responsable del contenido, el PCA es el asignatario del recurso de identificación denominado SENDER ID conforme al Capítulo 12 del TÍTULO VI de la presente resolución. Estos actores pueden o no estar directamente conectados con el o los PRST sobre los cuales prestan sus servicios, por lo que el PCA puede cursar su tráfico a través de la infraestructura de conexión de un IT o por intermedio de su propia infraestructura de conexión con acceso directo a un PRST, caso en el cual deberá ser asignatario tanto del SENDER ID como del recurso de identificación denominado código corto A2P conforme al Capítulo 4 del TÍTULO VI de la presente resolución. ~~Quedan comprendidos bajo esta definición todos aquellos actores que presten sus funciones como productores, generadores o agregadores de contenido.~~

(…)».

**ARTÍCULO 3.** Modificar el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES.** Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude:

**2.1.10.7.1. Obligaciones generales:**

**2.1.10.7.1.1.** Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes y debe hacer controles periódicos respecto a la efectividad de estos mecanismos.

**2.1.10.7.1.2.** Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) que pueda tener relación con un presunto fraude, el operador debe investigar sus causas; y en caso de que determine la no existencia de un fraude, le debe demostrar al usuario las razones por las cuales no procede su PQR (petición, queja/ reclamo o recurso). Sin embargo, si se demuestra que el usuario actuó diligentemente en el uso del servicio contratado, no habrá lugar al cobro de los consumos objeto de reclamación.

**2.1.10.7.2. Obligaciones particulares:**

**2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P.**

**2.1.10.7.2.1.1.** Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar sistemas de monitoreo y control del tráfico de mensajes cortos de texto entre personas (P2P) orientados a la detección oportuna de patrones de uso atípico que sean indicativos de un posible uso fraudulento del servicio, incluyendo en particular los patrones asociados al uso masivo de planes con SMS ilimitados o con alto saldo para cursar el tráfico de naturaleza A2P simulado como P2P, al funcionamiento de granjas de SIM o a la comercialización del saldo de mensajes de texto entre usuarios. En consecuencia, cada PRST podrá seleccionar libremente las herramientas técnicas, los algoritmos y las metodologías de análisis que considere más eficientes para alcanzar los objetivos de detección y respuesta establecidos en el presente artículo, siempre que acredite ante la CRC que los sistemas de monitoreo implementados tienen la capacidad de detectar, como mínimo: (i) Volumen inusual de mensajes salientes por usuario; (ii) Alta dispersión de destinatarios; (iii) Homogeneidad del contenido; (iv) Periodicidad

mecánica[2]; (v) Ausencia de tráfico entrante correlacionado; y (vi) Concentración geográfica o de red.

**2.1.10.7.2.1.2.** Una vez el sistema de monitoreo detecte en una línea o conjunto de líneas la configuración de alguno de los patrones descritos anteriormente, el operador aplicará el siguiente esquema de respuesta escalonado, progresando de una etapa a la siguiente cuando la etapa anterior no haya resultado en la cesación del patrón detectado dentro del plazo establecido:

**Primera etapa — Alerta interna y análisis.** El sistema de monitoreo registrará el evento de detección en los logs del PRST con la identificación de la línea o líneas involucradas, el patrón detectado, la fecha y hora de inicio y el volumen de tráfico asociado. El PRST analizará el evento con el propósito de descartar falsas alarmas, para lo cual podrá considerar el historial de comportamiento de la línea, el tipo de plan contratado y cualquier otro factor de contexto relevante. Esta etapa no podrá exceder de veinticuatro (24) horas desde la detección del evento.

**Segunda etapa — Notificación al usuario.** Si superada la primera etapa el PRST concluye que el patrón detectado no corresponde a una falsa alarma, notificará al usuario titular de la línea o líneas afectadas, a través del canal de atención que el usuario haya habilitado, informándole sobre el comportamiento atípico detectado en su línea, las posibles consecuencias para la prestación del servicio si el patrón continúa, y los canales disponibles para que el usuario manifieste la existencia de una causa legítima que explique el comportamiento. El usuario tendrá un plazo de cuarenta y ocho (48) horas desde la notificación para manifestarse. Si el usuario acredita una causa legítima a satisfacción del PRST, este registrará el hecho en su sistema y no procederá a las etapas siguientes.

**Tercera etapa — Autenticación adicional.** Si vencido el plazo de la segunda etapa el usuario no se ha manifestado o la causa alegada no es satisfactoria, o si el patrón de tráfico continúa o se intensifica, el PRST podrá exigir al usuario la realización de una autenticación adicional para continuar usando el servicio de mensajería, a través de los mecanismos que el PRST defina para el efecto. Si el usuario no completa la autenticación dentro de las cuarenta y ocho (48) horas siguientes al requerimiento, el PRST procederá a la siguiente etapa.

**Cuarta etapa — Restricción temporal del servicio de mensajería.** Si superadas las etapas anteriores el patrón atípico persiste o el usuario no ha completado la autenticación requerida, el PRST podrá restringir temporalmente la capacidad de envío de mensajes de texto de la línea o líneas identificadas. La restricción tendrá una duración máxima de siete (7) días calendario, al vencimiento de los cuales se levantará automáticamente si no se han presentado nuevos eventos de detección. La restricción no afectará la capacidad del usuario de recibir mensajes de texto ni de realizar o recibir llamadas de voz.

**Quinta etapa — Reporte a la CRC y decisión sobre continuidad de la relación contractual.** Si la restricción temporal no elimina el patrón de uso atípico o si la línea vuelve a exhibir el mismo patrón dentro de los treinta (30) días calendario siguientes al levantamiento de la restricción, el PRST reportará el caso a la CRC y el PRST quedará habilitado para evaluar y decidir, conforme a las condiciones contractuales aplicables y a las disposiciones del régimen de protección de usuarios establecido en el presente título, la terminación del contrato de prestación del servicio con el usuario titular de la línea.

El esquema de respuesta escalonado previsto en el presente numeral no podrá ser aplicado de manera discriminatoria entre usuarios con el mismo perfil de comportamiento. El PRST deberá asegurar que los criterios de activación de cada etapa sean uniformes, objetivos y verificables.

**2.1.10.7.2.1.3.** La aplicación del esquema de respuesta escalonado no exime al PRST de su obligación de atender las PQR que el usuario afectado presente en relación con la restricción del servicio de mensajería, conforme al régimen de PQR vigente. El usuario tendrá derecho a solicitar en cualquier momento la revisión de la medida adoptada, acreditando que su comportamiento de uso responde a una causa legítima.

[2] Se refiere a un patrón de envío de mensajes que se repite en intervalos regulares, constantes o altamente predecibles, típicamente generado por sistemas automatizados (máquinas) y no por un comportamiento humano normal.

**2.1.10.7.2.1.4.** Los Proveedores de Redes y Servicios de Telecomunicaciones tienen la obligación de participar en el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles que se crea en virtud del artículo 2.1.10.7.3 de la presente resolución. En el referido comité los participantes podrán proponer y acordar la forma de mejorar los parámetros mínimos de detección descritos en el numeral 2.1.10.7.2.1.1 cuando la evolución de las modalidades de fraude así lo requiera. En caso de que no haya propuestas o acuerdos de actualización o mejora, aplicarán los estándares mínimos establecidos en el mencionado numeral.

**2.1.10.7.2.1.5.** Los PRST deberán implementar los sistemas de monitoreo previstos en el presente artículo y acreditar su puesta en operación ante la CRC dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que los adoptó. La acreditación se realizará mediante la presentación ante la CRC de un informe técnico que describa la arquitectura del sistema implementado, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas. Dentro de los seis (6) meses siguientes a la presentación de ese primer informe, los PRST remitirán un segundo informe a la CRC que contendrá lo siguiente:

a. El número de eventos de detección de patrones de tráfico P2P atípico registrados en el período transcurrido desde la implementación de las medidas, discriminado por tipo de patrón detectado.

b. El número de casos en que el sistema descartó el evento como falso positivo en la primera etapa del esquema de respuesta, con indicación de los factores de contexto que motivaron esa determinación.

c. El número de casos en que el usuario manifestó una causa legítima en la segunda etapa y el PRST aceptó dicha justificación, con indicación agregada del tipo de causa alegada.

d. El número de restricciones temporales del servicio de mensajería aplicadas en la cuarta etapa, discriminado por duración de la restricción.

e. El número de casos reportados a la CRC en la quinta etapa y el número de terminaciones contractuales derivadas de la aplicación del presente artículo.

f. Los umbrales y criterios aplicados por el PRST para la detección de cada uno de los patrones, con indicación de las actualizaciones realizadas a dichos criterios durante el período reportado.

g. Las PQR recibidas en relación con la aplicación del presente artículo, con indicación de su resultado.

**2.1.10.7.2.2. Obligaciones particulares en materia de prevención del fraude en los servicios tradicionales de voz.** Los Proveedores de Redes y Servicios de Telecomunicaciones deberán implementar las siguientes medidas orientadas a prevenir el contacto fraudulento a usuarios a través de llamadas de voz:

**2.1.10.7.2.2.1.** Los PRST deberán bloquear las llamadas internacionales entrantes que presenten como identificador de línea llamante (CLI) un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de tráfico de roaming internacional debidamente identificado como tal por el carrier de origen. Los carriers internacionales interconectados con operadores colombianos para la terminación de tráfico en la red móvil nacional deberán cumplir con los formatos y longitudes de numeración establecidos en la Recomendación UIT-T E.164, respetando el código de país correspondiente al origen real de la llamada.

**2.1.10.7.2.2.2.** Los PRST deberán implementar sistemas de monitoreo en tiempo real del tráfico de voz con capacidad de detectar, como mínimo, los siguientes patrones indicativos de actividad potencialmente sospechosa, las cuales pueden ser actualizadas o mejoradas en el marco del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles que se crea en virtud del artículo 2.1.10.7.3 de la presente resolución:

- Volumen inusual de llamadas por relación origen/destino, conforme a los umbrales que el PRST defina en su metodología interna, los cuales podrán ser dinámicos mediante técnicas de aprendizaje de máquina.

- Patrones repetitivos de llamadas cortas y secuenciales típicos de robocall, evaluados a través de indicadores como la duración promedio de llamada (ACD) y la tasa de respuesta (ASR).

- Correlación con listas de numeración asociadas a actividad fraudulenta, nacionales o internacionales, incluyendo las disponibles a través de mecanismos de intercambio legítimo de información.

- Eventos de enmascaramiento de numeración nacional.

Cuando el sistema de monitoreo detecte alguno de estos patrones, el PRST deberá etiquetar las llamadas originadas desde el número o rango de numeración involucrado con la indicación «Alerta de llamada sospechosa», visible en el dispositivo del usuario receptor. El etiquetado tendrá carácter temporal y se mantendrá mientras persista el patrón detectado. En ningún caso podrá extenderse por más de un mes contado desde la fecha en que cese el patrón que lo motivó.

**2.1.10.7.2.2.2.1. Etiquetado de llamadas con fines publicitarios.** Los PRSTM deberán crear un mecanismo que le permita a sus clientes corporativos, que utilicen los servicios tradicionales de voz para contactar a usuarios con fines publicitarios, inscribir de manera previa los rangos de numeración, números de teléfono o identidades de llamada utilizados con esa finalidad. Los referidos clientes corporativos tendrán la obligación de inscribirse en el registro creado por el PRSTM, previo a utilizar la numeración asignada que usarán con fines publicitarios. De esta manera, los PRSTM administrarán esa lista propia centralizada y dinámica de llamadas con la finalidad de etiquetar las llamadas que cumplan con esas características, originadas desde las líneas de dichos clientes, con la indicación «Llamada con fines publicitarios», visible en el dispositivo del usuario receptor. Para este efecto, los PRSTM mantendrán actualizado el registro de los clientes sujetos a este etiquetado en una lista propia administrada por el PRSTM que puede ser modificada de manera dinámica, ya sea porque sus clientes lo soliciten o porque los PRSTM así lo deciden. Aquellos PRSTM que identifiquen, en el marco del cumplimiento de las obligaciones derivadas del RNE, que sus clientes corporativos están realizando llamadas publicitarias a personas inscritas en el mencionado RNE, procederán a bloquear las llamadas en lugar de etiquetarlas.

Cada seis (6) meses, los PRST consolidarán una base de datos de todos los clientes u originadores inscritos en sus listas propias a las que hace referencia este artículo y de todas las llamadas etiquetadas como «Llamada con fines publicitarios» durante el período correspondiente y remitirán dicha información a la Superintendencia de Industria y Comercio (SIC), con copia a la CRC, dentro de los treinta (30) días hábiles siguientes al vencimiento de cada período semestral. La SIC utilizará esta información como insumo en el ejercicio de sus competencias de vigilancia y control en materia de cumplimiento del Registro de Números Excluidos (RNE), de conformidad con el artículo 9 de la Ley 2300 de 2023.

**2.1.10.7.2.2.2.2. Procedimiento de revisión del etiquetado de llamada sospechosa.** El usuario titular de una línea de numeración nacional que sea objeto del etiquetado previsto en el presente artículo podrá solicitar al PRST la revisión de la medida dentro de los diez (10) días hábiles siguientes a la notificación del etiquetado, acreditando que su comportamiento de uso responde a una causa legítima. El PRST resolverá la solicitud conforme al siguiente procedimiento:

**2.1.10.7.2.2.2.2.1.** Una vez recibida la solicitud, el PRST analizará la información aportada por el titular y podrá requerir información adicional dentro de los tres (3) días hábiles siguientes. El plazo total para resolver no podrá exceder de diez (10) días hábiles contados desde la recepción de la solicitud completa.

**2.1.10.7.2.2.2.2.2.** Si el PRST determina que el comportamiento detectado corresponde al uso del servicio para fines publicitarios o comerciales, comunicará esta conclusión al titular de la línea y procederá a sustituir la etiqueta «Alerta de llamada sospechosa» por la etiqueta «Llamada con fines publicitarios» conforme al numeral 2.1.10.7.2.2.2.1. del presente artículo.

**2.1.10.7.2.2.2.2.3.** Si el titular de la línea no presenta la solicitud de revisión dentro del plazo establecido, o si habiéndola presentado no logra acreditar una causa legítima que explique el comportamiento detectado, el PRST podrá, previa comunicación escrita al titular con antelación

mínima de cinco (5) días hábiles, dar por terminado el contrato de prestación del servicio de voz con el usuario titular de la línea, de conformidad con las condiciones contractuales aplicables y con las disposiciones del régimen de protección de usuarios de servicios de comunicaciones. La terminación del contrato no impedirá que el PRST reporte el caso al CTLFSM previsto en el artículo 2.1.10.7.3. de la presente resolución cuando el patrón detectado sea indicativo de actividad sospechosa a gran escala.

**2.1.10.7.2.2.2.2.4.** La aplicación del procedimiento previsto en el presente numeral no suspende el etiquetado de la llamada durante su tramitación. El etiquetado se mantendrá activo hasta que el PRST comunique al titular la conclusión del procedimiento o hasta que el patrón que lo motivó cese, lo que ocurra primero.

**2.1.10.7.2.2.3.** Los PRST deberán mantener e implementar en sus redes una lista de No Originación (DNO) que contenga, como mínimo, la numeración nacional que no debe ser utilizada como identificador de línea llamante (CLI) por corresponder a numeración no atribuida, no asignada, no adjudicada por la CRC, o reservada exclusivamente para la recepción de llamadas. Los PRST deberán bloquear las llamadas que presenten numeración incluida en la lista DNO.

El Administrador de los Recursos de Identificación publicará y mantendrá actualizada en el SIGRI la relación de numeración que debe ser incluida obligatoriamente en la lista DNO de todos los PRST. Los PRST podrán añadir a su lista DNO numeración adicional que identifiquen en el ejercicio de sus funciones de monitoreo, e informarán de dichas adiciones a la CRC dentro de los cinco (5) días hábiles siguientes a la modificación de su lista DNO.

**2.1.10.7.2.2.4. Plazo de implementación y reporte**. Los PRST deberán implementar las medidas previstas en los numerales 2.1.10.7.2.2.1., 2.1.10.7.2.2.2. y 2.1.10.7.2.2.3 del presente artículo dentro de los tres (3) meses siguientes a la publicación en el Diario Oficial de la resolución que las adoptó, y acreditarán su puesta en operación ante la CRC mediante informe técnico que describa los sistemas implementados, los parámetros de detección adoptados y los resultados de las pruebas de funcionamiento realizadas, los cuales serán presentados a más tardar dentro del mes siguiente al vencimiento del plazo otorgado para su implementación. Los PRST deberán reportar, previo requerimiento de la CRC, los eventos de detección, las medidas de etiquetado aplicadas, las revisiones solicitadas por usuarios y las actualizaciones realizadas a sus listas DNO, conforme al requerimiento que expida la Comisión.

**2.1.10.7.3. Creación del Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles.** Créase el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, en adelante CTLFSM, como instancia de intercambio de alertas, identificación de patrones de fraude y espacio de revisión técnica de medidas frente al fraude cibernético a través de los servicios de voz móvil y mensajes cortos de texto (SMS). El CTLFSM será liderado y convocado por la CRC, con base en las reglas de funcionamiento y administración que se definen más adelante.

**2.1.10.7.3.1. Conformación.** El CTLFSM estará conformado por los siguientes participantes obligatorios:

- Por representantes de los PRST para las temáticas relacionadas con el fraude en los servicios tradicionales de voz y SMS, ya sea en el ecosistema P2P o A2P.

- Por los asignatarios de recursos de identificación denominado código corto A2P para las temáticas relacionadas con el fraude en el ecosistema A2P.

- La CRC, quién presidirá el Comité y ejercerá su secretaría técnica.

Podrán ser invitadas a participar en sesiones específicas, cuando los temas a tratar así lo requieran, entidades del orden nacional o territorial con competencias relacionadas con la prevención del fraude cibernético en servicios móviles, incluyendo el COLCERT, la Fiscalía General de la Nación, la Policía Nacional, la Superintendencia de Industria y Comercio y la Superintendencia Financiera de Colombia, o cualquier otra entidad estatal o privada según las necesidades de los temas a discutir. La participación de estas entidades como invitadas no tendrá carácter vinculante para ellas.

**2.1.10.7.3.2. Periodicidad y convocatoria.** El CTLFSM sesionará ordinariamente con una intensidad no inferior a cuatro sesiones al año. Las sesiones podrán ser presenciales o virtuales, según como lo determine la CRC en la respectiva convocatoria. La CRC podrá convocarlo de manera extraordinaria cuando se presenten incidentes de fraude en servicios móviles que requieran atención urgente o cuando las circunstancias del ecosistema así lo demanden. Los participantes obligatorios podrán igualmente solicitar a la CRC la convocatoria a sesión extraordinaria cuando lo consideren necesario, pero será potestativo de la CRC acceder a la referida convocatoria.

**2.1.10.7.3.3. Información a intercambiar.** En el marco del CTLFSM, los PRST y los asignatarios de código corto A2P, según corresponda, presentarán la información estandarizada que la CRC defina mediante requerimiento de información (en la convocatoria a la sesión), en los formatos y con la periodicidad que esta establezca.

La CRC podrá requerir adicionalmente la presentación de estadísticas consolidadas, por ejemplo, discriminadas por tipo de anomalía, tipo de métrica o PRST emisor, con el propósito de construir una visión nacional agregada de los patrones de fraude.

En ningún caso se compartirá, en el marco del CTLFSM, información comercialmente sensible entre competidores, ni información que contenga datos personales de usuarios.

**2.1.10.7.3.4. Vinculatoriedad.** En el marco del CTLFSM los participantes podrán proponer y acordar mejoras en la implementación de las medidas mínimas establecidas en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016, cuando la evolución de las modalidades de fraude así lo requieran. En caso de que no haya propuestas o acuerdos de mejoras, aplicarán los estándares mínimos establecidos en el mencionado artículo. Las decisiones del CTLFSM sobre tales parámetros serán de cumplimiento obligatorio para los PRST en los términos y plazos establecidos en la respectiva acta de sesión y, de identificarse necesario, en la resolución por medio de la cual se incorporen actualizaciones a la regulación general, la cual será expedida por el Director Ejecutivo de la Comisión de Regulación de Comunicaciones, previa aprobación del Comité de Comisionados de Comunicaciones de la CRC. La vinculatoriedad de estas decisiones deriva de la obligación regulatoria de participar en el CTLFSM. Las decisiones del CTLFSM no podrán, en ningún caso, desmejorar, degradar, modificar o derogar los parámetros técnicos mínimos establecidos en el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016.

**2.1.10.7.3.5. Requerimiento de información y sanciones.** En el marco del CTLFSM, la CRC hará uso de su facultad de requerir a los agentes obligados información amplia, exacta, veraz y oportuna sobre los temas objeto del Comité. En caso de incumplimiento de los requerimientos realizados, la CRC podrá imponer las multas a que haya lugar conforme al numeral 19 del artículo 22 de la Ley 1341 de 2009.

**2.1.10.7.3.6. Adaptación regulatoria.** Los resultados y actas del CTLFSM servirán a la CRC como insumo técnico para la actualización de cualquier medida contenida en la Resolución CRC 5050 de 2016 que tenga como finalidad la lucha o prevención contra el fraude en materia de servicios tradicionales de voz o SMS. Los resultados y actas del CTLFSM no son vinculantes para la CRC, pero sí para sus miembros en los términos definidos en el artículo 2.1.10.7.3.4. de esta resolución.

**2.1.10.7.3.7. Presidencia.** La Presidencia del CTLFSM será ejercida por el Comisionado de la Sesión de Comunicaciones de la CRC que tiene la calidad de ingeniero, en los términos del numeral 20.2 del artículo 20 de la Ley 1341 de 2009, o por quien este designe.

**2.1.10.7.3.8. Secretaría.** La Secretaría del CTLFSM será ejercida por el funcionario de la Comisión de Regulación de Comunicaciones que haga las veces de Coordinador del Grupo Interno de Trabajo de Relaciones con Grupos de Valor o por el servidor en quien se delegue esta función por parte del Comité de Comunicaciones de la CRC, y tendrá a su cargo la convocatoria a las sesiones, la remisión de la documentación pertinente, el levantamiento de actas, el registro y control de la documentación generada y la información de contacto de los miembros.

**2.1.10.7.3.9. Representación.** Cada miembro obligado participará en el CTLFSM a través de un representante con facultades suficientes para asumir en su nombre las obligaciones derivadas de las determinaciones técnicas adoptadas en el Comité. Cada miembro designará un

representante principal y un suplente, e informará a la Secretaría cualquier cambio en dicha designación dentro de los cinco (5) días hábiles siguientes a que se produzca.

**2.1.10.7.3.10. Convocatoria.** La Secretaría convocará las sesiones ordinarias y extraordinarias mediante comunicación escrita o correo electrónico dirigida a los representantes de los miembros obligados y, cuando sea el caso, a los invitados, con antelación mínima de cinco (5) días hábiles para las sesiones ordinarias y de dos (2) días hábiles para las sesiones extraordinarias. La convocatoria incluirá el orden del día, el requerimiento de la información que cada participante deberá presentar ante la CRC y la documentación que será analizada en la sesión.

**2.1.10.7.3.11. Quórum y votación.** Las sesiones del CTLFSM se realizarán válidamente con la asistencia de la mayoría simple de los miembros obligados. La Secretaría del CTLFSM identificará e informará la cantidad y calidad de los miembros obligados a participar en el CTLFSM. Cada miembro obligado tendrá derecho a un voto, con independencia de su tamaño o participación de mercado. Las determinaciones técnicas y operativas se adoptarán por mayoría simple de los miembros presentes. En caso de empate, la CRC tendrá voto dirimente. Los votos de abstención se contabilizarán únicamente para registro.

**2.1.10.7.3.12. Actas.** De cada sesión se levantará un acta en la que constarán como mínimo la fecha, hora y lugar, los asistentes, el orden del día, los temas tratados, las determinaciones adoptadas con indicación del resultado de la votación cuando corresponda, y los compromisos asumidos por cada miembro con sus respectivos plazos. Las actas serán publicadas en la página web de la CRC dentro de los diez (10) días hábiles siguientes a la sesión, salvo la información que tenga carácter confidencial o reservado, la cual se mantendrá en archivo independiente. Las actas serán firmadas por el Presidente y el Secretario del CTLFSM. Las decisiones del CTLFSM no serán vinculantes para la CRC ni afectarán sus competencias en materia de regulación. Por el contrario, estas decisiones serán un insumo técnico, no vinculante, que la CRC tendrá en cuenta para efectos de modificar su regulación en caso de que haya lugar y previo al respectivo Análisis de Impacto Normativo (AIN).

**2.1.10.7.3.13. Mesas de trabajo.** La Presidencia podrá proponer al CTLFSM la conformación de mesas de trabajo técnico o jurídico para el análisis de temas específicos. Las mesas de trabajo tendrán carácter temporal, estarán integradas por los representantes técnicos que cada miembro designe para el efecto, y presentarán sus conclusiones al pleno del CTLFSM en la sesión que la Presidencia determine. Las conclusiones de las mesas de trabajo tendrán carácter de propuesta y no serán vinculantes.

**2.1.10.7.3.14. Confidencialidad.** La información presentada por los miembros en el marco del CTLFSM tendrá carácter reservado frente a terceros no participantes, salvo que la CRC determine su publicación por razones de transparencia regulatoria. Los participantes no podrán utilizar la información conocida en el marco del CTLFSM para fines distintos a los del Comité ni divulgarla a terceros sin autorización expresa de la CRC.

**2.1.10.7.3.15. Ingreso de nuevos miembros.** Cuando un nuevo agente adquiera la calidad de PRST o de asignatario de código corto A2P con posterioridad a la constitución del CTLFSM, al mismo tiempo adquirirá la obligación de ser parte del CTLFSM. Por lo tanto, dicho agente deberá designar su representante y suplente dentro de los treinta (30) días hábiles siguientes al día en el que adquirió esa calidad.

**2.1.10.7.3.16. Vigencia del CTLFSM.** El CTLFSM estará constituido de manera permanente. La CRC podrá, mediante acto administrativo, ampliar, restringir o modificar sus funciones, composición o reglas de funcionamiento cuando las circunstancias regulatorias así lo requieran.

**PARÁGRAFO.** Cualquier incumplimiento a las disposiciones establecidas en el artículo 2.1.10.7. dará lugar a que la CRC realice el respectivo traslado a la SIC o al MinTIC para el ejercicio de sus funciones de vigilancia y control de conformidad con sus respectivas competencias.

**ARTÍCULO 4.** Modificar el artículo 2.1.18.1. de la Resolución CRC 5050 de 2016, el cual quedará así:

**«ARTÍCULO 2.1.18.1. ACCESO AL REGISTRO DE NÚMEROS EXCLUIDOS.** Toda persona que no desee ser contactada mediante mensajes publicitarios o comerciales enviados a través de SMS, aplicaciones o web o correo electrónico, ni mediante llamadas telefónicas de carácter

comercial o publicitario, podrá inscribirse en el Registro de Números Excluidos (RNE), el cual es administrado por la CRC. Quienes se inscriban en el RNE podrán solicitar, en cualquier momento y de forma gratuita, que su inscripción sea eliminada del registro. La inscripción o eliminación al registro se hará efectiva a partir del día hábil siguiente.

La inscripción en el RNE no se referirá a los contactos que tengan como finalidad informar al consumidor sobre la confirmación oportuna de las operaciones monetarias realizadas, sobre ahorros voluntarios y cesantías, enviar información solicitada por el consumidor o generar alertas sobre transacciones fraudulentas, inusuales o sospechosas.

Los productores y proveedores de bienes y servicios podrán acceder al RNE para efectos de conocer si los consumidores o usuarios a quienes pretenden contactar para fines comerciales o publicitarios se encuentran inscritos en él o no.

Aquellos productores y proveedores de bienes y servicios que se encuentran inscritos en el RNE para conocer la información de los consumidores o usuarios que pretenden contactar podrán solicitar a la CRC que certifique la inscripción efectiva mediante una constancia escrita.

**PARÁGRAFO**. La Superintendencia de Industria y Comercio (SIC), en el marco de sus competencias y, en especial, en virtud de la facultad prevista en el artículo 9 de la Ley 2300 de 2023, podrá solicitar a la CRC cualquier tipo de información relacionada con los trámites administrativos de recuperación de recursos de identificación establecidos en el TÍTULO VI de la Resolución CRC 5050 de 2016, con la finalidad de que sirvan de insumo para las investigaciones que la SIC adelanta relacionadas con el RNE. La SIC podrá solicitar información al validador centralizado, una vez esté operativo el funcionamiento de este tercero, con la finalidad de recabar insumos y pruebas que sirvan para las investigaciones que la SIC adelanta relacionada con el RNE».

**ARTÍCULO 5.** Adicionar los numerales 4.1.2.6.4 y 4.1.2.6.5 al artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV de la Resolución CRC 5050 de 2016, así:

«**ARTÍCULO 4.1.2.6. OPOSICIÓN A LA INTERCONEXIÓN**. Los proveedores de redes y servicios de telecomunicaciones sólo podrán negarse u oponerse a otorgar la interconexión solicitada cuando demuestren fundada y razonablemente ante la CRC, en un plazo no mayor de quince (15) días calendario, contados a partir de la respectiva solicitud, que la interconexión causaría alguno de las siguientes consecuencias:

(...)

**4.1.2.6.4.** Que el hecho de acceder a la solicitud implique otorgarle acceso a un asignatario de códigos cortos, ya sea PCA o IT, respecto del cual la CRC había autorizado la desconexión en el año inmediatamente anterior a la fecha de la solicitud de acceso, en los términos del parágrafo 4 del artículo 6.1.1.8 de la Resolución CRC 5050 de 2016. Si la solicitud de acceso es presentada una vez haya transcurrido más de un año, desde la fecha de ejecutoria del acto administrativo que autorizó la referida desconexión, esta causal de oposición no podrá alegarse.

**4.1.2.6.5**. Que el hecho de acceder a la solicitud implique otorgarle acceso a un asignatario de códigos cortos, ya sea PCA o IT, respecto del cual la CRC había autorizado la desconexión en los términos del parágrafo No. 4 del artículo 6.1.1.8 de la Resolución CRC 5050 de 2016, y que el referido asignatario no haya tomado las medidas suficientes para prevenir el envío de mensajes de contenido fraudulento por medio de los códigos cortos a él asignados y las medidas necesarias para demostrar que no volverá a incurrir en las causales de recuperación de códigos cortos que motivaron la referida autorización de desconexión. En el evento en el que el PRST alegue esta causal, la Comisión le otorgará al PCA/IT asignatario la oportunidad para que, en el respectivo trámite administrativo, demuestre lo contrario.

El proveedor de redes y servicios de telecomunicaciones que se niegue a otorgar la interconexión está obligado a presentar, en su argumentación ante la CRC, las alternativas para evitar los daños alegados y los responsables sugeridos para adelantar tales acciones.

En caso de no llegarse a un acuerdo entre las partes afectadas, estas podrán acudir ante la CRC para iniciar un trámite administrativo de solución de controversias sobre los puntos en desacuerdo. Lo resuelto por la CRC será de obligatorio acatamiento por las partes, sin perjuicio de las acciones que puedan iniciarse ante otras autoridades y de las sanciones por incumplimientos regulatorios a que haya lugar.»

**ARTÍCULO 6.** Modificar el artículo 6.1.1.5. de la Resolución CRC 5050 de 2016, el cual quedará así:

**"ARTÍCULO 6.1.1.5. ASIGNACIÓN DE RECURSOS DE IDENTIFICACIÓN.** El Administrador de los Recursos de Identificación, asignará, de oficio o a petición de los solicitantes, recursos de identificación para lo cual tendrá en cuenta las atribuciones definidas para cada recurso que se encuentren registradas en el SIGRI.

La asignación de los recursos de identificación no genera costo, por lo que los asignatarios no podrán cobrar remuneración alguna a sus usuarios por efectos de la asignación y utilización correspondiente.

**PARÁGRAFO.** Los recursos de identificación no pueden ser objeto de venta o comercialización. Tampoco pueden ser cedidos o transferidos, excepto cuando el Administrador de los Recursos de Identificación lo autorice de manera expresa, de oficio o a solicitud de parte, para lo cual el nuevo asignatario deberá cumplir los requisitos de asignación correspondientes. En el caso de emitirse una autorización expresa de cesión o transferencia de los derechos de uso de los recursos de identificación, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos. El recurso de identificación llamado código corto, regulado en el Capítulo 4 del TÍTULO VI de esta resolución, no puede ser objeto de venta, comercialización, cesión o transferencia.

**ARTÍCULO 7.** Modificar el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la Resolución CRC 5050 de 2016, el cual quedará así:

**"ARTÍCULO 6.1.1.6. OBLIGACIONES**. Las obligaciones del Administrador de los Recursos de Identificación y de los asignatarios de esos recursos son las siguientes:

(…)

**6.1.1.6.2. OBLIGACIONES GENERALES DE LOS ASIGNATARIOS DE LOS RECURSOS DE IDENTIFICACIÓN.**

**6.1.1.6.2.1.** Demostrar que los recursos de identificación se usan eficientemente según la solicitud y la consecuente asignación por parte de la Comisión.

**6.1.1.6.2.2.** Utilizar el recurso de identificación en la forma y aplicación específica para la que le ha sido asignado.

**6.1.1.6.2.3.** No vender ni comercializar los recursos de identificación. Tampoco cederlos ni transferirlos hasta que no se tenga la autorización del Administrador de los Recursos de Identificación. El recurso de identificación llamado código corto, regulado en el Capítulo 4 del TÍTULO VI de esta resolución, no puede ser objeto de venta, comercialización, cesión o transferencia.

**6.1.1.6.2.4.** Implementar las acciones necesarias para garantizar el máximo aprovechamiento de cada recurso de identificación asignado, de acuerdo con los criterios de uso eficiente establecidos para tal fin.

**6.1.1.6.2.5.** Facilitar la información de manera veraz, completa y oportuna que sea solicitada por el Administrador de los Recursos de Identificación.

**6.1.1.6.2.6.** Tramitar su inscripción en el portal de trámites de la CRC o aquel sistema que lo sustituya, como requisito administrativo para la asignación de los recursos de identificación.

**6.1.1.6.2.7.** Mantener actualizada su información en el portal de trámites de la CRC o aquel sistema que lo sustituya. Cuando el asignatario deje de prestar sus servicios, se recuperen o se acepte la devolución de todos los recursos de identificación que le sean asignados, deberá cancelar el registro realizado en portal de trámites de la CRC, sin perjuicio de que esta Entidad conserve los datos para el ejercicio de sus funciones.

**6.1.1.6.2.8.** Implementar los recursos de identificación asignados dentro del término establecido para el efecto, el cual será contado a partir de la ejecutoria del acto administrativo de asignación.

**6.1.1.6.2.9.** Tener en cuenta los estados de los recursos de identificación registrados en el SIGRI. En el mismo sentido, los PRST deberán considerar ese estado al momento de la implementación de los recursos de identificación en sus redes, de tal forma que se garantice que estos se encuentren en estado de asignación. En todo caso, los recursos de identificación que hayan sido recuperados o se encuentren en estado disponible no podrán estar implementados en la red de los PRST, para lo cual el asignatario deberá informar a los PRST lo correspondiente, una vez la decisión de recuperación se encuentre ejecutoriada.

**6.1.1.6.2.10.** Devolver de manera oportuna aquellos recursos que ya no use o no necesite, en concordancia con los criterios de uso eficiente definidos.

**6.1.1.6.2.11.** Usar herramientas y mecanismos que resulten necesarios para garantizar que los recursos de identificación se utilizan conforme fueron asignados.

**6.1.1.6.2.12.** El asignatario de un código corto deberá contar con la autorización expresa y por escrito del tercero que lo autoriza, cuando los recursos de identificación sean utilizados para enviar contenido en nombre de esos terceros.

**6.1.1.6.2.13.** En el evento en que un PCA asignatario de un código corto pretenda cambiar su integrador tecnológico para un código corto asignado, deberá informar previamente a la CRC para efectos de modificar las condiciones de asignación iniciales.

**6.1.1.6.2.14.** Los asignatarios que estén obligados a contar con matrícula mercantil en los términos del Código de Comercio deberán mantenerla debidamente actualizada en los términos ordenados por el artículo 33 del Código de Comercio. De no estar actualizada la CRC puede recuperar los recursos de identificación que tenga esa sociedad asignada.

**6.1.1.6.2.15.** Mantener actualizada su información en el RPCAI en los términos del numeral 4.2.3.2 de esta resolución.

**ARTÍCULO 8.** Modificar el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016, el cual quedará así:

**"ARTÍCULO 6.1.1.8. RECUPERACIÓN DE LOS RECURSOS DE IDENTIFICACIÓN**. Cuando el Administrador de los Recursos de Identificación, mediante los mecanismos de verificación de uso diseñados para tal fin, detecte la presunta configuración de alguna de las causales de recuperación establecidas o el presunto uso ineficiente de algún recurso de identificación asignado, adelantará el procedimiento de recuperación establecido en este artículo, teniendo en cuenta lo establecido en el Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA) para las actuaciones administrativas.

**6.1.1.8.1.** El Administrador de los Recursos de Identificación remitirá un oficio de apertura de actuación administrativa de recuperación al asignatario donde justifique las razones por las cuales se ha identificado el presunto uso ineficiente del recurso, especificando expresamente las faltas a los criterios de uso eficiente o las causales de recuperación en las que está incurriendo, con el objeto de garantizar el derecho a la defensa y al debido proceso.

Este oficio de apertura de la actuación administrativa de recuperación será publicado por la CRC en un micrositio contenido en su página web al que tendrá acceso cualquier persona, con la

finalidad de garantizar los escenarios contemplados en el artículo 38 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (CPACA).

La persona que acredite ante la CRC un interés directo e individual en la actuación administrativa tendrá el carácter de tercero interesado y podrá, dentro de los cinco (5) días hábiles posteriores a la publicación del oficio de apertura de la actuación administrativa de recuperación en la página web de la CRC, intervenir aportando las consideraciones y pruebas que pretendan hacer valer para que la CRC las tenga en cuenta al momento de decidir. La CRC resolverá de plano la solicitud del tercero, ya sea para reconocer su participación en la actuación o negarla, y contra esta decisión no procederá recurso alguno.

La CRC dará traslado al asignatario de los documentos y pruebas aportadas por los terceros mediante documento en el que también fijará un término para que los asignatarios se pronuncien sobre lo aportado.

**6.1.1.8.2.** Una vez obtenida la respuesta del asignatario, esta será analizada por el Administrador de los Recursos de Identificación. Se podrá solicitar la información adicional que se considere necesaria para constatar si procede o no la recuperación del recurso.

**6.1.1.8.3.** En caso de proceder la recuperación, se expedirá y notificará la respectiva resolución de recuperación de los recursos de identificación contemplados en el inicio de la actuación administrativa particular. En la decisión se contemplará el establecimiento de tiempos en estado de reserva en el caso que el Administrador de los Recursos de Identificación los considere aplicables. La decisión de recuperación se informará a todos los PRST para que procedan con la desactivación de ese recurso en su red, según corresponda.

**6.1.1.8.4.** Una vez en firme el acto administrativo particular de recuperación, se registrarán las respectivas modificaciones de estado de los recursos recuperados en el SIGRI.

**PARÁGRAFO 1o.** En el evento de que pueda haber usuarios afectados por la recuperación de algún recurso de identificación, el Administrador de los Recursos de Identificación otorgará un plazo para la transición, que no podrá ser menor a seis (6) meses ni superior a un (1) año, para adelantar las gestiones relativas a la migración y la publicidad a dichos usuarios. Pasado este plazo, los recursos recuperados podrán ser puestos en estado «reservado» por el periodo que considere adecuado el Administrador de los Recursos de Identificación antes de pasar a estado «disponible», con el objeto de minimizar posibles riesgos a la hora de una nueva implementación.

**PARÁGRAFO 2o.** El procedimiento de recuperación previsto en este artículo no se aplicará cuando el asignatario manifieste en forma expresa que no utiliza los recursos de identificación asignados. En este caso, la CRC analizará la situación manifestada por el asignatario y de, considerarlo pertinente, expedirá una resolución que cambie el estado del recurso de identificación de «asignado» a «disponible» en el SIGRI.

**PARÁGRAFO 3o.** En las actuaciones administrativas de recuperación de códigos cortos iniciadas por las causales señaladas en los numerales 6.4.3.2.2., 6.4.3.2.8. y 6.4.3.2.9. del artículo 6.4.3.2. de la presente resolución, la CRC podrá ordenar, en el acto de apertura de la actuación administrativa, o en cualquier estado del trámite administrativo, la suspensión temporal del uso del recurso de identificación. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses. Para los recursos de identificación código corto A2P y SENDER ID, la suspensión temporal se regirá por los parágrafos 2 de los artículos 6.4.3.2 y 6.12.3.2 de la presente resolución, respectivamente.

**PARÁGRAFO 4o**. Los PRST podrán suspender provisionalmente la relación de acceso con los PCA/IT que sean asignatarios de recursos de identificación, en aquellos casos en que a estos agentes la CRC les haya recuperado por segunda vez un código corto por las causales contenidas en los numerales 6.4.3.2.2., 6.4.3.2.8 y 6.4.3.2.9. del artículo 6.4.3.2 de la Resolución CRC 5050 de 2016. En este escenario, los PRST podrán suspender por un mes dicha relación de acceso en forma unilateral, para lo cual deberán informar tanto a la CRC como a la SIC sobre las medidas adoptadas para minimizar los efectos de tal suspensión en los usuarios.

Una vez superado el referido periodo de suspensión, y en el escenario en el que la CRC recupere por tercera vez un código corto por las causales indicadas en este parágrafo, los PRST podrán solicitar a la CRC la autorización para la terminación definitiva de la relación de acceso vigente

con los PCA/IT que sean asignatarios de recursos de identificación, en el marco de un trámite administrativo de desconexión definitiva ante la CRC con el fin de que esta Comisión autorice tal terminación.

Esta medida tiene efectos hacía futuro desde la fecha de publicación en el Diario Oficial de la resolución por medio de la cual se adoptó. Por lo tanto, los actos administrativos de recuperación de códigos cortos que se tendrán en cuenta para efectos de aplicar las consecuencias descritas en este parágrafo serán aquellos expedidos por la CRC con posterioridad a la adopción de esta medida».

**ARTÍCULO 9.** Modificar el artículo 6.4.2.1. de la Resolución CRC 5050 de 2016, el cual quedará así:

«**ARTÍCULO 6.4.2.1. REQUISITOS PARA LA ASIGNACIÓN DE NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD**. Para solicitar numeración de códigos cortos, el solicitante debe remitir al Administrador de los Recursos de Identificación, a través del trámite unificado de recursos de identificación dispuesto para tal fin, la siguiente información:

**6.4.2.1.1.** Constancia de inscripción previa en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI), en la que conste la actividad que desarrollará una vez le sean asignados los códigos cortos.

**6.4.2.1.2.** Código corto solicitado, el cual debe solicitarse teniendo en cuenta las diferentes modalidades del servicio, de conformidad con el artículo 6.4.1.2. o aquel que lo modifique o sustituya, y según la disponibilidad del recurso en el momento de la solicitud de acuerdo con la información del SIGRI.

**6.4.2.1.3.** Descripción detallada del servicio que se prestará a través del código corto solicitado donde se especifique, como mínimo, lo siguiente:

i) La indicación de si se trata de un contenido o aplicación.

ii) La descripción del contenido o de aplicación a ofrecer al usuario, con base en la categoría del contenido y las actividades operativas específicas asociadas a la prestación del servicio, lo que deberá incluir la identificación del origen del mensaje y los mecanismos que permiten su trazabilidad a lo largo del flujo de comunicación hasta la notificación al usuario final.

iii) El procedimiento de interacción con el usuario.

iv) La forma de pago prevista, en caso de que no sea un servicio gratuito.

v) Informar en detalle las medidas de control y herramientas tecnológicas que serán empleadas por parte del asignatario y su integrador tecnológico (según aplique) para prevenir fraudes o usos indebidos a través del envío de mensajes SMS o USSD mediante los códigos cortos solicitados, precisando su aplicación según la modalidad o categoría correspondiente.

**6.4.2.1.4.** En caso de contar con códigos cortos previamente asignados para la misma modalidad de servicio de la solicitud, el estado de implementación de tales códigos, detallando el tráfico, los ingresos y los usuarios haciendo uso del Formato T.5.2 del Título Reportes de Información.

**6.4.2.1.5.** Justificación detallada de la necesidad del código corto solicitado y el propósito específico del uso del código, así como cualquier otra información que el solicitante considere necesaria, pertinente y útil para soportar la solicitud de asignación.

**6.4.2.1.6.** Razón social y NIT del integrador tecnológico, si el solicitante soporta sus servicios en uno de ellos. Si el solicitante es un integrador tecnológico, deberá informarlo de forma expresa.

**6.4.2.1.7.** Certificado de existencia y representación legal vigente del solicitante, expedido con no más de noventa (90) días, en el que conste que la matricula legal está vigente.

Además, certificado de existencia y representación legal vigente del integrador tecnológico, en caso de aplicar.

**6.4.2.1.8**. Declaración suscrita por el representante legal y, en caso de aplicar, por el revisor fiscal, en la que manifiesten quienes son los accionistas de la persona jurídica solicitante del recurso de identificación. Esta declaración deberá ser presentada para solicitar la asignación del respectivo recurso de identificación y, para aquellos asignatarios que ya cuenten con recursos asignados, estarán obligados a presentarla dentro de los treinta días hábiles siguientes a la fecha de adopción de esta medida.

**ARTÍCULO 10.** Modificar el artículo 6.4.3.1. de la Resolución CRC 5050 de 2016, el cual quedará así:

**"ARTÍCULO 6.4.3.1. CRITERIOS DE USO EFICIENTE.** El Administrador de los Recursos de Identificación verificará el uso eficiente de la numeración de códigos cortos para SMS y USSD asignada, en observancia de los siguientes criterios:

**6.4.3.1.1.** Los asignatarios deberán dar pleno cumplimiento a las obligaciones generales definidas en el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la presente resolución.

**6.4.3.1.2.** Los códigos cortos asignados deben ser implementados en un término máximo de seis (6) meses contados a partir de la firmeza del acto administrativo de asignación.

**6.4.3.1.3.** Los códigos cortos implementados no deberán reportar ausencia de tráfico en periodos consecutivos iguales o superiores a seis (6) meses.

**6.4.3.1.4.** Los códigos cortos implementados no deberán reportar tráfico para un único usuario por un periodo superior a tres (3) meses.

**ARTÍCULO 11.** Modificar el artículo 6.4.3.2. de la Resolución CRC 5050 de 2016, el cual quedará así:

**"ARTÍCULO 6.4.3.2. CAUSALES DE RECUPERACIÓN DE LA NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD.** El Administrador de los Recursos de Identificación podrá recuperar total o parcialmente la numeración de códigos cortos para SMS y USSD asignada conforme el procedimiento de recuperación establecido en el artículo 6.1.1.8. de la presente resolución, cuando el asignatario incumpla con alguno de los criterios de uso eficiente establecidos en el artículo 6.4.3.1. de la presente resolución, o incurra en alguna de las siguientes causales de recuperación:

**6.4.3.2.1.** Cuando el asignatario incumpla alguna de las obligaciones generales definidas en el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la presente resolución.

**6.4.3.2.2.** Cuando los códigos cortos asignados presenten un uso diferente a aquél para el que fueron asignados.

**6.4.3.2.3.** Cuando los códigos cortos no hayan sido implementados dentro de los seis (6) meses siguientes a la fecha de la asignación.

**6.4.3.2.4.** Cuando no se reporte tráfico asociado al código corto durante un periodo de seis (6) meses.

**6.4.3.2.5.** Cuando se reporte tráfico de un código corto asociado a un único usuario, en un periodo igual o superior a tres (3) meses.

**6.4.3.2.6.** Cuando existan razones de interés general o seguridad nacional que justifiquen la recuperación.

**6.4.3.2.7.** Cuando el Administrador de los Recursos de Identificación modifique una modalidad de servicio asociada a un determinado conjunto de códigos cortos.

**6.4.3.2.8.** Cuando a través de esta numeración se envíen mensajes en nombre de terceros que no hayan autorizado expresamente y por escrito su envío o su contenido.

**6.4.3.2.9.** Cuando a través de códigos cortos se envíen mensajes a usuarios inscritos en el RNE cuyo envío no haya sido autorizado expresamente por el usuario.

**6.4.3.2.10.** Cuando con ocasión de la utilización de códigos cortos se establezca mediante decisión ejecutoriada de autoridad competente el incumplimiento de disposiciones en materia de protección de datos personales.

**6.4.3.2.11.** Cuando el asignatario se encuentra en la imposibilidad para continuar ejerciendo su objeto social, por ejemplo, pero sin limitarse a ello, cuando entra en estado de liquidación judicial o voluntaria.»

**ARTÍCULO 12.** Subróguese el Capítulo 4 del TÍTULO VI — Régimen de Administración de Recursos de Identificación — de la Resolución CRC 5050 de 2016 a partir del vencimiento del período de transición establecido en el artículo 19 de la presente resolución. A partir de ese momento, el Capítulo 4 del TÍTULO VI quedará así:

«**CAPÍTULO 4**
**CÓDIGO CORTO PARA SERVICIOS DE MENSAJERÍA A2P**

**SECCIÓN 1.**
**PLANIFICACIÓN Y FUNCIONAMIENTO DEL CÓDIGO CORTO A2P**

**ARTÍCULO 6.4.1.1. NATURALEZA DEL CÓDIGO CORTO A2P.** El código corto A2P es el recurso de identificación administrado por la CRC que identifica de manera exclusiva e individual a cada agente que, en virtud de una relación contractual con un PRST, tiene conexión directa con este para cursar tráfico A2P de mensajería de texto (SMS). A través de un único código corto A2P, el asignatario cursará el tráfico A2P de todas las personas naturales o jurídicas vinculadas a él mediante el recurso de identificación denominado SENDER ID.

**ARTÍCULO 6.4.1.2. ESTRUCTURA DEL CÓDIGO CORTO A2P.** El código corto A2P se compone por cadenas de 5 y 6 dígitos que identifican de manera única al agente asignatario.

**ARTÍCULO 6.4.1.3. ASIGNATARIOS DEL CÓDIGO CORTO A2P.** Podrán solicitar y ser asignatarios de un código corto A2P los agentes que, en virtud de una relación contractual con un PRST, tienen conexión directa con este para cursar el tráfico de mensajería A2P. Estos agentes pueden ser integradores tecnológicos o PCA que cuenten con dicha conexión directa. También podrán ser asignatarios los PRST que lo requieran para soportar sus servicios, en su calidad de integrador tecnológico.

**PARÁGRAFO 1.** Los PCA con conexión directa al PRST que sean a su vez responsables directos por la producción y generación de sus propios contenidos o aplicaciones deberán ser asignatarios tanto de código corto A2P como de SENDER ID. En este caso, el agente podrá presentar directamente la solicitud de asignación del SENDER ID sin intermediación de un tercero.

**PARÁGRAFO 2.** Los agentes que únicamente provean infraestructura de conexión para cursar el tráfico de mensajería de terceros, sin ser responsables directos por la producción del contenido, serán integradores tecnológicos asignatarios únicamente de código corto A2P.

**ARTÍCULO 6.4.1.4. UNICIDAD DEL CÓDIGO CORTO A2P.** Cada solicitante tendrá derecho a la asignación de un único código corto A2P, el cual lo identificará de manera inequívoca en el ecosistema de mensajería A2P. Un mismo agente no podrá ser titular de más de un código corto A2P asignado simultáneamente.

**SECCIÓN 2.**
**ASIGNACIÓN DEL CÓDIGO CORTO A2P**

**ARTÍCULO 6.4.2.1. REQUISITOS PARA LA ASIGNACIÓN DEL CÓDIGO CORTO A2P**. Para solicitar la asignación de un código corto A2P, el solicitante deberá remitir al Administrador de los Recursos de Identificación, a través del trámite unificado de recursos de identificación, la siguiente información:

**6.4.2.1.1.** Constancia de inscripción previa en el RPCAI, con indicación de si actúa en calidad de PCA con conexión directa al PRST o de integrador tecnológico.

**6.4.2.1.2.** Código corto A2P solicitado, de conformidad con la estructura del artículo 6.4.1.2 y la disponibilidad en el SIGRI.

**6.4.2.1.3.** Descripción detallada del servicio o función que desempeñará como asignatario del código corto A2P, que incluya como mínimo la descripción de la infraestructura técnica de conexión con el o los PRST, y la identificación de los PRST con quienes mantendrá o mantiene relaciones de acceso.

**6.4.2.1.4.** Justificación detallada de la necesidad del código corto A2P solicitado.

**6.4.2.1.5.** Certificado de existencia y representación legal vigente, expedido con no más de noventa (90) días de anterioridad.

**6.4.2.1.6.** Copia del contrato de acceso suscrito con al menos un PRST, o declaración juramentada de que se encuentra en proceso de negociación y que presentará copia dentro de los treinta (30) días hábiles siguientes a la firmeza del acto de asignación. En este último caso, la asignación quedará condicionada a la presentación oportuna del contrato.

**6.4.2.1.7.** Certificación expedida por el validador centralizado, en los términos del Capítulo 13 del TÍTULO VI de esta resolución, en la que conste la verificación de la identidad del agente, su objeto social y el cumplimiento de los requisitos de debida diligencia.

**6.4.2.1.8.** Descripción en detalle de las medidas de control y herramientas tecnológicas para prevenir fraudes mediante los accesos a sus plataformas o herramientas para el envío de SMS, así como los mecanismos de trazabilidad del tráfico de mensajería A2P desde el asignatario de SENDER ID hasta la terminación en el usuario final.

**ARTÍCULO 6.4.2.2. PROCEDIMIENTO DE ASIGNACIÓN DEL CÓDIGO CORTO A2P.** Una vez presentada la solicitud conforme al artículo 6.4.2.1, el Administrador de los Recursos de Identificación resolverá en un término de quince (15) días hábiles conforme al siguiente procedimiento:

**6.4.2.2.1.** Se verificará que la solicitud cumpla con todos los requisitos del artículo 6.4.2.1. Si no los cumple, se negará la asignación.

**6.4.2.2.2.** Se verificará que el solicitante no tenga un código corto A2P previamente asignado en el SIGRI. Si existe uno previo asignado, se negará la asignación salvo solicitud simultánea de devolución del anterior.

**6.4.2.2.3.** Se verificarán que en el año inmediatamente anterior no se recuperó un código corto A2P del solicitante por las causales de los numerales 6.4.3.2.5. y 6.4.3.2.6. del artículo 6.4.3.2. Si hubo recuperación por esas causales, se negará la asignación.

**6.4.2.2.4.** Se llevará a cabo el análisis de las solicitudes según el orden de llegada.

**6.4.2.2.5.** Se verificará la consistencia entre la descripción del servicio, los mecanismos de trazabilidad y la certificación del validador centralizado.

**6.4.2.2.6.** Se verificará la disponibilidad y viabilidad en el SIGRI. Si se cumplen todos los requisitos, se cambiará el estado a «Preasignado».

**6.4.2.2.7.** Se expedirá el acto administrativo de asignación y cambio de estado a «Asignado» en el SIGRI, una vez quede en firme.

**PARÁGRAFO.** El término de quince (15) días hábiles se suspende cuando se requiera información adicional y se reanuda al recibo de la respuesta completa.

## SECCIÓN 3.
## USO DEL CÓDIGO CORTO A2P

**ARTÍCULO 6.4.3.1. CRITERIOS DE USO EFICIENTE.** El Administrador de los Recursos de Identificación verificará el uso eficiente del código corto A2P asignado en observancia de los siguientes criterios:

**6.4.3.1.1.** Cumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

**6.4.3.1.2.** Cumplimiento de las obligaciones especiales de los asignatarios de código corto A2P establecidas en el Capítulo 13 del TÍTULO VI.

**6.4.3.1.3.** El código corto A2P debe ser implementado en un término máximo de seis (6) meses desde la firmeza del acto de asignación. Se entiende implementado cuando el asignatario ha establecido la conexión técnica operativa con al menos un PRST y puede cursar tráfico de mensajería A2P.

**6.4.3.1.4.** El código corto A2P implementado no deberá reportar ausencia de tráfico en períodos consecutivos iguales o superiores a seis (6) meses, salvo suspensión temporal ordenada por el Administrador de los Recursos de Identificación.

**6.4.3.1.5.** El asignatario deberá mantener vigente en todo momento al menos una relación contractual de acceso con un PRST. La terminación de todas las relaciones sin devolución del recurso constituirá indicio de uso ineficiente.

**6.4.3.1.6.** El asignatario deberá mantener actualizada su información de contacto en el RPCAI y en la respectiva matrícula mercantil que proporciona información al RUES.

**6.4.3.1.7.** A través del código corto A2P únicamente podrá cursarse tráfico A2P de personas naturales o jurídicas que cuenten con un SENDER ID previamente asignado y vigente vinculado al mismo, respaldado por una plantilla de contenido aprobada y vigente en el sistema del validador centralizado.

**ARTÍCULO 6.4.3.2. CAUSALES DE RECUPERACIÓN DEL CÓDIGO CORTO A2P.** El Administrador de Recursos de Identificación podrá recuperar el código corto A2P conforme al artículo 6.1.1.8 cuando el asignatario incumpla los criterios del artículo 6.4.3.1 o incurra en las siguientes causales:

**6.4.3.2.1.** Incumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

**6.4.3.2.2.** Incumplimiento de las obligaciones especiales de los asignatarios de código corto A2P establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

**6.4.3.2.3.** No implementación dentro de los seis (6) meses siguientes a la firmeza del acto de asignación.

**6.4.3.2.4.** Ausencia de tráfico durante seis (6) meses consecutivos.

**6.4.3.2.5.** Envío de mensajes de texto (SMS) en nombre de personas naturales o jurídicas que no cuenten con SENDER ID asignado y vigente vinculado al código corto A2P, o envío de mensajes sin respaldo de plantilla de contenido previamente aprobada y vigente en el sistema del validador centralizado.

**6.4.3.2.6.** Envío de mensajes de texto (SMS) que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario del código corto A2P conforme al artículo 6.13.4.4 de la presente resolución.

**6.4.3.2.7.** No presentación del contrato de acceso con el PRST dentro del plazo del numeral 6.4.2.1.6 cuando la asignación quedó condicionada a ello.

**6.4.3.2.8.** Imposibilidad de continuar ejerciendo su objeto social, incluyendo liquidación judicial o voluntaria, o cancelación de matrícula mercantil.

**6.4.3.2.9.** Razones de interés general o seguridad nacional.

**6.4.3.2.10.** Establecimiento, mediante decisión ejecutoriada, de incumplimiento de disposiciones en materia de protección de datos personales o propiedad intelectual.

**PARÁGRAFO 1.** La recuperación del código corto A2P tiene efectos sobre todos los SENDER ID vinculados. Simultáneamente con la notificación del acto administrativo que ordena la recuperación del código corto A2P, el Administrador de Recursos de Identificación notificará a todos los asignatarios de SENDER ID vinculados, de conformidad con la información que el validador centralizado le proporcione a la CRC, otorgándoles a los asignatarios de SENDER ID treinta (30) días hábiles para acreditar una nueva relación comercial con un titular de un código corto A2P.

**PARÁGRAFO 2.** Cuando la causal de recuperación sea la del numeral 6.4.3.2.5 o la del numeral 6.4.3.2.6, la CRC podrá ordenar, en el acto de apertura de la actuación administrativa, o en cualquier estado de la actuación administrativa, la suspensión temporal del uso del recurso de identificación denominado código corto A2P. Dicha suspensión se mantendrá durante el trámite administrativo y no podrá exceder un plazo máximo de seis (6) meses».

**ARTÍCULO 13.** Adiciónese el Capítulo 12 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, en los siguientes términos:

«**CAPÍTULO 12**
**SENDER ID**

**SECCIÓN 1.**
**PLANIFICACIÓN Y FUNCIONAMIENTO DEL SENDER ID**

**ARTÍCULO 6.12.1.1. ESTRUCTURA DEL SENDER ID.** El SENDER ID para Colombia es un identificador alfanumérico visible para el usuario final en el encabezado del mensaje recibido. Tendrá una extensión mínima de tres (3) caracteres y máxima de once (11) caracteres alfanuméricos. El Administrador de los Recursos de Identificación mantendrá y publicará en el SIGRI una lista dinámica de los SENDER ID asignados, actualizada en tiempo real a medida que se produzcan nuevas asignaciones. Las denominaciones de SENDER ID sugeridas por los solicitantes podrán ser objeto de evaluación y eventual asignación, siempre que acrediten el cumplimiento de los requisitos técnicos, operativos y regulatorios aplicables que están contenidos en esta resolución.

**PARÁGRAFO.** El SENDER ID deberá tener relación de manera inequívoca con: (i) la razón social de la persona jurídica; o (ii) el nombre de la persona natural; o (iii) el nombre comercial; o (iv) la marca registrada del asignatario. No se admitirán identificadores que puedan inducir al usuario en error o confusión, que imiten nombres de entidades públicas, financieras u operadores de telecomunicaciones, ni que contengan palabras reservadas por el Administrador de Recursos de Identificación, las cuales serán publicadas y actualizada en el SIGRI de manera dinámica cuando la CRC lo estime necesario por vía de circular.

**ARTÍCULO 6.12.1.2. ASIGNATARIOS DEL SENDER ID.** Podrán solicitar y ser asignatarios de SENDER ID los agentes responsables directos por la producción y generación de contenidos o aplicaciones enviados a través de SMS y USSD. El asignatario del SENDER ID no será asignatario de código corto A2P, salvo la situación descrita en el Parágrafo 1 del artículo 6.4.1.3. También podrán ser asignatarios:

**6.12.1.2.1.** Los PCA e IT inscritos en el RPCAI, responsables directos por la producción de contenidos y/o aplicaciones propias.

**6.12.1.2.2.** Las entidades de la fuerza pública y organismos del Estado cuya función esté orientada a preservar el orden público, el orden constitucional y/o la administración de justicia.

**6.12.1.2.3.** Los PRST en su condición de PCA, cuando sean responsables directos por la producción de contenidos propios para sus usuarios.

**PARÁGRAFO 1.** Los agentes que únicamente provean infraestructura de conexión para cursar tráfico de mensajes de texto (SMS) de terceros no podrán ser asignatarios de SENDER ID.

**PARÁGRAFO 2.** A cada persona natural o jurídica le será asignado un único SENDER ID. La CRC solo asignará un SENDER ID por número de identificación tributaria (NIT) o por cédula de ciudadanía. No podrán existir dos asignatarios distintos con el mismo número de identificación, ni un mismo asignatario con más de un SENDER ID asignado simultáneamente. Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto.

**ARTÍCULO 6.12.1.3. MODALIDADES DE CONTENIDO QUE SE ASOCIAN AL SENDER ID.** Los SENDER ID podrán utilizarse para una o varias de las siguientes modalidades de contenido, conforme a las que el asignatario justifique al momento de la solicitud:

**6.12.1.3.1. MENSAJES DE AUTENTICACIÓN Y SEGURIDAD.** Son aquellos mensajes cortos de texto A2P destinados exclusivamente a verificar la identidad del usuario o proteger la seguridad de accesos y operaciones. Incluyen, entre otros, los códigos de verificación de un solo uso (OTP) enviados como parte de sistemas de autenticación multifactor, las alertas inmediatas de seguridad sobre inicios de sesión o actividades inusuales en una cuenta, y las confirmaciones de activación o desbloqueo de servicios por parte del usuario.

En virtud de su naturaleza, estos mensajes se generan normalmente a solicitud explícita del usuario o como parte intrínseca de un servicio contratado (por ejemplo, al iniciar sesión en una plataforma o autorizar una transacción sensible), por lo que su envío no requiere un consentimiento adicional expreso del usuario, entendiéndose amparado por la acción u operación que los origina y el vínculo servicio-usuario existente.

**6.12.1.3.2. MENSAJES TRANSACCIONALES E INFORMATIVOS.** Son los mensajes cortos de texto A2P vinculados a la prestación de un servicio, transacción o relación contractual en curso, cuyo contenido tiene carácter operativo o explicativo y está directamente asociado a acciones o eventos que el usuario espera.

Comprenden, por ejemplo, notificaciones de transacciones bancarias realizadas (avisos de débito o crédito en cuenta), confirmaciones de operaciones o solicitudes (como confirmación de una compra, de una reserva o de una cita), avisos de logística (seguimiento de envíos, entrega de paquetes), recordatorios de pago oportuno o vencimientos, así como otras comunicaciones de servicio al cliente (actualización de saldos, cambios de condiciones, mensajes de cobranza bajo un contrato vigente).

En estos casos, el consentimiento del usuario se entiende implícito o derivado de la relación contractual o la solicitud previa que soporta la comunicación, es decir, el usuario ha proporcionado su número dentro del contexto del servicio o transacción, autorizando estas notificaciones necesarias para la correcta ejecución del servicio.

**6.12.1.3.3. MENSAJES COMERCIALES O PUBLICITARIOS.** Son los mensajes cortos de texto A2P con fines de promoción, mercadeo o publicidad, dirigidos a ofrecer, difundir o incentivar la contratación de bienes, servicios, eventos o programas de fidelización a los usuarios finales.

Esta categoría incluye, por ejemplo, las campañas de publicidad o promociones enviadas por empresas (descuentos, anuncios de nuevos productos, invitaciones a eventos comerciales), los mensajes de mercadeo directo para la captación de clientes o ventas, las encuestas de satisfacción con carácter comercial, así como cualquier otra comunicación cuyo objetivo principal sea publicitario o de telemercadeo (fidelización, branding, posicionamiento de marca, etc.).

Dado su carácter no solicitado dentro de una transacción específica, estos mensajes requieren el consentimiento expreso previo del usuario (opt-in), otorgado de forma libre, específica e informada, para ser enviados de conformidad con la normativa de protección de datos y protección al usuario vigente. En particular, el remitente debe contar con una autorización clara del destinatario para recibir comunicaciones comerciales por este medio, y es responsable de respetar las preferencias del usuario sobre no recepción de publicidad en línea con las reglas de la inscripción del número que el usuario haya realizado en el Registro de Números Excluidos – RNE.

**6.12.1.3.4. MENSAJES REGULATORIOS Y DE INTERÉS PÚBLICO.** Son aquellos mensajes cortos de texto A2P cuyo envío responde a obligaciones legales, regulatorias o a finalidades de

interés general, y no tienen un propósito comercial ni obedecen a una solicitud individual del usuario sino al cumplimiento de un deber normativo o la protección del bienestar público.

Esta categoría abarca, entre otros, los mensajes exigidos por la regulación sectorial a los proveedores de servicios (por ejemplo, notificaciones que un operador móvil debe enviar obligatoriamente sobre activación de servicios, confirmación de recargas, consumos de datos o condiciones tarifarias, de acuerdo con la normativa vigente), las alertas oficiales de emergencia o gestión del riesgo emitidas por organismos gubernamentales (tales como avisos de desastres naturales, seguridad ciudadana o salud pública), las comunicaciones masivas de carácter institucional (por ejemplo, campañas de servicio público, información de beneficios sociales a poblaciones vulnerables) y, en general, las notificaciones institucionales o administrativas que las entidades públicas o privadas deban remitir a los usuarios en virtud de normas específicas.

Estos mensajes se emiten sin requerir consentimiento previo del usuario, ya que su envío está justificado en un mandato normativo expreso o en razones de interés público esencial. Por tanto, pueden enviarse incluso a usuarios que hayan manifestado su preferencia de no recibir comunicaciones comerciales, dado que no persiguen fines publicitarios sino el cumplimiento de un deber legal o la difusión de información relevante para la colectividad.

**PARÁGRAFO.** Un mismo SENDER ID podrá utilizarse para más de una modalidad siempre que exista una plantilla de contenido independiente aprobada por el validador centralizado para cada modalidad, y que el asignatario haya acreditado ante el validador el cumplimiento de las condiciones aplicables a cada una. El asignatario de SENDER ID podrá solicitar ante el Administrador de Recursos de Identificación la modificación de la asignación del respectivo recurso de identificación, con la finalidad de adicionar o eliminar modalidades de contenido asociadas al respectivo SENDER ID.

## SECCIÓN 2.
## ASIGNACIÓN DEL SENDER ID

**ARTÍCULO 6.12.2.1. REQUISITOS PARA LA ASIGNACIÓN DEL SENDER ID.** El asignatario del código corto A2P, vinculado al solicitante del SENDER ID, remitirá al Administrador de Recursos de Identificación, en nombre y representación del solicitante del SENDER ID, a través del trámite unificado de recursos de identificación, la siguiente información:

**6.12.2.1.1.** Constancia de inscripción previa del futuro asignatario del SENDER ID en el RPCAI como PCA. Los solicitantes extranjeros podrán ser asignatarios siempre que hayan establecido una sucursal en Colombia, en los términos de las disposiciones legales y reglamentarias previstas para el efecto.

**6.12.2.1.2.** Sugerencia del SENDER ID solicitado y que requiere ser asignado, con indicación detallada de la modalidad o modalidades de contenido para las cuales se solicita su uso, con la justificación de cada una de ellas.

**6.12.2.1.3.** Soporte del derecho al uso del identificador alfanumérico mediante alguno de los siguientes documentos: certificado de registro de marca ante la SIC; certificado de existencia y representación legal que acredite que la razón social o nombre comercial corresponde al identificador solicitado; matrícula mercantil y, para el caso de personas naturales, cédula de ciudadanía. Para entidades del numeral 6.12.1.2.2. de esta resolución, el acto de creación o acto que acredite su denominación oficial.

**6.12.2.1.4.** Descripción del servicio o servicios a prestar por cada modalidad solicitada, incluyendo: indicación de si es contenido, aplicación o ambos; descripción del contenido y propósito de cada tipo de comunicación; procedimiento de interacción con el usuario y mecanismo de obtención del consentimiento por modalidad; forma de pago si no es gratuito; y medidas de control para prevenir fraudes.

**6.12.2.1.5.** Identificación del código corto A2P del agente solicitante, con acreditación de que está asignado e implementado en el SIGRI y que existe contrato vigente entre el asignatario del código corto A2P y el potencial asignatario del SENDER ID.

**6.12.2.1.6.** Certificado de existencia y representación legal vigente del asignatario del código corto A2P, expedido con no más de noventa (90) días.

**6.12.2.1.7.** Certificado de existencia y representación legal vigente del potencial asignatario del SENDER ID, expedido con no más de noventa (90) días, en caso de que se trate de una persona jurídica.

**6.12.2.1.8.** Certificación del validador centralizado conforme al Capítulo 13 del Título VI de esta resolución, en la que conste el cumplimiento del KYC por parte del asignatario del código corto A2P respecto del potencial asignatario del SENDER ID, la acreditación del contrato vigente y la validación de la información comercial y técnica del servicio por cada modalidad solicitada.

**6.12.2.1.9.** Cualquier otra información que el solicitante considere pertinente.

**PARÁGRAFO 1.** Cuando el asignatario del SENDER ID sea a su vez asignatario de código corto A2P conforme al Parágrafo 1 del artículo 6.4.1.3, podrá presentar directamente la solicitud adaptando los requisitos.

**PARÁGRAFO 2.** Para las entidades del numeral 6.12.1.2.2. de esta resolución, el requisito de inscripción en el RPCAI no es exigible y podrán presentar directamente la solicitud ante el Administrador de Recursos de Identificación.

**ARTÍCULO 6.12.2.2. PROCEDIMIENTO DE ASIGNACIÓN DEL SENDER ID.** Una vez presentada la solicitud conforme al artículo 6.12.2.1, el Administrador de Recursos de Identificación resolverá en quince (15) días hábiles conforme al siguiente procedimiento:

**6.12.2.2.1.** Se verificará que la solicitud cumpla con todos los requisitos del artículo 6.12.2.1. Si no los cumple, se negará la asignación.

**6.12.2.2.2.** Se verificará que el código corto A2P está asignado e implementado, y que el contrato entre el asignatario del código corto A2P y el potencial asignatario del SENDER ID está vigente.

**6.12.2.2.3.** Se verificará que en el año anterior no se recuperó al potencial asignatario un SENDER ID por los numerales 6.12.3.2.5., 6.12.3.2.6., 6.12.3.2.7. o 6.12.3.2.12. del artículo 6.12.3.2. Si hubo recuperación por esas causales, se negará la asignación.

**6.12.2.2.4.** Se verificará que el identificador alfanumérico no corresponde a uno ya asignado en el SIGRI, ni a una denominación engañosa conforme al Parágrafo del artículo 6.12.1.1. En caso de homonimia total se negará. En caso de similitud, que a juicio de la CRC pueda ser considerada engañosa o confusa, se requerirá un identificador alternativo.

**6.12.2.2.5.** Se verificará que el solicitante no cuenta con un SENDER ID asignado en el SIGRI bajo el mismo número de identificación tributaria (NIT) o cédula de ciudadanía. Si existe un SENDER ID asignado para ese número de identificación, se negará la asignación.

**6.12.2.2.6.** Se verificará que la descripción del servicio es consistente con la modalidad o modalidades de contenido solicitadas y con la justificación presentada conforme al numeral 6.12.2.1.2. de esta resolución.

**6.12.2.2.7.** Se llevará a cabo el análisis de las solicitudes según orden de llegada y justificación presentada.

**6.12.2.2.8.** Se verificará la disponibilidad en el SIGRI del SENDER ID solicitado. Si se cumplen todos los requisitos, el estado del SENDER ID solicitado pasará a «Preasignado».

**6.12.2.2.9.** Cumplidos los pasos anteriores, se procederá con la expedición del acto administrativo de asignación y se cambiará el estado del SENDER ID a «Asignado» en el SIGRI, una vez quede en firme dicho acto administrativo.

**PARÁGRAFO.** El término de quince (15) días hábiles se suspende cuando se requiera información adicional o cuando se requiera al solicitante proponer un identificador alternativo.

## SECCIÓN 3.
## USO DEL SENDER ID

**ARTÍCULO 6.12.3.1. CRITERIOS DE USO EFICIENTE.** El Administrador de Recursos de Identificación verificará el uso eficiente del SENDER ID en observancia de los siguientes criterios:

**6.12.3.1.1.** Cumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6. de esta resolución.

**6.12.3.1.2.** Cumplimiento de las obligaciones especiales del asignatario del SENDER ID establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

**6.12.3.1.3.** El SENDER ID debe ser implementado en un término máximo de seis (6) meses desde la firmeza del acto de asignación.

**6.12.3.1.4.** El SENDER ID implementado no deberá reportar ausencia de tráfico en períodos consecutivos iguales o superiores a seis (6) meses.

**6.12.3.1.5.** El asignatario deberá mantener vigente en todo momento al menos una relación contractual con un asignatario de código corto A2P con conexión directa operativa a un PRST, salvo que él mismo sea el asignatario de código corto A2P.

**6.12.3.1.6.** A través del SENDER ID únicamente podrán enviarse mensajes correspondientes a las modalidades para las que fue asignado conforme a la solicitud del artículo 6.12.2.1.2. de esta resolución, respaldados por una plantilla previamente aprobada y vigente en el sistema del validador centralizado.

**6.12.3.1.7.** A través del SENDER ID no podrán enviarse mensajes en nombre de terceros distintos al asignatario.

**6.12.3.1.8.** El asignatario deberá mantener actualizada su información en el RPCAI y en la respectiva matrícula mercantil que proporciona información al RUES.

**6.12.3.1.9.** El asignatario deberá completar la validación anual ante el validador centralizado conforme al artículo 6.12.3.3 de la presente resolución. El incumplimiento de esta obligación dentro del plazo establecido constituirá un uso ineficiente y dará lugar al inicio del procedimiento de recuperación conforme al artículo 6.1.1.8. de esta resolución.

**ARTÍCULO 6.12.3.2. CAUSALES DE RECUPERACIÓN DEL SENDER ID.** El Administrador de Recursos de Identificación podrá recuperar el SENDER ID conforme al artículo 6.1.1.8 cuando el asignatario incumpla los criterios del artículo 6.12.3.1 o incurra en las siguientes causales:

**6.12.3.2.1.** Incumplimiento de las obligaciones generales del numeral 6.1.1.6.2. del artículo 6.1.1.6.

**6.12.3.2.2.** Incumplimiento de las obligaciones especiales del asignatario del SENDER ID establecidas en el Capítulo 13 del TÍTULO VI de esta resolución.

**6.12.3.2.3.** No implementación dentro de los seis (6) meses siguientes a la firmeza del acto de asignación.

**6.12.3.2.4.** Ausencia de tráfico durante seis (6) meses consecutivos.

**6.12.3.2.5.** Uso diferente al declarado al momento de la solicitud, incluyendo mensajes cuyo contenido no corresponda a ninguna modalidad para la que fue solicitado el SENDER ID conforme al numeral 6.12.2.1.2, o sin respaldo de plantilla aprobada y vigente.

**6.12.3.2.6.** Envío de mensajes en nombre de terceros distintos al asignatario.

**6.12.3.2.7.** Envío de mensajes a usuarios inscritos en el RNE cuyo envío no haya sido autorizado conforme a la modalidad de contenido de la plantilla previamente aprobada.

**6.12.3.2.8.** Establecimiento, mediante decisión ejecutoriada, de incumplimiento de disposiciones en materia de protección de datos personales o propiedad intelectual.

**6.12.3.2.9.** Imposibilidad de continuar ejerciendo su objeto social, incluyendo liquidación judicial o voluntaria, o cancelación de matrícula mercantil.

**6.12.3.2.10.** Razones de interés general o seguridad nacional.

**6.12.3.2.11.** Modificación, por parte del Administrador de Recursos de Identificación, de una modalidad de contenido que haga incompatible el uso del SENDER ID para dicha modalidad.

**6.12.3.2.12.** Envío de mensajes de texto (SMS) que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario del SENDER ID conforme al artículo 6.13.4.4 de la presente resolución.

**6.12.3.2.13.** Incumplimiento injustificado de la validación anual establecida en el artículo 6.12.3.3. de esta resolución dentro del plazo establecido para su realización.

**PARÁGRAFO 1.** La recuperación del SENDER ID genera efectos sobre todas las plantillas activas vinculadas al mismo. Simultáneamente con el inicio del procedimiento, cuando la causal de recuperación sea la de los numerales 6.12.3.2.5., 6.12.3.2.6., 6.12.3.2.7. o 6.12.3.2.12. del artículo 6.12.3.2, la CRC podrá ordenar al validador centralizado la suspensión inmediata de todas las plantillas activas vinculadas al SENDER ID. Una vez en firme el acto de recuperación, todas las plantillas asociadas deberán quedar desactivadas y no se podrán enviar mensajes mediante dicho SENDER ID.

**PARÁGRAFO 2.** La recuperación del SENDER ID no implica automáticamente la recuperación del código corto A2P, salvo que el motivo configure también una causal de recuperación del código corto A2P.

**ARTÍCULO 6.12.3.3. VALIDACIÓN ANUAL DEL SENDER ID.** El asignatario del SENDER ID deberá completar una validación anual ante el validador centralizado para mantener vigente el derecho al uso del recurso. Esta validación se realizará dentro de los treinta (30) días hábiles anteriores al vencimiento de cada año contado desde la firmeza del acto de asignación o desde la última validación exitosa. La validación anual comprende como mínimo:

**6.12.3.3.1.** Confirmación de la vigencia de la relación contractual con el asignatario del código corto A2P.

**6.12.3.3.2.** Actualización de la información del KYC conforme al artículo 6.13.3.2 de la presente resolución.

**6.12.3.3.3.** Revisión y confirmación o actualización de las modalidades de contenido para las cuales se utiliza el SENDER ID, con acreditación del cumplimiento de las condiciones aplicables a cada una.

**6.12.3.3.4.** Confirmación de que las plantillas activas vinculadas al SENDER ID corresponden a las comunicaciones efectivamente enviadas, con actualización o desactivación de aquellas que ya no se utilicen.

**PARÁGRAFO**. Si el asignatario no completa la validación dentro del plazo establecido, el validador centralizado notificará al Administrador de los Recursos de Identificación, quien iniciará el procedimiento de recuperación conforme al artículo 6.1.1.8. de esta resolución».

**ARTÍCULO 14.** Adiciónese el Capítulo 13 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, en los siguientes términos:

**«CAPÍTULO 13**
**REGLAS COMUNES A LOS RECURSOS DE IDENTIFICACIÓN DENOMINADOS CÓDIGO CORTO A2P Y SENDER ID**

**SECCIÓN 1.**
**VALIDADOR CENTRALIZADO**

**ARTÍCULO 6.13.1.1. NATURALEZA Y FUNCIÓN DEL VALIDADOR CENTRALIZADO.** El validador centralizado es la persona jurídica seleccionada por los PRSTM, que tiene a su cargo la administración, gestión e integridad del proceso de validación de los agentes, marcas y plantillas de contenido que participan en el ecosistema de tráfico de mensajería A2P. El validador centralizado garantiza que únicamente los agentes que hayan acreditado su legitimidad y el cumplimiento de los requisitos de debida diligencia puedan acceder a los recursos de identificación denominados código corto A2P y SENDER ID, y que únicamente los mensajes cortos de texto, asociados a las plantillas aprobadas conforme al presente capítulo, puedan ser entregados a los usuarios finales.

El validador centralizado no tiene competencias de Administrador de los Recursos de Identificación ni actúa en nombre de la CRC. Sus funciones son de naturaleza técnica, operativa y de verificación documental, y se circunscriben a los lineamientos regulatorios establecidos en el presente capítulo y en los actos administrativos que para el efecto expida el Administrador de los Recursos de Identificación. Las decisiones de asignación, recuperación y devolución de los recursos de identificación son competencia exclusiva de la CRC en su calidad de Administrador de Recursos de Identificación.

**ARTÍCULO 6.13.1.2. FINANCIAMIENTO DEL VALIDADOR CENTRALIZADO.** Los costos de implementación, gestión, operación y mantenimiento del validador centralizado serán remunerados por parte de los asignatarios de código corto A2P en favor de la persona jurídica que sea seleccionada como validador centralizado, aplicando el principio de orientación a costos más utilidad razonable.

El pago de la tarifa o tarifas acordadas será incorporado al contrato de operación que suscribirá cada asignatario de código corto A2P con el validador centralizado.

La tarifa o tarifas deberán reflejar los costos reales de operación, incluyendo infraestructura tecnológica, personal, garantías y sistemas de seguridad.

La tarifa podrá ser diferenciada según el volumen de tráfico A2P cursado por cada asignatario de código corto A2P o la cantidad de SENDER ID vinculados a su infraestructura, o cualquier otro criterio objetivo acordado, siempre que no genere discriminación injustificada entre los asignatarios de código corto A2P.

**ARTÍCULO 6.13.1.3. REQUISITOS DEL VALIDADOR CENTRALIZADO.** Para ser seleccionado, el candidato deberá acreditar como mínimo:

**6.13.1.3.1.** Ser persona jurídica legalmente constituida en Colombia o con sucursal establecida en el país conforme a las disposiciones legales y reglamentarias vigentes.

**6.13.1.3.2.** Contar con capacidad técnica y operativa suficiente para administrar en tiempo real el proceso de validación de agentes, marcas y plantillas de contenido en los volúmenes del ecosistema A2P nacional, incluyendo disponibilidad de sistemas de información, las interfaces de acceso y la infraestructura de seguridad.

**6.13.1.3.3.** Acreditar experiencia previa en la administración de sistemas de registro y validación de identidades en el sector de telecomunicaciones o sectores afines, o demostrar capacidad técnica equivalente mediante los estudios, certificaciones y referencias que puedan presentar.

**6.13.1.3.4.** No tener vínculos accionarios, contractuales o de control con ninguno de los asignatarios de código corto A2P ni con sus matrices, filiales o subordinadas, que puedan comprometer su independencia e imparcialidad. Tampoco podrá tener vínculos accionarios, contractuales o de control con ninguno de los PRSTM ni con sus matrices, filiales o subordinadas, que puedan comprometer su independencia e imparcialidad. En el marco del proceso de selección, el candidato presentará declaración juramentada de ausencia de conflictos de interés, acompañada de certificación del representante legal con la estructura de propiedad y control hasta el nivel del beneficiario final.

**6.13.1.3.5.** Contar con mecanismos robustos de seguridad de la información que garanticen la confidencialidad, integridad y disponibilidad de los datos de los agentes registrados, conforme a los estándares internacionales aplicables y a las disposiciones de la Ley 1581 de 2012 y sus normas reglamentarias.

**ARTÍCULO 6.13.1.4. VIGENCIA Y CAUSALES DE TERMINACIÓN.** La selección de validador centralizado tendrá una vigencia de cinco (5) años. Un año antes del vencimiento de ese plazo, los PRSTM, con acompañamiento de la CRC, adelantarán un nuevo proceso de selección con antelación suficiente para garantizar la continuidad sin interrupciones, ya sea para ratificar al mismo validador centralizado o votar por cambiarlo.

Son causales de revisión anticipada de la decisión de selección las siguientes:

**6.13.1.4.1.** El incumplimiento grave o reiterado de las obligaciones establecidas en el presente capítulo o en los respectivos contratos.

**6.13.1.4.2.** La pérdida sobreviniente de alguno de los requisitos del numeral 6.13.1.3. de esta resolución, incluyendo la configuración de un conflicto de interés que comprometa la imparcialidad en el ejercicio de sus funciones.

**6.13.1.4.3.** La solicitud voluntaria del validador centralizado de dar por terminadas sus funciones, presentada con antelación mínima de un año ante la CRC, la cual tendrá que ser justificada.

**6.13.1.4.4.** La imposibilidad sobreviniente de continuar ejerciendo sus funciones, incluyendo los casos de liquidación judicial o voluntaria, o la cancelación o suspensión de su matrícula mercantil por autoridad competente.

**PARÁGRAFO.** En los casos de revisión anticipada que conduzca a la selección de un nuevo validador, o cuando los PRSTM decidan no continuar con el validador actual, el validador saliente garantizará la transferencia ordenada de toda la información, los sistemas y los procesos al nuevo validador o a la CRC, en los términos y plazos que la CRC establezca, con plena observancia de las disposiciones aplicables en materia de protección de datos personales.

**ARTÍCULO 6.13.1.5. FUNCIONES DEL VALIDADOR CENTRALIZADO.** Son funciones del validador centralizado:

**6.13.1.5.1.** Recibir, revisar y procesar las solicitudes de registro de los agentes que pretendan ser asignatarios de código corto A2P o SENDER ID, verificando el cumplimiento de los requisitos de debida diligencia establecidos en el presente capítulo.

**6.13.1.5.2.** Adelantar el proceso de KYC respecto de los potenciales asignatarios de código corto A2P conforme a la Sección 3 del presente capítulo.

**6.13.1.5.3.** Verificar que los asignatarios de código corto A2P hayan adelantado el proceso de KYC respecto de los potenciales asignatarios de SENDER ID conforme a la Sección 3 del presente capítulo.

**6.13.1.5.4.** Recibir, revisar y aprobar o rechazar las plantillas de contenido A2P que los asignatarios de SENDER ID sometan a su consideración conforme a la Sección 4 del presente capítulo. La revisión implica la validación del contenido estático y el sentido del contenido dinámico de la plantilla, para que corresponda con la modalidad declarada de los mensajes.

**6.13.1.5.5.** Expedir las certificaciones requeridas en los procesos de asignación de código corto A2P y SENDER ID conforme a los artículos 6.4.2.1.7. y 6.12.2.1.8. de la presente resolución.

**6.13.1.5.6.** Mantener actualizado el registro de los agentes, marcas y plantillas de contenido validadas, con indicación del estado de cada una y del historial de novedades, en los sistemas de información del validador, con base en la información que aparece en el SIGRI y de conformidad con la ejecución de las actividades del validador centralizado.

**6.13.1.5.7.** Reportar al Administrador de Recursos de Identificación de manera inmediata sobre cualquier indicio de uso indebido de los recursos de identificación, o la existencia de tráfico potencialmente engañoso, o de incumplimiento de las obligaciones de los asignatarios detectado en el ejercicio de sus funciones.

**6.13.1.5.8.** Mantener listas dinámicas de URLs y dominios utilizados para actividades que incumplen el régimen de recursos de identificación y ponerlas a disposición de los PRST y de los asignatarios de código corto A2P a través de las interfaces definidas para el efecto.

**6.13.1.5.9.** Atender los requerimientos de información que le formule el Administrador de Recursos de Identificación dentro de los plazos que este establezca.

**6.13.1.5.10.** Garantizar la disponibilidad permanente del servicio de consulta en tiempo real del estado de los agentes y plantillas registrados, para efectos de que los PRST puedan verificar la validez de los recursos de identificación y de las plantillas antes del enrutamiento de cada mensaje corto de texto en el ecosistema A2P.

**6.13.1.5.11.** Participar en el Comité Técnico de Seguimiento previsto en la Sección 5 del presente capítulo y en los espacios de coordinación que convoque el Administrador de Recursos de Identificación.

**6.13.1.5.12.** Ejecutar el proceso de validación anual del SENDER ID previsto en el artículo 6.12.3.3 de la presente resolución, emitiendo las certificaciones de validación correspondientes y notificando al Administrador de Recursos de Identificación los casos de incumplimiento.

**ARTÍCULO 6.13.1.6. PROHIBICIONES DEL VALIDADOR CENTRALIZADO.** El validador centralizado tiene las siguientes prohibiciones en el ejercicio de sus funciones:

**6.13.1.6.1.** Compartir, divulgar o comercializar la información de los agentes registrados con terceros distintos del Administrador de los Recursos de Identificación o de las autoridades judiciales o administrativas competentes que la requieran mediante orden escrita motivada.

**6.13.1.6.2.** Otorgar certificaciones sin haber completado el proceso de verificación documental y de KYC, o expedir certificaciones con información falsa, incompleta o inconsistente.

**6.13.1.6.3.** Establecer vínculos contractuales, accionarios o de control con los agentes que registra y valida, o recibir contraprestaciones distintas a la tarifa o tarifas pactadas en el contrato.

**6.13.1.6.4.** Delegar en terceros las funciones de verificación documental y de KYC sin autorización expresa del Administrador de los Recursos de Identificación.

**6.13.1.6.5.** Negar injustificadamente o retardar el procesamiento de solicitudes de registro, de aprobación de plantillas o de expedición de certificaciones que cumplan con los requisitos establecidos en el presente capítulo.

## SECCIÓN 2.
## REQUERIMIENTOS TÉCNICOS Y OPERATIVOS DEL SISTEMA DE VALIDACIÓN

**ARTÍCULO 6.13.2.1. SISTEMA DE INFORMACIÓN DEL VALIDADOR CENTRALIZADO.** El validador centralizado deberá disponer de un sistema de información que cumpla como mínimo con las siguientes condiciones técnicas y operativas:

**6.13.2.1.1. Disponibilidad.** El sistema deberá operar con una disponibilidad mínima del noventa y nueve coma cinco por ciento (99,5%) mensual, medida en ventanas de treinta (30) días calendario. Las ventanas de mantenimiento programado deberán ser notificadas al Administrador de Recursos de Identificación y a los PRST con antelación mínima de setenta y dos (72) horas y no podrán realizarse en horarios de alta demanda de tráfico A2P.

**6.13.2.1.2. Capacidad de procesamiento.** El sistema deberá tener capacidad suficiente para procesar en tiempo real el volumen de consultas concurrentes del tráfico A2P nacional, con tiempos de respuesta máximos de doscientos (200) milisegundos promedio en condiciones normales y de quinientos (500) milisegundos en condiciones de alta demanda. El validador presentará al Administrador de Recursos de Identificación, con periodicidad semestral, un informe de capacidad del sistema que demuestre el cumplimiento de estos parámetros y proyecte la capacidad necesaria para los doce (12) meses siguientes.

**6.13.2.1.3. Interfaces de programación de aplicaciones (APIs).** El sistema deberá disponer de APIs seguras y estandarizadas para la integración con los sistemas de los PRST, los

asignatarios de código corto A2P y el SIGRI del Administrador de Recursos de Identificación. Las APIs deberán implementar mecanismos de autenticación robusta, cifrado mediante protocolos vigentes y trazabilidad completa de las transacciones realizadas.

**6.13.2.1.4. Seguridad de la información.** El sistema deberá implementar como mínimo: autenticación multifactor para el acceso administrativo; cifrado de extremo a extremo para la transmisión de datos sensibles; registros de auditoría completos e inmutables de todas las operaciones; mecanismos de detección y respuesta ante incidentes de seguridad; y planes de continuidad del negocio y recuperación ante desastres con tiempos de recuperación compatibles con las exigencias de disponibilidad del servicio. Los registros de auditoría deberán conservarse por un período mínimo de cinco (5) años y contar con mecanismos de integridad criptográfica verificable.

**6.13.2.1.5. Redundancia y continuidad operativa.** El sistema deberá operar sobre infraestructura redundante y contar con mecanismos automáticos de recuperación y conmutación ante fallas, a fin de evitar puntos únicos de falla y garantizar la continuidad de la validación del tráfico A2P nacional.

**ARTÍCULO 6.13.2.2. PLAN DE CONTINGENCIA.** El validador dispondrá de un plan de contingencia que establezca los mecanismos alternos de validación para casos de falla total o parcial del sistema principal, garantizando continuidad operativa y la trazabilidad de las operaciones realizadas durante la contingencia. El plan deberá incluir como mínimo:

**6.13.2.2.1.** Listas de emergencia de los agentes y plantillas validadas, disponibles para consulta offline por parte de los PRST durante el tiempo que dure la falla.

**6.13.2.2.2.** Procedimientos de escalamiento y tiempos máximos de resolución para diferentes tipos de fallas, diferenciando entre fallas parciales y fallas totales del sistema y eventos de degradación del servicio, así como los tiempos máximos de recuperación y restablecimiento de la operación.

**6.13.2.2.3.** Canales de comunicación alternativos para la notificación de fallas al Administrador de Recursos de Identificación, a los PRST y a los asignatarios de código corto A2P, con tiempos máximos de notificación no superiores a treinta (30) minutos desde la detección de la falla.

**6.13.2.2.4.** Mecanismos de sincronización para garantizar que las actualizaciones realizadas durante el período de contingencia sean incorporadas al sistema principal una vez restablecida la operación normal.

**6.13.2.2.5** Procedimientos para la activación, gestión y finalización del estado de contingencia, incluyendo la identificación de los responsables autorizados para declarar el inicio y terminación de la contingencia.

**6.13.2.2.6.** Mecanismos de continuidad operativa que permitan a los PRST cursar únicamente tráfico asociado a registros previamente validados y sincronizados antes de la activación de la contingencia.

**6.13.2.2.7.** Ejercicios de prueba y validación del plan de contingencia, que deberán realizarse como mínimo una (1) vez cada seis (6) meses, dejando evidencia documental de los resultados, incidentes identificados y acciones correctivas implementadas.

## SECCIÓN 3.
## PROCESO DE CONOCIMIENTO DEL CLIENTE (KYC)

**ARTÍCULO 6.13.3.1. OBLIGACIONES DE DEBIDA DILIGENCIA DE LOS ASIGNATARIOS DE CÓDIGO CORTO A2P.** Los asignatarios del código corto A2P adelantarán el proceso de conocimiento del cliente (KYC) respecto de cada agente con quien celebren contratos para cursar tráfico A2P, con carácter previo al inicio de la relación contractual y de manera continua durante su vigencia. Este proceso es condición necesaria para que el validador centralizado pueda expedir la certificación requerida para la asignación del SENDER ID conforme al artículo 6.12.2.1.8. de la presente resolución.

El proceso de KYC comprende como mínimo las siguientes obligaciones:

**6.13.3.1.1. Identificación del agente.** Verificación de la identidad de la persona natural o jurídica contratante mediante revisión de: certificado de existencia y representación legal con vigencia no superior a noventa (90) días; documento de identidad del representante legal y demás firmantes del contrato; RUT actualizado; y constancia de inscripción en el RPCAI cuando corresponda.

**6.13.3.1.2. Identificación del beneficiario final.** Identificación de la persona natural que en última instancia ejerce el control sobre la persona jurídica contratante. El potencial asignatario del SENDER ID diligenciará el formato de declaración de beneficiario final que disponga el validador centralizado, el cual será elaborado por este con base en criterios de identificación del beneficiario en materia de prevención del lavado de activos y financiación del terrorismo.

**6.13.3.1.3. Verificación del objeto social.** Verificación de que el objeto social del agente contratante es compatible con el tipo de contenido que pretende cursar a través del SENDER ID solicitado, y que las actividades comerciales declaradas son coherentes con el volumen y la modalidad de tráfico que se pretende generar.

**6.13.3.1.4. Acreditación del derecho al uso del identificador alfanumérico.** Verificación de que el agente contratante acredita el derecho al uso de la denominación comercial, marca, razón social o nombre que pretende registrar como SENDER ID, conforme a los documentos del numeral 6.12.2.1.3. del artículo 6.12.2.1. de la presente resolución.

**6.13.3.1.5. Evaluación del perfil de riesgo.** Evaluación del perfil de riesgo del agente contratante considerando como mínimo: historial de cumplimiento regulatorio en el sector de telecomunicaciones, incluyendo antecedentes de recuperación de recursos de identificación por la CRC; naturaleza del contenido que pretende cursar y su coherencia con el objeto social declarado; volumen de tráfico proyectado y su razonabilidad; y existencia de sanciones, investigaciones o procesos administrativos y/o judiciales en curso relacionados con fraudes a través de servicios de telecomunicaciones.

**6.13.3.1.6. Formalización contractual.** Celebración de contrato escrito con el agente contratante que establezca expresamente: la obligación del asignatario del SENDER ID de usar el recurso exclusivamente para los fines declarados y aprobados; la obligación de cursar tráfico únicamente a través de plantillas aprobadas y vigentes en el sistema del validador; la obligación de respetar el régimen de consentimiento del usuario por modalidad de contenido; la facultad del asignatario del código corto A2P de suspender el curso de tráfico de manera inmediata ante indicios de uso fraudulento y de reportar dicha suspensión al validador y al Administrador de Recursos de Identificación; y las consecuencias contractuales por incumplimiento, incluyendo la terminación del contrato por reincidencia.

**6.13.3.1.7. Conservación de la información.** Conservación de la totalidad de la información del KYC durante la vigencia de la relación contractual y por un período mínimo de cinco (5) años contados a partir de la terminación del contrato. Esta información deberá suministrarse al validador y al Administrador de Recursos de Identificación cuando sea requerida.

**ARTÍCULO 6.13.3.2. DEBIDA DILIGENCIA CONTINUA.** El proceso de KYC no se agota con la verificación inicial. Los asignatarios del código corto A2P adelantarán debida diligencia continua durante toda la vigencia de la relación contractual, que incluya como mínimo:

**6.13.3.2.1.** Actualización anual de la información del agente contratante, con verificación de la vigencia de los documentos presentados, del mantenimiento de las condiciones de elegibilidad y de la ausencia de nuevos factores de riesgo.

**6.13.3.2.2.** Monitoreo del tráfico cursado a través de los SENDER ID del agente contratante, conforme a los parámetros de la Sección 4 del presente capítulo, con el propósito de detectar patrones anómalos indicativos de uso fraudulento.

**6.13.3.2.3.** Revisión de las plantillas de contenido activas del agente contratante, para verificar que el contenido cursado corresponde a las plantillas aprobadas.

**6.13.3.2.4.** Reporte inmediato al validador y al Administrador de Recursos de Identificación de cualquier novedad relevante en la situación jurídica, financiera o comercial del agente contratante

que pueda afectar su elegibilidad como asignatario del SENDER ID o el correcto uso del recurso de identificación.

## SECCIÓN 4.
## RÉGIMEN DE PLANTILLAS DE CONTENIDO A2P Y OBLIGACIONES DE LOS ACTORES

**ARTÍCULO 6.13.4.1. NATURALEZA Y FUNCIÓN DE LAS PLANTILLAS DE CONTENIDO A2P.** Las plantillas de contenido A2P son autorizaciones técnicas del validador centralizado que condicionan el envío de tráfico A2P por parte de los asignatarios del SENDER ID.

La aprobación de una plantilla por el validador centralizado es condición necesaria e indispensable para que el asignatario del SENDER ID pueda cursar tráfico A2P. Ningún mensaje A2P podrá ser enrutado por los PRST si no está respaldado por una plantilla aprobada y vigente en el sistema del validador, conforme a las obligaciones del artículo 6.13.4.7. de la presente resolución.

El mal uso de una plantilla aprobada genera consecuencias sobre los recursos de identificación código corto A2P y SENDER ID a través de los cuales se cursó el tráfico indebido, conforme a las causales de recuperación de los artículos 6.4.3.2.6. y 6.12.3.2.12 de esta resolución y a las reglas de atribución de responsabilidad del artículo 6.13.4.4 de la presente resolución.

**ARTÍCULO 6.13.4.2. INFORMACIÓN QUE CONTENDRÁN LAS PLANTILLAS DE CONTENIDO A2P.** Toda plantilla sometida a aprobación del validador centralizado deberá contemplar como mínimo la siguiente información:

**6.13.4.2.1.** Identificación del SENDER ID al que se vinculará la plantilla, acreditando que se encuentra asignado e implementado en el SIGRI.

**6.13.4.2.2.** Identificación del código corto A2P del agente que gestiona la solicitud en nombre del asignatario del SENDER ID, con acreditación de la relación contractual vigente.

**6.13.4.2.3.** Declaración de la modalidad de contenido aplicable conforme a las categorías del artículo 6.12.1.3. de esta resolución, con la justificación correspondiente y la indicación del tipo de consentimiento del usuario aplicable.

**6.13.4.2.4.** Texto base del mensaje de texto (SMS), con indicación expresa de los campos variables permitidos y la descripción del tipo de información que podrá insertarse en dichos campos.

**6.13.4.2.5.** Indicación de si el mensaje incluye URLs o dominios y, en caso afirmativo, especificación de cada URL o dominio autorizado, incluyendo los casos de enlaces acortados con indicación del dominio original.

**6.13.4.2.6.** Declaración expresa de que el contenido de la plantilla no es engañoso, no suplanta identidades de terceros no autorizados y no induce al usuario en error.

**6.13.4.2.7.** Para las plantillas de modalidad de autenticación y seguridad y de mensajes transaccionales e informativos cuando involucren entidades del sector financiero, acreditación de que el asignatario del SENDER ID es entidad sometida a inspección de la Superintendencia Financiera o que cuenta con autorización expresa del Administrador.

**6.13.4.2.8.** Para las plantillas de modalidad regulatoria y de interés público, acreditación de la habilitación de la autoridad competente o de la calidad de entidad pública del asignatario del SENDER ID.

**ARTÍCULO 6.13.4.3. PROCEDIMIENTO DE APROBACIÓN, MODIFICACIÓN, VIGENCIA Y DESACTIVACIÓN DE PLANTILLAS.**

**6.13.4.3.1. Procedimiento de aprobación**. El validador recibirá las solicitudes de aprobación presentadas por los asignatarios del código corto A2P en nombre de los asignatarios del SENDER ID y las resolverá conforme al siguiente procedimiento:

(i) verificará que la solicitud cumple todos los requisitos del artículo 6.13.4.2; si no los cumple, la rechazará mediante comunicación motivada, como máximo, dentro de las veinticuatro (24) horas siguientes a su recibo;

(ii) verificará que el contenido de la plantilla es coherente con la modalidad de contenido declarada y con el tipo de consentimiento indicado;

(iii) verificará que las URLs o dominios incluidos no figuren en las listas dinámicas del numeral 6.13.1.5.8. de esta resolución y que no presenten indicadores objetivos de actividad potencialmente engañosa;

(iv) verificará que el identificador alfanumérico del SENDER ID vinculado a la plantilla es consistente con el contenido del mensaje y no induce al usuario en error;

(v) si la plantilla cumple todos los requisitos, la aprobará y le asignará un código de identificación interno dentro de las cuarenta y ocho (48) horas siguientes al recibo de la solicitud completa;

(vi) si no cumple los requisitos de los literales ii), iii) o iv), la rechazará mediante comunicación motivada dentro de las mismas cuarenta y ocho (48) horas.

**PARÁGRAFO 1.** Los tiempos de respuesta son máximos. El validador establecerá en su reglamento interno objetivos de tiempo promedio compatibles con los ciclos operativos del ecosistema A2P.

**PARÁGRAFO 2.** El validador no podrá rechazar una plantilla por razones distintas a las establecidas en el presente numeral. Salvo que el rechazo sea consecuencia de actividad potencialmente engañosa, caso en el cual el validador reportará al Administrador de Recursos de Identificación conforme al numeral 6.13.1.5.7. de esta resolución.

**6.13.4.3.2. Modificación de plantillas aprobadas**. El asignatario del SENDER ID podrá solicitar la modificación de una plantilla aprobada cuando se presenten cambios en el contenido, en las URLs o dominios, o en la modalidad de contenido. El validador la procesará conforme al numeral 6.13.4.3.1 de esta resolución con los mismos tiempos de respuesta. Durante el trámite de la modificación, la plantilla original continuará vigente. Si la modificación implica un cambio de modalidad incompatible con el SENDER ID vinculado, el validador rechazará la modificación e informará al asignatario que deberá solicitar autorización para la adición de esa modalidad conforme al Parágrafo del artículo 6.12.1.3. de esta resolución.

**6.13.4.3.3. Vigencia y desactivación de plantillas.** Las plantillas aprobadas tendrán vigencia mensual. La vigencia mensual se renovará automáticamente al vencimiento de cada período, salvo que ocurra alguna de las siguientes circunstancias que den lugar a su desactivación:

i) El asignatario del SENDER ID solicite expresamente al validador la desactivación cuando la campaña o servicio asociado haya concluido y no se prevea su reutilización.

ii) El validador detecte un escenario de mal uso de la plantilla en los términos del artículo 6.13.4.4, caso en el cual procederá a desactivar la plantilla de manera inmediata y reportará el hecho al Administrador de Recursos de Identificación.

iii) El SENDER ID al que está vinculada la plantilla sea recuperado por el Administrador de Recursos de Identificación, caso en el cual todas las plantillas vinculadas al mismo SENDER ID serán desactivadas simultáneamente conforme al Parágrafo 1 del artículo 6.12.3.2. de esta resolución.

iv) El código corto A2P a través del cual fue gestionada la aprobación sea recuperado y no exista otro código corto A2P con relación contractual vigente con el asignatario del SENDER ID, caso en el cual se aplicará el procedimiento del Parágrafo 1 del artículo 6.4.3.2. de esta resolución.

**ARTÍCULO 6.13.4.4. ATRIBUCIÓN DE RESPONSABILIDAD POR MAL USO DE PLANTILLAS.** La atribución de responsabilidad por mal uso de las plantillas funcionará de conformidad con las siguientes reglas:

**6.13.4.4.1.** Se entiende que existe mal uso de una plantilla cuando el contenido efectivamente cursado difiere del aprobado por el validador, incluyendo: el contenido cursado corresponde a una modalidad distinta a la aprobada; se incluyen URLs o dominios no declarados en la solicitud de aprobación o en su última modificación aprobada; se introduce información que induce al usuario en error; o se cursan mensajes a usuarios inscritos en el RNE en contravención de las restricciones de la modalidad de la plantilla.

**6.13.4.4.2.** Cuando el mal uso sea directamente imputable al asignatario del SENDER ID, sin intervención ni conocimiento del asignatario del código corto A2P, las consecuencias regulatorias recaerán exclusivamente sobre el SENDER ID conforme a las causales del artículo 6.12.3.2. de esta resolución.

**6.13.4.4.3.** Cuando el mal uso sea directamente imputable al asignatario del código corto A2P, por haber permitido o facilitado el envío de tráfico no autorizado sin conocimiento del asignatario del SENDER ID, las consecuencias regulatorias recaerán exclusivamente sobre el código corto A2P conforme a las causales del artículo 6.4.3.2. de esta resolución.

**6.13.4.4.4.** Cuando el mal uso sea imputable de manera concurrente a ambos asignatarios, el Administrador de Recursos de Identificación podrá iniciar procedimientos de recuperación simultáneos o sucesivos sobre ambos recursos, con plena observancia del derecho a la defensa y al debido proceso.

**6.13.4.4.5.** A efectos de la atribución de responsabilidad, el validador conservará los registros de auditoría de todas las plantillas aprobadas, los mensajes cursados por cada SENDER ID y los eventos de divergencia entre el contenido aprobado y el contenido cursado, y los pondrá a disposición del Administrador de los Recursos de Identificación cuando sean requeridos.

**ARTÍCULO 6.13.4.5. OBLIGACIONES ESPECIALES DE LOS ASIGNATARIOS DEL CÓDIGO CORTO A2P.** Los asignatarios de código corto A2P tienen las siguientes obligaciones especiales:

**6.13.4.5.1.** Garantizar que únicamente cursen tráfico A2P a través de su infraestructura los asignatarios de SENDER ID que cuenten con certificación vigente del validador, con los recursos de identificación en estado asignado e implementado en el SIGRI, y con al menos una plantilla de contenido previamente aprobada y vigente.

**6.13.4.5.2.** Integrar sus plataformas de mensajería con el sistema del validador centralizado a través de las APIs disponibles para la consulta en tiempo real del estado de los recursos de identificación y de las plantillas.

**6.13.4.5.3.** Notificar al asignatario del SENDER ID, al validador centralizado y al Administrador de Recursos de Identificación, dentro de las veinticuatro (24) horas siguientes a su detección, cualquier incidente de uso indebido del tráfico A2P cursado a través de su infraestructura.

**6.13.4.5.4.** Suspender de manera inmediata el envío de tráfico de un asignatario de SENDER ID cuando el Administrador de Recursos de Identificación así lo indique.

**6.13.4.5.5.** Informar previamente al Administrador de Recursos de Identificación cualquier cambio en su infraestructura técnica de conexión con los PRST que pueda afectar la trazabilidad del tráfico A2P.

**6.13.4.5.6.** Mantener actualizado el registro de los asignatarios de SENDER ID que cursan tráfico a través de su infraestructura, con indicación del estado de la relación contractual y de las plantillas activas vinculadas a cada SENDER ID.

**ARTÍCULO 6.13.4.6. OBLIGACIONES ESPECIALES DE LOS ASIGNATARIOS DEL SENDER ID.** Los asignatarios de SENDER ID tienen las siguientes obligaciones especiales:

**6.13.4.6.1.** Garantizar que todos los mensajes cursados a través de su SENDER ID correspondan exclusivamente al contenido de las plantillas aprobadas y vigentes en el sistema del validador.

**6.13.4.6.2.** Obtener, documentar y conservar el consentimiento de los usuarios para el envío de mensajes en las modalidades que lo requieran, conforme a las categorías del artículo 6.12.1.3. de esta resolución.

**6.13.4.6.3.** Respetar en todo momento las restricciones del RNE aplicables a cada modalidad de contenido conforme al artículo 6.12.1.3. de la presente resolución.

**6.13.4.6.4.** Garantizar que las URLs y dominios incluidos en los mensajes cursados correspondan exclusivamente a los declarados y aprobados en la plantilla vigente, y que no redirijan a sitios web fraudulentos, maliciosos o no verificados.

**6.13.4.6.5.** Notificar al asignatario del código corto A2P y al validador, dentro de las veinticuatro (24) horas siguientes a su conocimiento, cualquier indicio de uso indebido de su SENDER ID por parte de terceros no autorizados.

**6.13.4.6.6.** Mantener actualizada su información en el RPCAI, en la matrícula mercantil que alimenta el RUES y ante el validador.

**6.13.4.6.7.** Solicitar la desactivación de las plantillas cuando las campañas o servicios asociados hayan concluido y no se prevea su reutilización.

**6.13.4.6.8.** Completar oportunamente la validación anual ante el validador centralizado conforme al artículo 6.12.3.3 de la presente resolución.

**ARTÍCULO 6.13.4.7. OBLIGACIONES ESPECIALES DE LOS PRST.** Los PRST tienen las siguientes obligaciones especiales:

**6.13.4.7.1.** Integrar sus plataformas de mensajería (SMSC) con el sistema del validador centralizado a través de las APIs disponibles, de modo que puedan consultar en tiempo real, previo al enrutamiento de cada mensaje A2P, la validez del código corto A2P, del SENDER ID y de la plantilla de contenido asociados al mensaje.

**6.13.4.7.2.** Verificar, previo al enrutamiento de cada mensaje A2P, que cuente con un código corto A2P y un SENDER ID en estado asignado e implementado en el SIGRI, y con una plantilla de contenido aprobada y vigente en el sistema del validador. En ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, y a elección del PRST, marcarlo con la etiqueta «sin verificar».

**6.13.4.7.3.** Reportar mensualmente al validador centralizado los mensajes bloqueados por ausencia o invalidez de identificadores o de plantilla. El Administrador de Recursos de Identificación podrá acceder a esa información, previo requerimiento de información enviado al validador centralizado o al PRST.

**6.13.4.7.4.** Suspender de manera inmediata el envío de tráfico A2P asociado a un código corto A2P, SENDER ID o plantilla de contenido A2P cuando el Administrador así lo indique en el marco de una actuación administrativa de recuperación o de una medida de suspensión preventiva conforme al Parágrafo 3o. del artículo 6.1.1.8. de la presente resolución.

## SECCIÓN 5.
## COMITÉ TÉCNICO DE SEGUIMIENTO Y COORDINACIÓN OPERATIVA

**ARTÍCULO 6.13.5.1. COMITÉ TÉCNICO DE SEGUIMIENTO (CTS).** Créase el Comité Técnico de Seguimiento del régimen de recursos de identificación asociados al ecosistema A2P, en adelante CTS, como instancia permanente de carácter consultivo bajo la dirección de la CRC.

**6.13.5.1.1. Objeto.** El CTS es la instancia mediante la cual la CRC realizará el seguimiento a la implementación y operación del régimen de código corto A2P, SENDER ID y plantillas de contenido A2P, y coordinará la respuesta del ecosistema frente a incidentes de fraude.

**6.13.5.1.2. Conformación.** El CTS estará conformado por todos los asignatarios de código corto A2P. La CRC presidirá el Comité y ejercerá la secretaría técnica. El validador centralizado participará como invitado permanente, con derecho a voz, pero sin derecho a voto. Podrán ser invitados a sesiones específicas representantes de los PRST, asignatarios de SENDER ID,

asociaciones gremiales del sector, entidades del orden nacional con competencias en prevención del fraude cibernético y organismos internacionales de referencia.

**6.13.5.1.3. Presidencia.** La Presidencia del CTS será ejercida por un Comisionado de la Sesión de Comunicaciones de la CRC o por quien este designe. Ante la ausencia del Presidente actuará quien este designe.

**6.13.5.1.4. Secretaría.** La Secretaría del CTS será ejercida por la CRC. El Secretario tendrá a su cargo la convocatoria a las sesiones, el levantamiento de actas, el registro y control de la documentación y la información de contacto de los miembros, y el seguimiento a las determinaciones adoptadas.

**6.13.5.1.5. Funciones del CTS.** Son funciones del CTS:

i) Hacer seguimiento a la implementación del nuevo régimen.

ii) Revisar y proponer la actualización de los parámetros técnicos de monitoreo de tráfico A2P, incluyendo los umbrales de detección de patrones anómalos y los criterios de gestión de las listas dinámicas de URLs y dominios fraudulentos.

iii) Analizar los incidentes de fraude detectados durante el período y proponer acciones correctivas y preventivas.

iv) Facilitar el intercambio de información relevante sobre fraude cibernético entre los actores del ecosistema, con plena observancia de las disposiciones aplicables en materia de protección de datos personales y de confidencialidad de información comercialmente sensible.

v) Proponer a la CRC los ajustes regulatorios que la experiencia de operación del nuevo régimen haga necesarios.

vi) Documentar en actas de sesión las determinaciones técnicas y operativas adoptadas.

**6.13.5.1.6. Funciones de la Presidencia del CTS.** Son funciones de la Presidencia: presidir las sesiones del CTS; proponer el orden del día; facilitar y dar por terminada la discusión de los temas tratados; proponer al CTS la conformación y realización de mesas de trabajo; e invitar a participar en las sesiones a otras autoridades cuando los temas a tratar así lo requieran.

**6.13.5.1.7. Funciones de la Secretaría del CTS.** Son funciones de la Secretaría: convocar las sesiones y remitir la documentación pertinente; verificar la asistencia y las facultades de los representantes; consultar el sentido de la votación de los miembros con derecho a voto; levantar las actas de cada sesión; llevar el registro y control de la documentación generada; y llevar el registro de la información de contacto de los miembros del CTS.

**6.13.5.1.8. Convocatoria.** La Secretaría convocará las sesiones mediante comunicación escrita o correo electrónico a los representantes de los asignatarios de código corto A2P y, cuando sea el caso, al validador centralizado y a otras autoridades invitadas, con antelación mínima de diez (10) días hábiles a la fecha de la sesión. La convocatoria estará disponible en la página web de la CRC. El CTS se reunirá, por lo menos, dos veces al año (una por semestre), sin perjuicio de que la CRC lo convoque de manera extraordinaria cuando las circunstancias del caso lo ameriten.

**6.13.5.1.9. Sesiones.** Las sesiones iniciarán con la verificación de la asistencia y de las facultades de los representantes. Los temas que se someterán a consideración de los miembros se pondrán en su conocimiento al menos dos (2) días hábiles antes de la sesión. Cuando la Presidencia considere que la discusión de un tema ha sido agotada, lo someterá a votación.

En el acta de cada sesión se incluirán las propuestas que hayan obtenido mayoría simple de los miembros asistentes con derecho a voto, contando un voto por asignatario de código corto A2P. Los votos de abstención sólo se contabilizarán para registro y no se sumarán a ninguna de las opciones. Las posturas cuya votación resulte empatada quedarán incluidas en el acta junto con los argumentos de cada posición.

El acta de cada sesión se cerrará con su lectura y la firma de los representantes presentes. La falta de firma de algún representante no viciará el acta ni las votaciones alcanzadas en la sesión; la Secretaría dejará constancia del hecho e indicará las razones cuando las hubiere.

**6.13.5.1.10. Actas.** De cada sesión se levantará un acta en la que se especificarán como mínimo: fecha, hora, lugar, orden del día, temas tratados y resultados. Las actas se conservarán en archivo de libre consulta para los miembros del CTS en la CRC y serán publicadas en la página web de la CRC, por vía de una circular, salvo la información que tenga carácter de confidencial o reservado, la cual se mantendrá en archivo independiente.

**6.13.5.1.11. Naturaleza y vinculatoriedad de las determinaciones del CTS.** Las determinaciones del CTS son de naturaleza consultiva y técnica en relación con la CRC y no limitan su competencia regulatoria. De otra parte, las determinaciones que establezcan parámetros técnicos de operación entre los participantes del ecosistema, tales como especificaciones de las APIs de integración, formatos de reporte de incidentes, protocolos de comunicación entre sistemas, umbrales de monitoreo de tráfico y procedimientos de gestión de contingencias, serán de cumplimiento obligatorio para los asignatarios de código corto A2P, los PRST y el validador centralizado en los términos y plazos establecidos en la respectiva acta de sesión. Esta vinculatoriedad deriva de la obligación regulatoria de participar en el CTS e implementar las condiciones técnicas necesarias para el funcionamiento del nuevo régimen, así como de la autonomía de la voluntad privada entre los actores. Las actas que documenten estas determinaciones no constituyen actos administrativos de carácter particular ni general y no son susceptibles de los recursos de la vía gubernativa. Estas determinaciones deberán ser implementadas por los agentes en los respectivos contratos que se hayan suscrito con el validador centralizado.

**6.13.5.1.12. Incumplimiento de las determinaciones técnicas del CTS.** El incumplimiento injustificado de las determinaciones técnicas y operativas adoptadas conforme al numeral 6.13.5.1.11 será reportado por la CRC, en su condición de secretaría técnica, a las entidades de control y vigilancia competentes para la imposición de las sanciones que correspondan, sin perjuicio de las demás consecuencias regulatorias establecidas en la presente resolución.

**6.13.5.1.13. Vigencia del CTS.** El CTS tendrá una vigencia indefinida.

**ARTÍCULO 6.13.5.2. SEGUIMIENTO Y REPORTE DE INCIDENTES.**

**6.13.5.2.1.** Ante la detección de un incidente de uso potencialmente engañoso de un recurso de identificación o de mal uso de una plantilla, el validador o el asignatario de código corto A2P que lo detecte notificará al Administrador de Recursos de Identificación a más tardar dentro de las dos (2) horas siguientes.

**6.13.5.2.2.** La notificación de incidente incluirá como mínimo: la identificación del recurso de identificación y la plantilla involucrados; la descripción de la conducta detectada; la fecha y hora de detección; el volumen de tráfico potencialmente afectado; y las medidas de contención adoptadas de manera inmediata.

**6.13.5.2.3.** Dentro de las cuarenta y ocho (48) horas siguientes a la notificación inicial, el validador centralizado y el asignatario de código corto A2P reportante presentarán al Administrador de Recursos de Identificación un informe completo del incidente que incluya el análisis de causa raíz, la descripción detallada de las medidas de contención y corrección adoptadas y las recomendaciones para prevenir la recurrencia.

**6.13.5.2.4.** El Administrador de Recursos de Identificación consolidará los reportes de incidentes recibidos y los pondrá a disposición del CTS en cada sesión ordinaria, con indicación de las tendencias identificadas.

**ARTÍCULO 15.** Adiciónese el Capítulo 14 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, el cual quedará así:

«**CAPÍTULO 14**
**MEDIDAS EDUCATIVAS, PEDAGÓGICAS Y DE INTERACCIÓN CON USUARIOS EN MATERIA DE PREVENCIÓN DEL FRAUDE EN EL MARCO DEL RÉGIMEN DE ADMINISTRACIÓN DE RECURSOS DE IDENTIFICACIÓN**

## SECCIÓN 1.
## MEDIDAS COMUNES PARA SMS Y VOZ

**ARTÍCULO 6.14.1.1. MICROSITIO DE LA CRC Y DOCUMENTOS DE CONSULTA PÚBLICA.** La CRC elaborará y publicará en un micrositio específico de su página web contenido educativo y pedagógico dirigido al público en general que contenga consejos, recomendaciones y guías para la identificación de mensajes de texto y llamadas de voz con fines presuntamente fraudulentos. De manera complementaria, la CRC elaborará contenido dirigido exclusivamente a entidades públicas, el cual será compartido a través del mismo canal.

La CRC actualizará ese contenido de manera periódica en función de avances tecnológicos, nuevas modalidades de fraude o cualquier otro elemento que haga necesario su ajuste. Para la elaboración de ese contenido dirigido al público en general, la CRC tendrá en cuenta que sus destinatarios pueden tener características diversas que ameritan un tratamiento diferencial, incluyendo la edad, las condiciones socioeconómicas y la región de residencia, entre otras.

Con ocasión de la publicación de este contenido, la CRC organizará periódicamente talleres prácticos, principalmente virtuales, dirigidos al público en general y a entidades públicas. Las condiciones de tiempo, modo y lugar de estos espacios serán publicadas en el micrositio al que hace referencia el presente artículo.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial del acto administrativo que creó este micrositio para habilitar y/o ajustar el micrositio al que hace referencia el presente artículo, así como para publicar los contenidos a los que hace referencia esta disposición.

**ARTÍCULO 6.14.1.2. OBLIGACIÓN DE DIFUSIÓN DEL MICROSITIO POR PARTE DE LOS ASIGNATARIOS Y OPERADORES.** Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán incluir en sus páginas web una pestaña específica a través de la cual sus usuarios, clientes y el público en general sean redirigidos al micrositio de la CRC al que hace referencia el artículo 6.14.1.1. Esta obligación deberá cumplirse dentro del mes siguiente a la publicación del micrositio por parte de la CRC.

**ARTÍCULO 6.14.1.3. CAMPAÑAS PEDAGÓGICAS DE LOS ASIGNATARIOS Y OPERADORES.** Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán desarrollar al menos cuatro (4) campañas pedagógicas de prevención de fraude al año, una por cada trimestre calendario (enero a marzo, abril a junio, julio a septiembre, octubre a diciembre), difundidas en todas sus redes sociales y páginas web. Las campañas deberán ser masivas, sostenidas y utilizar múltiples canales de comunicación.

El contenido de las campañas deberá incluir, sin limitarse a ello, información sobre los derechos de los usuarios respecto de sus datos personales, las modalidades de fraude existentes a través de mensajes de texto y llamadas de voz, las técnicas de ingeniería social utilizadas por los ciberdelincuentes para obtener información confidencial, y las acciones que los usuarios pueden tomar para prevenirlas o mitigarlas. Las campañas deben tener un enfoque diferencial para usuarios en condición de vulnerabilidad, incluyendo adultos mayores, usuarios con bajos niveles de alfabetización digital y usuarios en zonas con menor acceso a servicios digitales.

La CRC definirá mediante una circular un hashtag oficial para el seguimiento de estas campañas en cada trimestre, así como los criterios mínimos de contenido, alcance y medios que deberán cumplir.

Dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remitirá a la CRC los comprobantes que acrediten su cumplimiento.

**ARTÍCULO 6.14.1.4. ESPACIOS INTERINSTITUCIONALES.** La CRC promoverá espacios de coordinación interinstitucional orientados a crear sinergias y aunar esfuerzos en materia pedagógica y educativa para la prevención del fraude. Con este propósito, al menos dos veces al año, la CRC organizará espacios a los que invitará a la Superintendencia de Industria y Comercio, a la Superintendencia Financiera de Colombia, al Ministerio de Tecnologías de la Información y las Comunicaciones, al COLCERT, a la Fiscalía General de la Nación y a organizaciones nacionales e internacionales de reconocida trayectoria en materia de lucha contra el fraude cibernético, con

la finalidad de compartir experiencias en materia educativa y de transparencia con los usuarios y articular esfuerzos en la realización de campañas pedagógicas conjuntas.

**ARTÍCULO 6.14.1.5. FORMACIÓN INTERNA EN MATERIA DE PREVENCIÓN DEL FRAUDE.** Los asignatarios de recursos de identificación que hagan parte del ecosistema A2P y los PRST deberán implementar programas de formación interna en materia de prevención del fraude cibernético dirigidos a sus equipos de trabajo, con una periodicidad mínima de cuatro (4) sesiones al año, una por cada trimestre calendario. Los programas de formación deberán cubrir, como mínimo, los siguientes contenidos:

**6.14.1.5.1.** Las modalidades de fraude cibernético más frecuentes en el sector de las telecomunicaciones, incluyendo mecanismos tales como smishing, vishing y spoofing, así como las técnicas de ingeniería social utilizadas por los defraudadores para explotar los canales de voz y mensajería de texto.

**6.14.1.5.2.** El marco regulatorio vigente en materia de prevención del fraude, incluyendo las obligaciones establecidas en la presente resolución y las consecuencias regulatorias y contractuales derivadas de su incumplimiento.

**6.14.1.5.3.** Los procedimientos internos del agente para la detección, reporte y gestión de incidentes de fraude, incluyendo los canales de escalamiento hacia el validador centralizado, el Administrador de los Recursos de Identificación y el CTLFSM, según corresponda.

**6.14.1.5.4.** Los protocolos de atención al usuario en situaciones relacionadas con el fraude, con énfasis en el trato adecuado a usuarios en condición de vulnerabilidad, incluyendo adultos mayores y usuarios con bajos niveles de alfabetización digital.

**6.14.1.5.5.** Las buenas prácticas en materia de protección de datos personales en el contexto de la prestación de servicios de telecomunicaciones y mensajería A2P.

Los programas de formación deberán alcanzar, como mínimo, a los equipos de atención al usuario, gestión de clientes corporativos, operaciones de red, cumplimiento regulatorio y áreas comerciales. Los agentes obligados deberán garantizar que el personal que se incorpore con posterioridad al inicio de cada ciclo anual reciba la capacitación correspondiente dentro de los treinta (30) días hábiles siguientes a su vinculación.

Dentro de los quince (15) días hábiles siguientes a la finalización de cada trimestre, el agente obligado remitirá a la CRC un reporte que acredite el cumplimiento del programa de formación del período, con indicación del número de empleados capacitados, los contenidos cubiertos, la metodología utilizada y la cobertura por área funcional. Además, en las oportunidades que la CRC lo determine en el marco del CTLFSM, los agentes obligados presentarán los comprobantes, experiencias y resultados obtenidos producto de sus programas de formación de equipos internos.

## SECCIÓN 2.
## MEDIDAS PEDAGÓGICAS ESPECÍFICAS PARA SMS

**ARTÍCULO 6.14.2.1. DIFUSIÓN PÚBLICA DE ACTUACIONES ADMINISTRATIVAS DE RECUPERACIÓN.** La CRC promoverá la difusión pública de las actuaciones administrativas de recuperación de recursos de identificación, con el propósito de facilitar la participación de cualquier tercero interesado conforme a los artículos 37 y 38 de la Ley 1437 de 2011. Para tal efecto, la CRC habilitará en su página web un micrositio específico en el que se publicará el inicio y el resultado de las actuaciones administrativas de recuperación de recursos de identificación, de modo que cualquier ciudadano pueda conocerlos y, cuando lo considere pertinente, vincularse a los respectivos trámites para aportar, solicitar pruebas y, en general, ejercer derechos como tercero interesado. Para este efecto, la CRC utilizará el micrositio previsto en el numeral 6.1.1.8.1 del artículo 6.1.1.8 de la presente resolución.

**ARTÍCULO 6.14.2.2. INSCRIPCIÓN DE CÓDIGOS CORTOS DEL SECTOR FINANCIERO.** Los asignatarios de recursos de identificación utilizados para el envío de mensajes cortos de texto deberán incluir en sus contratos con clientes corporativos del sector financiero la obligación de que dichos clientes inscriban, en el portal que la CRC disponga para el efecto, los códigos cortos

y los SENDER ID, según aplique, que utilicen para soportar sus servicios de mensajería. La información inscrita será de consulta pública a través del micrositio de la CRC.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial de la resolución que creó esta obligación para habilitar el portal y el micrositio a los que hace referencia el presente artículo. Los asignatarios tendrán un plazo de seis (6) meses contados a partir del vencimiento del plazo anterior para ajustar sus contratos e informar a la CRC sobre el cumplimiento de esta obligación.

**SECCIÓN 3.**
**MEDIDAS PEDAGÓGICAS ESPECÍFICAS PARA VOZ**

**ARTÍCULO 6.14.3.1. INSCRIPCIÓN DE NUMERACIÓN DEL SECTOR FINANCIERO.** Los PRST deberán incluir en sus contratos con clientes corporativos del sector financiero la obligación de que dichos clientes inscriban, en el portal que la CRC disponga para el efecto, la numeración E.164 geográfica o no geográfica que utilicen para soportar sus servicios de llamadas de voz. La información inscrita será de consulta pública a través del micrositio de la CRC, con el propósito de que los ciudadanos puedan verificar si un número que los ha contactado corresponde a una entidad financiera legítima.

La CRC tendrá un plazo de seis (6) meses contados a partir de la publicación en el Diario Oficial del acto administrativo que creó esta obligación para habilitar el portal y el micrositio a los que hace referencia el presente artículo. Los PRST tendrán un plazo de tres (3) meses contados a partir del vencimiento del plazo anterior para ajustar sus contratos e informar a la CRC sobre el cumplimiento de esta obligación».

**ARTÍCULO 16.** Adicionar el numeral 11.1.1.2.6. al artículo 11.1.1.2. del Capítulo 1 del Título XI de la Resolución CRC 5050 de 2016, el cual quedará así:

"**ARTÍCULO 11.1.1.2. CASOS DE PROYECTOS DE REGULACIÓN QUE NO SON SUJETOS DE PUBLICACIÓN.** No se dará aplicación a lo previsto en el artículo 2.2.13.3.2 del Decreto 1078 de 2015 en los siguientes casos:

(…)

**11.1.1.2.6**. En la expedición de las resoluciones de las que trata el artículo 2.1.10.7.3.4. relacionadas con las decisiones que adopte el CTLFSM en los términos allí contenidos".

**ARTÍCULO 17.** Adiciónese el siguiente formato al TÍTULO REPORTES DE INFORMACIÓN de la Resolución CRC 5050 de 2016:

**FORMATO T.5.9 — INFORMACIÓN DE SENDER ID**

**Periodicidad:** Trimestral.

**Contenido:** Mensual.

**Plazo:** Hasta 30 días calendario después de finalizado el trimestre.

Este formato deberá ser diligenciado por el Validador Centralizado encargado de la administración, validación y trazabilidad de LOS SENDER ID utilizados en servicios de mensajería SMS A2P, y contendrá la información asociada a los SENDER ID que cursen tráfico a través del esquema de validación centralizado, con el fin de reportar el uso, tráfico, implementación y cumplimiento del recurso asignado.

Vigencia: A partir del vencimiento del período de transición establecido en el artículo 19 de la resolución que adoptó este formato.

**Contenido del reporte:**

**A. Identificación, Relación de Entidades y Tráfico General**

Esta parte consolida los datos de control temporal, la caracterización del recurso (SENDER ID), su vinculación con los códigos cortos A2P y los volúmenes de tráfico de red.

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| | | | | | | *Tráfico cursado SMS* | | |
| *Año* | *Trimestre* | *Mes* | *Sender ID* | *Código corto A2P asociado* | *Razón social del asignatario del código corto A2P* | *Tráfico MT* | *Tráfico MO* | *Cantidad de campañas o contenidos utilizados* |

**1. Año:** Corresponde al año para el cual se reporta la información. Campo numérico entero de 4 dígitos.

**2. Trimestre:** Corresponde al trimestre del año para el cual se reporta la información. Campo numérico entero con valores entre 1 y 4.

**3. Mes:** Corresponde al mes del trimestre reportado. Campo numérico entero con valores entre 1 y 3.

**4. Sender ID:** Identificador alfanumérico utilizado para el envío de mensajes SMS y sobre el cual versa la información reportada.

**5. Código corto A2P asociado:** Código corto A2P habilitado para el uso del Sender ID durante el período reportado.

**6. Razón social del asignatario del código corto A2P**: Razón social del asignatario del código corto A2P habilitado para el uso del Sender ID.

**7. Tráfico cursado SMS MT**: Número total de mensajes SMS terminados en terminales móviles y cursados mediante el Sender ID reportado.

**8. Tráfico cursado SMS MO:** Número total de mensajes SMS originados desde terminales móviles asociados al Sender ID reportado.

**9. Cantidad de campañas o contenidos utilizados**: Número de campañas, templates, contenidos o estructuras de mensajes asociados al Sender ID durante el período reportado.

**B: Validación de Plantillas, Gestión de Fraude y Cumplimiento**

Esta parte se enfoca en la operación técnica del Validador Centralizado: la trazabilidad, aprobación o rechazo de plantillas A2P, las alarmas de seguridad y el estado operativo.

| *1* | *2* | *3* | *4* | *5* | *6* | *7* | *8* | *9* | *10* | *11* | *12* | *13* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | *Plantillas* | | | | | | | | | |
| *Sender ID* | *Coincidencias validadas* | *Rechazos de validación* | *Pre aprobadas* | *Aprobadas y vigentes* | *Solicitudes de aprobación* | *Aprobadas* | *Rechazadas y causal* | *Desactivadas y causa* | *Incidentes de uso potencialmente fraudulento* | *Reportes de uso indebido* | *Estado de implementación* | *Observación* |

**1. Sender ID:** Identificador alfanumérico utilizado para el envío de mensajes SMS y sobre el cual versa la información reportada.

**2. Coincidencias validadas**: Número de mensajes que cumplieron satisfactoriamente las reglas del esquema de validación centralizada.

**3. Rechazos de validación:** Número de mensajes rechazados por inconsistencias de validación, trazabilidad o incumplimiento de reglas definidas por el esquema centralizado.

**4. Plantillas pre aprobadas:** Estructuras base de mensajes validados de forma previa en el sistema antes de su puesta en producción.

**5. Plantillas aprobadas y vigentes:** Número total de plantillas de contenido A2P aprobadas y vigentes al cierre del período, discriminadas por modalidad de contenido.

**6. Solicitudes de aprobación de plantillas**: Número de solicitudes de aprobación de plantillas recibidas durante el período reportado.

**7. Plantillas aprobadas:** Número de plantillas aprobadas durante el período reportado.

**8. Plantillas rechazadas y causal**: Número de plantillas rechazadas durante el período reportado y causal de rechazo asociada.

**9. Plantillas desactivadas y causa:** Número de plantillas desactivadas durante el período reportado y causa asociada.

**10. Incidentes de uso potencialmente fraudulento**: Número de incidentes detectados relacionados con posibles usos fraudulentos de recursos de identificación durante el período reportado.

**11. Reportes de uso indebido:** Número de reportes remitidos al Administrador de Recursos de Identificación sobre indicios de uso indebido, discriminados por tipo de conducta detectada.
**12.Estado de implementación:** Estado de utilización efectiva y operativa del Sender ID durante el período reportado.

**13. Observación:** Campo destinado al registro de incidencias, novedades o situaciones relevantes asociadas al Sender ID reportado.

**ARTÍCULO 18.** El proceso de selección de la persona jurídica que cumplirá las funciones del validador centralizado al que hace referencia el Capítulo 13 del TÍTULO VI de la Resolución CRC 5050 de 2016 se someterá a las siguientes reglas:

**18.1. RESPONSABILIDAD DE SELECCIÓN.** Los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) son responsables de la selección del validador centralizado conforme a los numerales siguientes, bajo la supervisión de la CRC. Lo anterior, en atención a que el validador centralizado deberá integrarse técnicamente con las redes de los PRSTM, razón por la cual son estos proveedores quienes se encuentran en mejor posición para evaluar los requerimientos técnicos, la capacidad operativa y la idoneidad del candidato seleccionado. La participación en el proceso de selección es una obligación regulatoria de todos los PRSTM. La financiación de los costos de implementación, gestión, operación y mantenimiento del validador centralizado estará a cargo de los asignatarios del código corto A2P, en los términos del artículo 6.13.1.2. de la Resolución CRC 5050 de 2016.

**18.1.1. CONSTITUCIÓN DEL COMITÉ DE SELECCIÓN.** Dentro de los cinco (5) días calendario siguientes a partir de la publicación en el Diario Oficial de la resolución por medio de la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P, la CRC citará a una reunión a los PRSTM y declarará constituido el Comité de Selección, integrado por todos los PRSTM. La CRC actuará como secretaría técnica del Comité durante todo el proceso, sin derecho a voto. Cada PRSTM miembro tendrá derecho a un voto, con independencia de su tamaño o participación de mercado. Las decisiones se adoptarán por mayoría simple de los miembros presentes. En caso de empate, la CRC tendrá voto dirimente. El incumplimiento de la obligación de participar en el Comité de Selección será reportado por la CRC a las entidades de control y vigilancia para la imposición de las sanciones que correspondan.

**18.1.2. PROCESO DE SELECCIÓN.** Una vez constituido el Comité de Selección, sus miembros tendrán un plazo de diez (10) días calendario para elaborar conjuntamente, en la forma en la que decidan organizarse de manera autónoma, el documento con las condiciones del proceso de selección del validador centralizado, incluyendo los criterios de evaluación técnica y operativa y el modelo de contrato a suscribir. En la elaboración de este documento los PRSTM deberán tener en cuenta los requisitos establecidos en el artículo 6.13.1.3. de la Resolución CRC 5050 de 2016 y las condiciones de financiamiento previstas en el artículo 6.13.1.2. de la misma resolución, dado que son los asignatarios del código corto A2P quienes asumirán los costos del validador. Dicha información será sometida a revisión de la CRC dentro de los dos (2) días calendario siguientes al vencimiento del anterior plazo. La Comisión emitirá concepto dentro de un plazo máximo de

cinco (5) días calendario. Las observaciones de la CRC serán de obligatorio cumplimiento por parte del Comité. El proceso de selección no podrá tener una duración superior a quince (15) días calendario, contados a partir del concepto emitido por la CRC.

**18.1.3. VERIFICACIÓN POR PARTE DE LA CRC.** Una vez el Comité de Selección haya seleccionado al validador centralizado, remitirá a la CRC, dentro de los dos (2) días calendario siguientes, la documentación completa del proceso, el proyecto de contrato y la propuesta de esquema de financiamiento. La CRC contará con cinco (5) días calendario para pronunciarse, verificando: que el candidato cumple los requisitos del numeral 6.13.1.3. de la Resolución CRC 5050 de 2016; que el proceso respetó los principios de transparencia, imparcialidad, competencia y no discriminación; que el contrato incluye todas las obligaciones de las partes conforme al Capítulo 13 del TÍTULO VI de la Resolución CRC 5050 de 2016; que el esquema de financiamiento es compatible con el principio de orientación a costos más utilidad razonable y no genera cargas discriminatorias entre los asignatarios del código corto A2P; y que el candidato no tiene vínculos que comprometan su independencia conforme al numeral 6.13.1.3.4. de la Resolución CRC 5050 de 2016. Si la CRC no formula objeciones dentro del plazo, el candidato queda habilitado para suscribir los contratos. Si formula objeciones, el Comité tendrá diez (10) días calendario para subsanarlas o seleccionar un candidato alternativo.

El incumplimiento de cualquiera de estas obligaciones dentro de los plazos fijados para tal efecto será informado por la CRC a las entidades de control y vigilancia para la imposición de las sanciones correspondientes.

Seguidamente se resume el cronograma descrito:

| **Actividad** | **Plazo** |
|---|---|
| La CRC declarará constituido el Comité de Selección | 5 días calendario a partir de la publicación en el Diario Oficial de la resolución por medio de la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P |
| Plazo para elaborar los documentos del proceso de selección | 10 días calendario desde la constitución del Comité |
| Envío a la CRC de los documentos del proceso de selección | 2 días calendario desde el vencimiento del plazo anterior |
| Concepto de la CRC sobre los documentos del proceso de selección | 5 días calendario desde la recepción de los documentos |
| Proceso de selección del validador centralizado | 15 días calendario desde el concepto de la CRC |
| Remisión a la CRC de la documentación completa del proceso | 2 días calendario desde la culminación del proceso de selección |
| Verificación de la CRC | 5 días calendario desde la recepción de documentos |
| **Total:** | **44 días calendario** |
| Escenario en que la CRC no formula objeciones | El candidato queda habilitado para suscribir los contratos |
| Escenario en que la CRC formula objeciones | El Comité tendrá 10 días calendario adicionales para subsanar o seleccionar candidato alternativo |
| **Total con objeciones:** | **54 días calendario** |

**18.1.4. SUSCRIPCIÓN DE CONTRATOS.** Concluido el proceso de selección y superada la verificación de la CRC, cada asignatario del código corto A2P suscribirá con el validador centralizado el contrato de operación que establezca las condiciones técnicas, operativas y financieras de la relación.

**ARTÍCULO 19.** Para efectos de garantizar un tránsito e implementación ordenada y sin traumatismos de los cambios implementados en el Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 (versión subrogada que aplicará luego del periodo de transición establecido en este artículo) y de las adiciones de los Capítulos 12 y 13 al TÍTULO VI de la Resolución CRC 5050 de

2016, se dispone un período de transición de seis (6) meses. Este periodo de transición empezará a contarse a partir de la publicación en el Diario Oficial de la resolución por medio de la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

Durante ese período, el Capítulo 4 del TÍTULO VI continuará vigente y los códigos cortos existentes operarán exactamente bajo las condiciones del régimen actual. Al vencimiento del período de transición, el Capítulo 4 del TÍTULO VI quedará subrogado y el envío de tráfico A2P se realizará exclusivamente a través del código corto A2P conforme al nuevo Capítulo 4 del TÍTULO VI de la Resolución CRC 5050 de 2016.

**19.1. DURACIÓN Y ESTRUCTURA GENERAL.** El período de transición se estructura en cuatro fases con objetivos específicos, concurrentes en algunos casos, así:

**19.1.1. FASE 1 — SELECCIÓN DEL VALIDADOR CENTRALIZADO (Meses 1 a 2)**

**19.1.1.1.** Esta fase comprende los tiempos y plazos establecidos en el artículo 18 de esta resolución, los cuales no podrán superar un tiempo máximo de 54 días (meses 1 a 2) calendario contados a partir de la publicación en el Diario Oficial de la resolución por medio de la cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

**19.1.1.2.** Una vez seleccionado el validador y superado el control de la CRC, el validador podrá iniciar operaciones, lo que incluye la integración técnica que se requiera con la CRC y la activación de las APIs para los PRST y los potenciales asignatarios de código corto A2P.

**19.1.1.3.** La CRC publicará en su página web la comunicación oficial de entrada en operación del validador centralizado, la cual constituye el hito de inicio de las Fases 2, 3 y 4.

**19.1.2. FASE 2 — REGISTRO DE POTENCIALES ASIGNATARIOS Y SOLICITUD DE RECURSOS (Meses 3 a 4).**

A partir del hito de inicio del validador centralizado:

**19.1.2.1.** Los potenciales asignatarios de código corto A2P iniciarán ante el validador el proceso de KYC propio previsto en el numeral 6.13.1.5.2 de la Resolución CRC 5050 de 2016 y obtendrán la certificación requerida para solicitar la asignación del código corto A2P conforme al numeral 6.4.2.1.7. de la misma resolución.

**19.1.2.2.** Los potenciales asignatarios de SENDER ID iniciarán ante los potenciales asignatarios de código corto A2P el proceso de KYC como clientes conforme al artículo 6.13.3.1 de la Resolución CRC 5050 de 2016, obtendrán la certificación correspondiente y formalizarán los contratos requeridos.

**19.1.2.3.** Una vez obtenida la certificación del validador, los potenciales asignatarios de código corto A2P presentarán sus solicitudes de asignación ante el Administrador de Recursos de Identificación conforme al artículo 6.4.2.1. de la Resolución CRC 5050 de 2016, en su versión subrogada.

**19.1.2.4.** Una vez se cumpla la firmeza del acto de asignación del código corto A2P y obtenida la certificación del validador respecto del potencial asignatario del SENDER ID, los asignatarios de código corto A2P presentarán en nombre de sus clientes las solicitudes de asignación de SENDER ID conforme al artículo 6.12.2.1. de la Resolución CRC 5050 de 2016, en su versión subrogada.

**19.1.2.5.** El Administrador de Recursos de Identificación procesará las solicitudes de código corto A2P y SENDER ID con prioridad durante el período de transición, procurando resolver en plazos inferiores a los máximos establecidos en los artículos 6.4.2.2 y 6.12.2.2. de la Resolución CRC 5050 de 2016, en su versión subrogada. En esta etapa se dará prioridad a las solicitudes que presenten las personas jurídicas que estén bajo la inspección, vigilancia y control de la Superintendencia Financiera de Colombia.

**19.1.3. FASE 3 — REGISTRO DE PLANTILLAS Y PRUEBAS TÉCNICAS (Mes 5).**

**19.1.3.1.** Los asignatarios de SENDER ID que hayan obtenido la asignación de su recurso iniciarán ante el validador centralizado el proceso de registro y aprobación de sus plantillas de contenido conforme a la Sección 4 del Capítulo 13 del Título VI de la Resolución CRC 5050 de 2016, en su versión subrogada.

**19.1.3.2.** Los asignatarios de código corto A2P y los PRST realizarán las adecuaciones técnicas necesarias en sus plataformas de mensajería para integrarse con el sistema del validador a través de las APIs conforme a los artículos 6.13.4.5.2 y 6.13.4.7.1 de la Resolución CRC 5050 de 2016, y adelantarán pruebas de integración en entornos no productivos.

**19.1.4. FASE 4 — CONSOLIDACIÓN DE CÓDIGOS CORTOS Y ENTRADA EN PLENA VIGENCIA DEL NUEVO RÉGIMEN (Meses 5 a 6).**

**19.1.4.1.** Los asignatarios de código corto A2P que también sean asignatarios de múltiples códigos cortos bajo el régimen del Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 en su versión vigente deberán iniciar el proceso de consolidación conforme a los numerales 19.1.5. y siguientes del presente artículo.

**19.1.4.2.** Al vencimiento del período de transición, el Capítulo 4 del TÍTULO VI de la Resolución CRC 5050 de 2016 en su versión anterior quedará subrogado por el nuevo Capítulo 4 dispuesto en este acto administrativo. A partir de ese momento, el envío de tráfico A2P se realizará exclusivamente a través de código corto A2P. Los PRST actualizarán sus sistemas de enrutamiento para reconocer exclusivamente los códigos cortos A2P como identificadores válidos para cursar el tráfico A2P.

**19.1.4.3.** Los códigos cortos del régimen anterior que no hayan sido consolidados o devueltos al finalizar el período de transición pasarán al estado de «no implementado» y el Administrador de Recursos de Identificación iniciará el procedimiento de recuperación conforme al artículo 6.1.1.8. La no consolidación dentro del período de transición constituirá causal de recuperación.

**19.1.5. CONSOLIDACIÓN DE CÓDIGOS CORTOS DURANTE LA FASE 4.**

Los asignatarios que durante el período de transición tengan múltiples códigos cortos bajo el régimen del Capítulo 4 del Título VI de la Resolución CRC 5050 de 2016 en su versión anterior y que pretendan operar como asignatarios de código corto A2P deberán consolidar su numeración hacia el único código corto A2P asignado conforme al nuevo artículo 6.4.2.1. de la Resolución CRC 5050 de 2016, conforme a las siguientes reglas:

**19.1.5.1. Elección del código corto a conservar.** El asignatario elegirá libremente cuál de sus códigos cortos del régimen anterior conservará como código corto A2P y notificará su elección al Administrador de Recursos de Identificación dentro de los diez (10) días hábiles siguientes al inicio de la Fase 4 prevista en el numeral 19.1.4 del presente artículo. El Administrador de Recursos de Identificación solo podrá objetar la elección por razones técnicas objetivas. En tal caso, el asignatario tendrá quince (15) días hábiles para proponer una alternativa.

**19.1.5.2. Plan de consolidación.** Junto con la notificación del numeral anterior, el asignatario presentará un plan de consolidación con: cronograma de devolución de los códigos cortos excedentes; número estimado de usuarios activos afectados por cada código corto a devolver; mecanismo técnico de migración del servicio al código corto A2P elegido; y plan de notificación a usuarios conforme al numeral 19.1.5.4. de este artículo.

**19.1.5.3. Recuperación de códigos cortos excedentes.** Los códigos cortos excedentes serán recuperados por el Administrador de Recursos de Identificación conforme al artículo 6.1.1.8 de la Resolución CRC 5050 de 2016 una vez el asignatario acredite el cumplimiento del plan de consolidación.

**19.1.5.4. Notificación a usuarios.** Con antelación mínima de quince (15) días a la fecha prevista para la devolución de cada código corto excedente, el asignatario notificará a todos los usuarios con servicios activos o consentimientos vigentes mediante el propio canal SMS, indicando: la marca o servicio asociado al código corto que cambia; el nuevo código corto A2P desde el que se cursarán los mensajes; la opción de revocar el consentimiento; y las instrucciones para actualizar el número de contacto en el dispositivo. El consentimiento previamente otorgado

se entenderá extendido al nuevo código corto A2P cuando el usuario haya recibido la notificación y no haya ejercido la revocación dentro de los treinta (30) días siguientes.

**19.1.6. RÉGIMEN DE LOS ASIGNATARIOS DE CÓDIGOS CORTOS QUE NO TENGAN INTERÉS EN OPERAR COMO ASIGNATARIOS DE CÓDIGO CORTO A2P.**

Los asignatarios de códigos cortos bajo el régimen del Capítulo 4 del TÍTULO VI vigente que no pretendan operar como asignatarios de código corto A2P ni como asignatarios de SENDER ID podrán devolver de forma voluntaria sus códigos cortos conforme al artículo 6.1.1.7. de la Resolución CRC 5050 de 2016 en cualquier momento durante el período de transición. Al vencimiento del período de transición, en caso de no ser devueltos los códigos asignados, los mismos quedarán en estado de «no implementado» y serán objeto del procedimiento de recuperación establecido mediante el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016.

**19.1.7. SEGUIMIENTO Y PUBLICIDAD DE LA TRANSICIÓN.**

El Administrador de Recursos de Identificación publicará en la página web de la CRC, con periodicidad mensual durante el período de transición, un informe de avance que incluya: el número de asignatarios de código corto A2P y SENDER ID con recursos asignados; el número de plantillas aprobadas; el número de asignatarios de códigos cortos en proceso de consolidación; el número de consolidaciones completadas; y el número de recuperaciones de códigos cortos excedentes efectuadas.

Dentro de los treinta (30) días hábiles siguientes al vencimiento del período de transición, el Administrador de Recursos de Identificación publicará un informe de cierre de la transición con los resultados finales, obstáculos identificados y recomendaciones de ajuste regulatorio, en caso de existir.

**ARTÍCULO 20. VIGENCIA Y DEROGATORIAS**. Las disposiciones contenidas en esta resolución entran en vigor de la siguiente forma:

**a. Al momento de la publicación de esta resolución en el Diario Oficial:**

- Las definiciones de LISTA DNO (DO NOT ORIGINATE) y TRÁFICO P2P adicionadas al TÍTULO I de la Resolución CRC 5050 de 2016 mediante el artículo 1 de esta resolución.

- El artículo 3 de esta resolución, por medio del cual se modificó el artículo 2.1.10.7. de la Resolución CRC 5050 de 2016.

- El artículo 4 de esta resolución, por medio del cual se modificó el artículo 2.1.18.1. de la Resolución CRC 5050 de 2016.

- El artículo 5 de esta resolución, por medio del cual se adicionaron los numerales 4.1.2.6.4 y 4.1.2.6.5 al artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV de la Resolución CRC 5050 de 2016, los cuales estarán vigentes hasta que finalice el periodo de transición establecido en el artículo 19 de esta resolución. Una vez finalizado ese periodo de transición, los numerales 4.1.2.6.4 y 4.1.2.6.5 del artículo 4.1.2.6. del CAPÍTULO 2 del TÍTULO IV de la Resolución CRC 5050 de 2016 se entenderán derogados.

- El artículo 6 de esta resolución, por medio del cual se modificó el artículo 6.1.1.5. de la Resolución CRC 5050 de 2016.

- El artículo 7 de esta resolución, por medio del cual se modificó el numeral 6.1.1.6.2. del artículo 6.1.1.6. de la Resolución CRC 5050 de 2016.

- El artículo 8 de esta resolución, por medio del cual se modificó el artículo 6.1.1.8. de la Resolución CRC 5050 de 2016.

- El artículo 9 de esta resolución, por medio del cual se modificó el artículo 6.4.2.1. de la Resolución CRC 5050 de 2016.

- El artículo 10 de esta resolución, por medio del cual se modificó el artículo 6.4.3.1. de la Resolución CRC 5050 de 2016.

- El artículo 11 de esta resolución, por medio del cual se modificó el artículo 6.4.3.2. de la Resolución CRC 5050 de 2016.

- El artículo 15 de esta resolución, por medio del cual se adicionó el Capítulo 14 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016.

- El artículo 16 de esta resolución, por medio del cual se adicionó un escenario de excepción al deber de publicación.

- El artículo 18 de esta resolución, el cual establece el proceso de selección de la persona jurídica que cumplirá las funciones del validador centralizado al que hace referencia el Capítulo 13 del TÍTULO VI de la Resolución CRC 5050 de 2016, sin perjuicio de que su ejecución material comience a partir de la publicación en el Diario Oficial del acto administrativo por medio del cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

- El artículo 19 de esta resolución, el cual establece el periodo de transición, sin perjuicio de que su ejecución material comience a partir de la publicación en el Diario Oficial del acto administrativo por medio del cual la CRC defina la nueva remuneración aplicable al ecosistema A2P.

**b. Una vez cumplido el periodo de transición establecido en el artículo 19 de esta resolución:**

- Las definiciones de CONOCIMIENTO DEL CLIENTE – KYC (KNOW YOUR CUSTOMER), PLANTILLA DE CONTENIDO A2P (TEMPLATED ID), SENDER ID, TRÁFICO A2P (APPLICATION TO PERSON) y VALIDADOR CENTRALIZADO adicionadas al TÍTULO I de la Resolución CRC 5050 de 2016 mediante el artículo 1 de esta resolución, sin perjuicio de lo cual el contenido de estas definiciones guiará el cumplimiento de las fases previstas en el periodo de transición previsto en el artículo 19 de esta resolución.

- Las definiciones del TÍTULO I de la Resolución CRC 5050 de 2016 que fueron modificadas mediante el artículo 2 de esta resolución, sin perjuicio de lo cual, el contenido de estas definiciones guiará el cumplimiento de las fases previstas en el periodo de transición previsto en el artículo 19 de esta resolución.

- El artículo 12 de esta resolución, por medio del cual se subrogó el Capítulo 4 del TÍTULO VI — Régimen de Administración de Recursos de Identificación — de la Resolución CRC 5050 de 2016, sin perjuicio de lo cual podrá ser aplicado por la CRC durante el periodo de transición establecido en el artículo 19 de esta resolución, únicamente para efectos de darle cumplimiento a las fases allí descritas.

- El artículo 13 de esta resolución, por medio del cual se adicionó el Capítulo 12 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, sin perjuicio de lo cual podrá ser aplicado por la CRC durante el periodo de transición establecido en el artículo 19 de esta resolución, únicamente para efectos de darle cumplimiento a las fases allí descritas.

- El artículo 14 de esta resolución, por medio del cual se adicionó el Capítulo 13 al TÍTULO VI – Régimen de Administración de Recursos de Identificación – de la Resolución CRC 5050 de 2016, sin perjuicio de lo cual podrá ser aplicado por la CRC durante el periodo de transición establecido en el artículo 19 de esta resolución, únicamente para efectos de darle cumplimiento a las fases allí descritas.

- El artículo 17, por medio del cual se adicionó un formato al TÍTULO REPORTES DE INFORMACIÓN de la Resolución CRC 5050 de 2016.

Dada en Bogotá D.C. a los XX días del mes de XX de 2026.

**PUBLÍQUESE Y CÚMPLASE**

**NOMBRE**
Presidente

**FELIPE AUGUSTO DÍAZ SUAZA**
Director Ejecutivo

Proyecto No: 2000-41-7-1

C.C.C. XX/XX/2026 Acta XXXX
S.C.C. XX/XX/2026 Acta XXX