



Superintendencia de
Industria y Comercio

Bogotá, D.C., junio de 2026

Señores

COMISIÓN DE REGULACIÓN DE COMUNICACIONES

medidasantifraude@crcom.gov.co

Asunto: Comentarios de la **SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO** al proyecto de resolución “*Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones*”. (en adelante, el “proyecto”).

Respetados Señores:

Esta Superintendencia realiza un seguimiento permanente a los proyectos normativos que puedan incidir en las funciones¹ que le han sido asignadas. En ese sentido, y después de haber adelantado la revisión de la iniciativa mencionada en el asunto, se reitera, como se ha señalado en otras oportunidades, la necesidad de garantizar los derechos de los usuarios de servicios de comunicaciones y de evitar que los mecanismos de mitigación se conviertan en una carga adicional para ellos, especialmente en temas de alta relevancia, como la prevención y atención de fraudes a través de servicios móviles. En ese orden de ideas, se presentan los siguientes comentarios a algunas de las disposiciones que hacen parte del articulado del “proyecto”:

1. FRENTE A LAS DEFINICIONES

Disposición	Propuesta del artículo, numeral, inciso u observación con modificación	Justificación de la propuesta u observación
Página 10 “ ARTÍCULO 1. Adiciónense las siguientes definiciones al TÍTULO I de la Resolución CRC 5050 de 2016:” “ ARTÍCULO 1. Adiciónense las siguientes definiciones al TÍTULO I de la Resolución CRC 5050 de 2016:“(…)”.	Se sugiere la inclusión en el “proyecto” de las definiciones de los siguientes conceptos: • MECANISMO VALIDACIÓN. DE • MECANISMO AUTENTICACIÓN. DE	Se considera importante crear una definición general, sin ser restrictiva de lo que se entiende por mecanismo de validación y mecanismo de autenticación, dependiendo el contexto. El primero de ellos aplicaría para el tráfico (A2P), el segundo, para el tráfico (P2P) y otros trámites. Lo anterior, con el fin de que, para aquellas transacciones o trámites que requieran la plena verificación de la identidad del usuario o suscriptor, se utilicen herramientas robustas como la biometría obligatoria, por ejemplo, si se trata de trámites presenciales.





Superintendencia de
Industria y Comercio

2. FRENTE A LA PREVENCIÓN DE FRAUDES

Disposición	Propuesta del artículo, numeral, inciso u observación con modificación	Justificación de la propuesta u observación
<u>Página 12</u> "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: (...)"	Se sugiere la inclusión del siguiente numeral: 2.1.10.7.1.3. Los operadores tienen la obligación de usar biometría y consultar las bases de datos de la Registraduría Nacional del Estado Civil, cuando usen este factor de autenticación, en las solicitudes o trámites presenciales que requieran la verificación de la identidad del usuario y establecer mecanismos alternativos para ello, cuando los trámites se puedan realizar por la línea de atención, la página web u otros canales digitales.	La inclusión de esta obligación permitirá: a. Que la verificación de identidad de los usuarios o titulares se realice por medio de mecanismos confiables, cuando el trámite lo requiera, en armonía con lo establecido en el artículo 2.1.25.1.3 de la Res. CRC 5050/16. b. Que los PRST tengan certeza de que quien se acerque a realizar un trámite en una oficina física o quien esté realizando la gestión por la línea gratuita, u otro medio de atención o canal digital, sea realmente el usuario o titular y no un tercero. Así como la garantía para los usuarios de que el operador debe hacer uso de herramientas o mecanismos fuertes de autenticación para verificar la identidad, complementado con otros medios alternativos, para completar el proceso de autenticación.
"ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES. Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude: (...) 2.1.10.7.2. Obligaciones particulares:	"ARTÍCULO 2.1.10.7. PREVENCIÓN DE FRAUDES. Los operadores tienen las siguientes obligaciones generales y particulares en relación con la prevención del fraude: (...) 2.1.10.7.2. Obligaciones particulares:	En relación con esta modificación, se encuentra que es más claro para el usuario y de mejor trazabilidad para el PRST, establecer que esta notificación sea realizada por medio del correo electrónico suministrado por el usuario.





Superintendencia de
Industria y Comercio

RECIBIDO

2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P. (...) 2.1.10.7.2.1.2. (...) 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, <u>a través del correo electrónico que el usuario haya suministrado, (...)</u> (Subrayado propio)	2.1.10.7.2.1. Obligaciones particulares en materia de prevención del fraude en relación con el tráfico P2P. (...) 2.1.10.7.2.1.2. (...) Segunda etapa – Notificación al usuario. (...), notificará al usuario titular de la línea o líneas afectadas, <u>a través del correo electrónico que el usuario haya suministrado, (...)</u>	
---	---	--

Con todo lo anterior, esperamos contribuir al enriquecimiento de tan importante iniciativa, quedando a disposición para resolver cualquier inquietud relacionada con el particular

Atentamente,


ALEJANDRO BUSTOS MENDOZA
JEFE OFICINA ASESORA JURÍDICA

Elaboró: David Mancera

Revisó: Clara Vega

Aprobó: Alejandro Bustos

