COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Digitally signed by MARIANA SARMIENTO ARGUELLO
Date: 2025.04.14 08:56:26 -05:00
Reason: Fiel Copia del Original
Location: Colombia

Rad. 2025802307
Cod. 2000
Bogotá, D.C.

CRC
Radicación: 2025511274
Fecha: 11/04/2025 5:18:20 P. M.
Proceso: 2000 DISEÑO REGULATORIO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

REF: Su comunicación con asunto «Solicitud de Información sobre Regulaciones y Supervisión en Suplantación de Identidad y Protección de Datos en el Sector de Telecomunicaciones»

La Comisión de Regulación de Comunicaciones (CRC) recibió comunicación bajo el radicado 2025802307 del 28 de febrero de 2025, mediante la cual solicita una serie de peticiones relacionadas con regulaciones y supervisión en Suplantación de Identidad y Protección de Datos en el Sector de Telecomunicaciones con el «propósito de evaluar información relacionada con regulaciones, normativas y políticas aplicables al sector de telecomunicaciones en cuanto a la prevención de suplantación de identidad, la protección de datos y seguridad implementadas por los operadores de telecomunicaciones, en aras de garantizar que los usuarios cuenten con un entorno seguro para el uso de sus servicios.»

A. Alcance del presente pronunciamiento

Antes de proceder a responder sus inquietudes, consideramos pertinente mencionar que el pronunciamiento que presenta esta Comisión en relación con los asuntos expuestos en su escrito de consulta se efectúa con sujeción de lo establecido en el artículo 28 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo -CPACA[1]- y de las competencias que se le han otorgado en el ordenamiento jurídico vigente. Considerando lo establecido en la norma citada, el pronunciamiento sobre los asuntos contenidos en su consulta tendrá el alcance y las consecuencias definidas en la normatividad aplicable, al tratarse conceptos emitidos por autoridades administrativas.

En igual sentido, tenga en cuenta que en sede de esta consulta no es dable que se emitan pronunciamientos o se analicen situaciones de carácter particular y concreto, pues el resultado de

[1] Artículo 28. Alcance de los conceptos. Salvo disposición legal en contrario, los conceptos emitidos por las autoridades como respuestas a peticiones realizadas en ejercicio del derecho a formular consultas no serán de obligatorio cumplimiento o ejecución.

éste no desbordará los asuntos a los que se hace referencia a la materia por la cual se pregunta de manera general y abstracta, y sobre el contenido y aplicación del marco regulatorio; en este caso, lo correspondiente a las disposiciones legales y regulatorias, en lo relativo a las temáticas objeto de su consulta.

B. Consideraciones preliminares sobre las competencias de esta Comisión

Teniendo en cuenta el contexto general respecto del cual se enmarcan los asuntos que son materia de consulta, resulta oportuno señalar que según lo dispuesto por el artículo 19 de la Ley 1341 de 2009, modificada por la Ley 1978 de 2019, la CRC es «una Unidad Administrativa Especial, del orden nacional, con independencia administrativa, técnica, patrimonial, presupuestal, y con personería jurídica, la cual forma parte del Sector administrativo de Tecnologías de la Información y las Comunicaciones». A su turno, esta misma norma estableció que la CRC es el órgano encargado de promover la competencia en los mercados, promover 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, de las redes y los servicios de comunicaciones, incluidos los servicios de televisión abierta radiodifundida y de radiodifusión sonora.

De igual manera, la norma referida dispone que la CRC debe adoptar una regulación que promueva la inversión, la protección de los usuarios, la calidad de los servicios, la simplificación regulatoria, la neutralidad de la red, e incentive la construcción de un mercado competitivo que desarrolle los principios orientadores de la misma Ley 1341 de 2009.

Para desarrollar el anterior objeto misional, el legislador otorgó directamente a la CRC, a través del artículo 22 de la Ley en comento, modificada por la Ley 1978 de 2019, así como de la Ley 1369 de 2009, facultades que típicamente debe ostentar un regulador para promover la competencia en los servicios de telecomunicaciones, maximizar el bienestar de los usuarios, regular el acceso y uso de instalaciones esenciales necesarias para facilitar la entrada de agentes al mercado, definir las condiciones para la interconexión y la interoperabilidad de las redes de telecomunicaciones, regular el uso adecuado de los recursos escasos diferentes al espectro, proteger el pluralismo y las audiencias, solucionar controversias y promover y garantizar los derechos de los usuarios de los servicios de comunicaciones, en términos generales.

Sobre la base de las precisiones anotadas, también se considera pertinente aclarar que la CRC no ejerce funciones de inspección, vigilancia y control en materia de los asuntos relacionados con la protección de datos. Las facultades de inspección, vigilancia y control sobre los asuntos derivados de este asunto se encuentran a cargo de la Superintendencia de Industria y Comercio (SIC).

C. Las respuestas a las solicitudes planteadas

Entendido lo anterior, la CRC procede a responder puntualmente a sus solicitudes, así:

«**1.1 Normativas y directrices sobre suplantación de identidad:**

- Solicito un listado detallado de las normativas y directrices expedidas por la CRC entre los años 2020 y 2025 sobre prevención de suplantación de identidad y autenticación en el sector de telecomunicaciones, indicando su fecha de expedición, su campo de aplicación y si han sido objeto de actualización o modificación.
- Solicito información detallada sobre los estándares de autenticación que la CRC recomienda a los operadores de telecomunicaciones en Colombia.
En particular, solicito conocer los lineamientos específicos sobre autenticación multifactor y el uso de biometría.
- Solicito un resumen detallado de las mejores prácticas en verificación de identidad sugeridas por la Comisión de Regulación de Comunicaciones (CRC) para operadores de telecomunicaciones y proveedores de servicios digitales en Colombia.»

RESPUESTA:

En la regulación de carácter general dispuesta en la Resolución Compilatoria CRC 5050 de 2016 en numeral 2.7.2.1.24. del artículo 2.7.2.1, modificado por el artículo 21 de la Resolución 5586 de 2019, la Comisión dispuso como obligación de los Proveedores de Redes y Servicios de Telecomunicaciones Móviles -PRSTM-, lo siguiente:

> «Implementar un proceso de identificación y validación del usuario para que cuando este solicite el desbloqueo de un equipo que fue reportado inicialmente como hurtado o extraviado, el PRSTM asegure que el usuario que realizó el reporte del equipo sea el único que puede solicitar su desbloqueo. Para este proceso de validación y como requisito previo para el desbloqueo del equipo, el PRSTM debe validar la identidad del usuario, para lo cual debe realizar alguno de los siguientes métodos de verificación: i) requerir el código o clave que fue entregado al usuario durante el proceso de reporte, o ii) requerir la presentación personal del usuario con el equipo recuperado, o iii) autenticar la identidad del usuario titular de la línea a través de los sistemas y aplicativos que para tal fin disponen las centrales de riesgo, o a través de medios biométricos, o realizando preguntas relacionadas con la actividad de la línea a reactivar.»

De acuerdo con lo anterior, los operadores de servicios de telecomunicaciones móviles deben contar con las herramientas tecnológicas para prevenir el fraude e identificar y validar la identificación de sus usuarios. Mecanismos que van más allá de una simple revisión documental de la cédula y otros documentos y cuyo incumplimiento es sancionable por las autoridades de inspección, vigilancia y control.

Vale la pena aclarar que durante los años 2020 al 2025 la CRC no ha expedido lineamientos o directrices específicas sobre sobre prevención de suplantación de identidad y autenticación en el sector de telecomunicaciones o verificación de identidad. Como tampoco ha expedido lineamientos específicos sobre autenticación multifactor y el uso de biometría.

De igual manera, debe esta Comisión señalar que no reglamenta la operación y funcionamiento de los servicios digitales OTT (Over the Top), referidos a las plataformas que utilizan las redes de Internet existentes para ofrecer soluciones como mensajería, redes sociales, contenido audiovisual, llamadas y comercio electrónico que utilizan la red de Internet, ya que, de acuerdo con lo mencionado anteriormente, la CRC no tiene competencias para establecer regulación al respecto. Por lo tanto, adicionalmente cabe señalar que dentro de los archivos de la Comisión no se encuentra ningún documento del que se pueda extraer un resumen detallado de las mejores prácticas en verificación de identidad para el sector de las telecomunicaciones.

> **«1.2 Medidas de supervisión y cumplimiento normativo:**
>
> - Solicito un informe detallado sobre los mecanismos de supervisión utilizados por la Comisión de Regulación de Comunicaciones (CRC), y los criterios de evaluación para verificar el cumplimiento en el sector de telecomunicaciones y tecnologías de la información.
> - Solicito un reporte de auditorías y visitas de inspección realizadas en los últimos tres años sobre estas materias Traduce a español: (en la medida en que la información no sea de carácter reservado).
> - Solicito información detallada sobre sanciones o acciones correctivas impuestas por la Comisión de Regulación de Comunicaciones (CRC) en casos de incumplimiento normativo en los últimos 3 años.»

RESPUESTA:

Lo primero que debe ponerse de presente, de acuerdo con las aclaraciones normativas realizadas previamente, es que, al ejercer su labor regulatoria, la CRC lo debe hacer respecto de aquellos asuntos frente a los cuales el legislador dispuso que versarían sus competencias. En otras palabras, la CRC regula solo aquello que la ley dispuso que puede regular.

Es por lo descrito que, esta Comisión no tiene funciones de supervisión o de realización de auditorías, razón por la cual no se cuenta con ningún protocolo o mecanismo de supervisión como tampoco reportes de auditorías realizadas al sector de telecomunicaciones. Es importante aclarar que estas funciones corresponden al Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en lo que respecta a la vigilancia, inspección y control de la regulación, y a la Superintendencia de Industria y Comercio (SIC), en lo relativo a la protección de los usuarios y la protección de los datos personales.

> **«1.3 Regulaciones específicas sobre protección de datos personales:** Solicito un resumen de las regulaciones expedidas por la CRC entre los años 2020 y 2025 en materia de protección de datos personales y prevención de accesos no autorizados en el sector de telecomunicaciones, incluyendo los requerimientos mínimos de seguridad exigidos a los operadores para el tratamiento y resguardo de datos personales.»

RESPUESTA:

De acuerdo con lo explicado previamente, en cuanto a las disposiciones legales que determinan las competencias de la CRC, así como respecto de los asuntos que en virtud de tales competencias

la CRC ha expedido regulación, debe esta Comisión informar que no dispone de ninguna reglamentación o normativa específica relacionada en materia de protección de datos personales y prevención de accesos no autorizados en el sector de telecomunicaciones y, por ende, no ha establecido requisitos o permisos para el uso de la imagen en ningún medio de comunicación.

Sin embargo, debe destacar esta Comisión que la autorización por parte del usuario para la recolección, almacenamiento, uso, circulación y actualización de sus datos personales por parte del operador; la finalidad que se le dará a los mismos; los derechos con que cuenta el usuario respecto de dichos datos; así como las condiciones en que procede la revocatoria de la autorización que el usuario otorgó al operador para el uso y circulación de sus datos personales, deben en todo momento atender y dar cumplimiento a las normas vigentes en materia de protección de datos personales, esto es, la Ley 1581 de 2012 o cualquier norma que la modifique, complemente o sustituya.

Recuerde que la Entidad que vigila y controla el cumplimiento de las obligaciones establecidas en la mencionada ley es la Superintendencia de Industria y Comercio (SIC).

> **«1.4 Estadísticas de cumplimiento normativo y reportes de incidentes:** Solicito estadísticas disponibles sobre incidentes de suplantación de identidad en telecomunicaciones, especificando el número de casos reportados anualmente y su clasificación según el tipo de afectación. Asimismo, requiero información sobre el nivel de cumplimiento normativo de los operadores en relación con estas incidencias.»

RESPUESTA:

De manera atenta le informamos que conforme a lo establecido en el Artículo 4 de la Resolución 5569 de 2018, los PRST deberán hacer el respectivo reporte de incidentes de seguridad de la información al Grupo de Respuesta de Emergencias Cibernéticas de Colombia (colCERT) conforme a lo establecido en el numeral 5.1.2.3.3 del artículo 5.1.2.3 de la Resolución 5050 de 2016, el cual establece, entre otros, lo siguiente:

> «5.1.2.3.3 Reporte de incidentes de seguridad de la información a las autoridades. Cuando se presenten incidentes de seguridad de la información, los PRST deberán enviar por medios electrónicos, después del cierre del incidente, esto es después de su contención, erradicación o recuperación, un reporte al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (colCERT), o quien haga sus veces, que incluya los elementos descritos en el numeral 5.1.2.3.2 del presente artículo, (fecha del incidente, servicio afectado, número de usuarios afectados, duración, categoría de incidente) y una descripción del incidente, así como de las acciones llevadas a cabo por el proveedor para mitigar o resolver el incidente, en todo caso el tiempo para el envío del reporte no podrá exceder los tres (3) meses, subsecuentes a la fecha de detección del incidente.»

> **«1.5 Proyectos y actualizaciones normativas en desarrollo:** Solicito información sobre proyectos normativos o actualizaciones en desarrollo entre 2023 y 2025, orientados a mejorar la seguridad de autenticación dentro del sector de telecomunicaciones.»

RESPUESTA:

La CRC En el marco del proyecto regulatorio "Revisión de medidas regulatorias aplicables a servicios móviles - fase 2", la CRC expidió la Resolución 7684 de 2025[2], mediante la cual establece un conjunto de medidas diseñadas para promover la competencia y mejorar la experiencia de los usuarios de servicios de telefonía móvil, Internet móvil y servicios empaquetados de voz e Internet. Con esta medida la CRC refuerza la protección de los derechos de los usuarios mediante la eliminación de barreras a la portabilidad numérica móvil y el fortalecimiento de los canales digitales de atención.

De igual manera, se informa que dentro de la Agenda Regulatoria 2025-2026, en el eje temático de Bienestar y Derechos de los Usuarios y Audiencias, se incluye el proyecto titulado "Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles". Con esta iniciativa se analizarán las medidas que deben ser adoptadas por los Proveedores de Contenidos y Aplicaciones (PCA) e integradores tecnológicos, asignatarios de códigos cortos, para la prevención de fraudes. Se revisará la pertinencia de definir obligaciones adicionales a los agentes que participan en la provisión de contenido y aplicaciones en las redes de servicios móviles mediante SMS y los requisitos para la asignación y recuperación de la numeración de códigos cortos para SMS.

Por último, se informa que la CRC no ha desarrollado proyectos regulatorios orientados a mejorar la seguridad de autenticación en el sector de telecomunicaciones. Si desea conocer las acciones regulatorias que la Comisión ha implementado y tiene previsto ejecutar durante el año 2025, lo invitamos a consultar el siguiente enlace, donde se publica, desglosado por año, la agenda regulatoria. Esta agenda permite conocer y debatir oportunamente las próximas acciones de regulación previstas a corto y mediano plazo. Enlace: https://www.crcom.gov.co/es/agenda-regulatoria

> **«1.6 Protocolos de atención al usuario y medidas preventivas:** En ejercicio del derecho de acceso a la información pública, conforme a la Ley 1712 de 2014, solicito amablemente un resumen de los protocolos de atención al usuario y medidas preventivas recomendadas por la CRC en materia de suplantación de identidad en el sector de telecomunicaciones. Adicionalmente, agradecería información sobre campañas educativas desarrolladas en los últimos años para la sensibilización y prevención de este delito.»

RESPUESTA:

[2] Disponible en línea en: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-38-3-17-1

La CRC ha dispuesto de un Régimen de Protección de los Derechos de los Usuarios de Servicios de comunicaciones (RPU) contenido en la Resolución CRC 5111 de 2017 y compilado en el Capítulo 1 del Título II de la Resolución CRC 5050 de 2016, dicho régimen corresponde a los distintos tipos de relacionamiento que pueden ocurrir entre el operador y el usuario, con ocasión de la prestación de los servicios de comunicaciones.

Dentro de este Régimen, el artículo 2.1.10.7 establece las condiciones para la prestación del servicio, señalando:

> **Prevención de Fraudes.** 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.
>
> 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.

Como se puede ver de la redacción de la disposición regulatoria citada, el propósito de la referencia a la realización de fraudes es prevenir que se realicen conductas engañosas o por parte de terceros no autorizados que puedan resultar en un detrimento o afectación para los usuarios. Para ello, en su segundo inciso, la norma impone obligaciones de prevención, atención y corrección en cabeza de los Proveedores de Redes y Servicios de Telecomunicaciones para aquellos casos en los que con ocasión de una conducta de este tipo pueda verse afectado un usuario.

> **«1.7 Recomendaciones para una autenticación segura:** Solicito de manera respetuosa información detallada sobre las recomendaciones y directrices técnicas emitidas por la CRC en relación con la implementación de mecanismos de autenticación segura en los servicios de telecomunicaciones y las mejores prácticas internacionales reconocidas o referenciadas por la CRC en esta materia.»

La CRC ha incorporado en su regulación varias recomendaciones de la UIT en materia de servicios de telecomunicaciones.

En este sentido, se ha establecido dentro de su normativa[3] que los proveedores de redes y servicios de telecomunicaciones que ofrecen acceso a Internet deben utilizar los recursos técnicos y logísticos necesarios para garantizar la seguridad de la red, la inviolabilidad de las comunicaciones, la protección contra virus y la integridad del servicio. Dicho proceso debe realizarse mediante el uso de herramientas tecnológicas y modelos de seguridad acordes con las características y necesidades específicas de cada red de acceso, conforme a lo definido por la UIT en las recomendaciones de la serie X.800, relativas a autenticación, acceso, no repudio, confidencialidad

[3] Artículo 2.9.2.3. Seguridad de la Red, Capítulo 9, del título II de la Resolución CRC 5050 de 2016

e integridad de datos y disponibilidad, según lo estipulado en el Artículo 5.1.2.3[4] del Capítulo I del Título V, o la norma que lo modifica, adición o sustitución.

Asimismo, los proveedores que facilitan el acceso a Internet a través de redes móviles deberán implementar modelos de seguridad que prevengan el acceso no autorizado, la interrupción, el repudio o la interferencia deliberada de la comunicación. Para ello, se deberá recurrir a modelos de cifrado, firmas digitales y controles de acceso descritos en las recomendaciones UIT X.1121 y X.1122, en los términos establecidos en el Artículo 5.1.2.3 del Capítulo I del Título V o en la norma que lo modifique, adicione o sustituya.

En los anteriores términos damos respuesta a su comunicación y quedamos atentos a cualquier aclaración adicional que requiera.

Cordial saludo,

MARIANA SARMIENTO ARGUELLO

Firmado digitalmente por MARIANA SARMIENTO ARGUELLO
Fecha: 2025.04.14 09:21:52 -05'00'

MARIANA SARMIENTO ARGÜELLO
Coordinadora de Relaciones con Grupos de Valor

Proyectado por: Jenny Rojas Granados
Revisado por: Alejandra Arenas Pinto

[4] Gestión de seguridad de la información en redes de telecomunicaciones