COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES

Documento de formulación del problema

Diseño Regulatorio

Julio de 2025

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

CONTENIDO

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES

1. INTRODUCCIÓN

En cumplimiento de las funciones legales dispuestas en los numerales 12[1] y 13[2] del artículo 22 de la Ley 1341 de 2009, modificado por el artículo 19 de la Ley 1978 de 2019, la Comisión de Regulación de Comunicaciones (CRC) ejerce la administración y regulación de los recursos de identificación en Colombia, bajo principios de eficiencia, disponibilidad y protección del interés general. Esta competencia se materializa en la asignación, modificación y recuperación de dichos recursos, así como en el seguimiento a su uso eficiente por parte de los asignatarios.

Es importante mencionar que, en el marco de los servicios de telecomunicaciones, los recursos de identificación, como la numeración usada para identificar los usuarios de telefonía fija y móvil (conocida como numeración E.164), los códigos cortos mediante los que se envían campañas publicitarias usando mensajes cortos de texto (SMS) y otros identificadores técnicos, desempeñan un papel fundamental para habilitar la originación, direccionamiento y autenticación de las comunicaciones[3].

Estos recursos permiten individualizar terminales, usuarios y servicios dentro de las redes, y son la base sobre la cual se soporta una parte importante de la interacción entre operadores, plataformas digitales y usuarios finales. Su uso adecuado, trazable y transparente resulta esencial no solo para la eficiencia del ecosistema, sino también para la protección de los derechos de los usuarios y la integridad de las comunicaciones.

Sin embargo, el aumento de la penetración de los servicios de telecomunicaciones ha traído consigo nuevos desafíos, particularmente en lo relacionado con las acciones irregulares orientadas al fraude cibernético. Mediante el uso de servicios tradicionales como las llamadas de voz y los SMS se ejecutan campañas maliciosas que buscan persuadir los usuarios para estafarlos, o capturar información sensible para, posteriormente, suplantar su identidad. Estas prácticas como el *smishing* (ejecutada mediante SMS) y el *vishing* (ejecutada por medio de llamadas de voz), afectan no solo la confianza de los usuarios, sino también la credibilidad y seguridad de los servicios de telecomunicaciones.

Si bien la CRC ha establecido obligaciones generales para promover la seguridad de la información en las redes de telecomunicaciones[4], esta Entidad ha identificado una tendencia creciente en la ocurrencia y reporte de dichos incidentes. En particular, estos hechos se reflejan en el aumento del 244,1% en la

[1] «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 -.co-».
[2] «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».
[3] International Telecommunication Union. (2020). ITU-T Recommendation E.101: Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations. [En línea]. Disponible en: https://www.itu.int/rec/T-REC-E.101/en
[4] Resolución CRC 5050 de 2016. Artículos 5.1.2.3.1, 5.1.2.3.2, 5.1.2.3.3.

recepción de PQR por contenido fraudulento, así como en un mayor número de actos administrativos y de recuperación de códigos cortos expedidos por uso indebido, con un incremento del 20,0% y 25,0%, tan solo cuando se compara lo ocurrido en el primer trimestre del 2025 frente al promedio anual observado para 2022-2024.

A esto se suma el crecimiento sostenido del 11% promedio anual en las denuncias registradas sobre delitos informáticos, de acuerdo con cifras del Observatorio de Derechos Humanos y Defensa Nacional del Ministerio de Defensa Nacional, y del 19% en las quejas relacionadas con posibles vulneraciones al tratamiento de datos personales según cifras de la Superintendencia de Industria y Comercio (SIC). Así mismo, las entidades y empresas que son usuarias o asignatarias de recursos de identificación también han experimentado un aumento exponencial en la detección de incidentes asociados a acciones irregulares con fines de fraude.

En este contexto, la Agenda Regulatoria CRC 2025-2026[5] incorporó como uno de sus proyectos prioritarios la *Identificación de medidas regulatorias para mitigar el fraude cibernético por medio de servicios móviles*, con el propósito de diagnosticar el problema, proponer y evaluar alternativas regulatorias y no regulatorias que refuercen la trazabilidad y control de las comunicaciones que hacen uso de recursos de identificación en servicios móviles, sin limitar la innovación o el acceso a estos servicios por parte de actores legítimos.

Cabe indicar que la CRC es consciente de que esta problemática desborda su marco competencial y reconoce, como lo han hecho otros reguladores en el mundo, que exige la coordinación y definición de una estrategia conjunta, intersectorial y que, incluso, involucre a actores del sector privado. Es por ello que, con este proyecto regulatorio, se busca generar un foco especial en los usuarios de servicios tradicionales de telecomunicaciones móviles que, si bien no son los únicos medios por los que se pueden contactar personas y dichos usuarios no son las únicas víctimas –dada la diversidad de modalidades y mecanismos de fraude que se utilizan y su rápida evolución e innovación–, tiene como finalidad aportar en la definición de condiciones de seguridad más exigentes en las comunicaciones y en otorgar herramientas claras a los usuarios para mitigar las probabilidades de convertirse en nuevas víctimas de fraude cibernético.

En este sentido, este documento tiene como objetivo formular el problema regulatorio, describir y evidenciar sus causas y consecuencias, y estructurar la planeación del proyecto conforme a los lineamientos de la metodología de Análisis de Impacto Normativo (AIN). De igual manera, con el ánimo de involucrar a los distintos grupos de valor que han manifestado su interés en participar activamente en todo el proceso de construcción de una posible propuesta de regulación, este documento contiene una consulta pública que se enfoca en preguntar por diferentes posibles soluciones, con el fin de identificar su viabilidad respecto de cada uno de los actores involucrados en las cadenas de la comunicación.

Así las cosas, se presenta un diagnóstico técnico, jurídico y de mercado, se definen objetivos y alcance, y se establece el marco general en el cual se trabajará para identificar la solución al problema que resulte más eficiente. La estructura del documento incluye esta introducción, el planteamiento del problema y diagnóstico integral de las causas y consecuencias, el análisis contextual, incluyendo la

[5] CRC. Agenda Regulatoria 2025-2026. [En línea]. Disponible en: https://www.crcom.gov.co/sites/default/files/agenda/agenda-regulatoria-2025-2026.pdf

revisión de experiencias internacionales, y la sección de consulta pública para que todos los interesados presenten sus observaciones y sugerencias.

2. COMENTARIOS DEL SECTOR SOBRE MEDIDAS DE PREVENCIÓN ANTE EL FRAUDE PRESENTADOS EN EL MARCO DE LA INICIATIVA REGULATORIA DE SIMPLIFICACIÓN Y LA CONVOCATORIA 2025 AL SANDBOX REGULATORIO CONVERGENTE

Con el fin de reconocer la preocupación generalizada que han expresado los distintos grupos de valor sobre la comisión de fraude mediante servicios de telecomunicaciones, y tenerlos en cuenta en la construcción de la identificación del problema, objetivos del proyecto y alternativas de solución preliminares, en la presente sección se traen a colación los comentarios, observaciones y sugerencias que se presentaron, por un lado, con relación a las medidas de prevención, en el marco de la discusión sectorial de la propuesta regulatoria del proyecto *Simplificación del marco regulatorio 2024*, publicada el 20 de diciembre de 2024; y, por el otro, las propuestas presentadas en la convocatoria 2025 al Sandbox Regulatorio Convergente.

En línea con lo anterior, primero se transcriben los comentarios presentados por **COMUNICACIÓN CELULAR S.A.** (**COMCEL**), **HABLAME COLOMBIA S.A. E.S.P.** (**HABLAME**), **PARTNERS TELECOM COLOMBIA S.A.S. EN REORGANIZACIÓN** (**PTC**), **COLOMBIA TELECOMUNICACIONES S.A. E.S.P BIC** (**TELEFÓNICA**) y el ciudadano **RODRIGO MONTUFAR**, en los términos del documento de respuestas a comentarios de las Resoluciones CRC 7810 y 7811 de 2025, para luego proceder a presentar la debida respuesta a partir de los análisis efectuados en el marco de esta iniciativa regulatoria.

COMCEL

En relación con la recuperación de códigos cortos, señala que resultaría útil establecer consecuencias para los casos en los que mediante dichos recursos se esté facilitando, promoviendo o permitiendo el fraude cibernético. Una de tales consecuencias, afirma, debería ser la posibilidad de dar por terminada la relación de acceso o interconexión cuando se haya recuperado numeración por su uso indebido (art. 6.4.3.2.). A lo anterior agrega que es necesario que la CRC agilice los procedimientos de recuperación de numeración en los casos en que esta se esté usando en contravía de la regulación, así como también que la CRC notifique a los operadores sobre tal recuperación para así evitar el envío de mensajes de contenido fraudulento.

HABLAME

Propone que el estándar de seguridad aplicable al servicio de voz, que requiere un enlace dedicado punto a punto, se extienda también a los mensajes de texto (SMS). Debido a que muchas entidades bancarias, gubernamentales y comerciales utilizan SMS para enviar información crítica. Argumenta que las VPN, aunque cifran los datos, dependen de la infraestructura de internet y están expuestas a múltiples amenazas. Indica que la UIT recomienda un enfoque integral de seguridad en redes de extremo a extremo (ITU-T X.805) y contramedidas para mitigar riesgos de ciberseguridad (ITU-T X.1205). Así mismo, en Europa, el Reglamento General de Protección de Datos (RGPD) y la Directiva

de Servicios de Pago (PSD2) fomentan infraestructuras seguras, mientras que en Norteamérica se restringe la transmisión de datos sensibles a canales controlados.

Transmitir SMS por internet puede exponerlos a ataques que bloqueen la comunicación, afectando la entrega de códigos OTP y claves bancarias, lo que puede resultar en bloqueos de cuentas y riesgo de fraude. Además, las VPN pueden ser vulnerables a ataques avanzados, manipulaciones de autenticación y problemas de congestión, pueden retrasar o extraviar mensajes SMS.

Así las cosas, **HABLAME** recomienda adoptar un enlace dedicado para SMS para mejorar la seguridad, reducir vulnerabilidades y cumplir con normativas de protección de datos. Además, sugiere que la CRC revise la normativa para incluir medidas de seguridad avanzadas como el cifrado de extremo a extremo y el monitoreo continuo de los enlaces dedicados, y permitir auditorías de seguridad para verificar el cumplimiento de estas exigencias y garantizar la protección de los usuarios.

PTC

Respecto del artículo 2.1.10.7 de la Resolución CRC 5050 de 2016, indica que está de acuerdo con la propuesta de modificación planteada por la CRC, sin embargo, sugiere que se amplíe el impacto de la medida en el sentido de señalar que se busca prevenir y detectar los posibles comportamientos irregulares. Al respecto, propone la siguiente redacción:

> «**ARTÍCULO 2.1.10.7. PREVENCIÓN Y DETECCIÓN DE ~~FRAUDES~~COMPORTAMIENTOS IRREGULARES.** Los operadores tienen la obligación de hacer uso de herramientas tecnológicas adecuadas para prevenir y/o detectar irregularidades ~~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 una presunta~~o~~ irregularidad en el uso o contratación del servicio ~~fraude~~, el operador debe investigar sus causas; y en caso de que determine la no existencia de esa irregularidad ~~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 servicios objeto de reclamación». (SPT).

TELEFÓNICA

Hace referencia al estudio «Analysys Mason - El mercado de mensajería A2P: problemáticas, retos y recomendaciones para Hispanoamérica», del cual destaca las siguientes recomendaciones sobre los mercados de mensajería: (i) menor regulación, (ii) diferenciación entre A2P y P2P, (iii) evitar la regulación asimétrica y (iv) trazabilidad y seguridad, donde se resalta que los operadores deberían poder verificar el origen del tráfico A2P, sobre todo en tráfico de interconexión.

Adicionalmente, señala las siguientes recomendaciones sobre mensajes spam: colaboración público-privada para combatir el spam y los fraudes; aprovechamiento de la IA para la detección y filtrado de spam y un marco regulatorio que promueva la inversión.

RODRIGO MONTUFAR

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Con respecto a la modificación del Artículo 2.1.18.6. «PREVENCIÓN DE COMPORTAMIENTOS IRREGULARES y DELITOS A CARGO DE LOS PCA E INTEGRADORES ASIGNATARIOS DE CÓDIGOS CORTOS» señala que los PCA e IT no solo son asignatarios de códigos cortos sino de otros recursos de identificación, por tanto, afirma que en el artículo se «debe ampliar el alcance a Recursos de Identificación pues las irregularidades y la comisión de delitos no es solo por SMS o USSD, también por llamadas de Voz, entre otros medios.

Sobre el mismo artículo señala que «El usuario que solicita investigación del SMS irregular no debe demostrar que la URL y el texto recibido es irregular, es deber del PCA analizarlo a tiempo, pues estas url desaparecen rápidamente». (sic)

Así mismo, indica que no se está cumpliendo el mandato del ARTÍCULO 2.1.19.9. sobre identificación del PCA, por lo cual señala que el hecho de que el SMS no cumpla con dicha identificación debería constituirse como una causal de bloqueo del recurso de identificación. En ese sentido, sugiere la siguiente redacción:

> «ARTÍCULO 2.1.18.6. PREVENCIÓN DE COMPORTAMIENTOS IRREGULARES Y DELITOS A CARGO ~~POR PARTE FRAUDES~~ DE LOS PCA E INTEGRADORES TECNOLÓGICOS ASIGNATARIOS DE ~~**CÓDIGOS CORTOS**~~ **RECURSOS DE IDENTIFICACIÓN**. Los PCA e Integradores Tecnológicos que sean asignatarios de ~~**códigos cortos**~~ **Recursos de identificación** deberán hacer uso de herramientas tecnológicas para prevenir irregularidades y la comisión de delitos ~~fraudes~~ a través del envío de mensajes SMS o USSD o **llamadas de voz**. Adicionalmente, deberá efectuar controles periódicos respecto de la efectividad de los mecanismos dispuestos para tal fin».

Frente a la modificación propuesta sobre los artículos 2.1.24.2. PRESENTACION DE PQR, y 2.1.24.7 SEGUIMIENTO DE LAS PQR, considera que no existe un mecanismo para presentar PQR ante los PCA e IT, para lo cual propone las siguientes redacciones:

> «ARTÍCULO 2.1.24.2. PRESENTACIÓN DE PQR. El usuario tiene derecho a presentar una PQR (petición, queja/reclamo o recurso) ante su operador, **PCA o IT** en cualquier momento sin que este último pueda imponer alguna condición~~, y~~. El usuario podrá presentar una PQR a través de cualquiera de los medios de atención del operador, **PCA o IT** (salvo que la respectiva interacción objeto de PQR haya migrado a la digitalización y se le haya informado previamente al usuario), así el servicio se encuentre suspendido. No obstante, ~~En todo caso~~ el usuario siempre podrá presentar su PQR a través de la línea de atención telefónica.»
>
> «ARTÍCULO 2.1.25.1. REQUISITOS DE LOS MEDIOS DE ATENCIÓN. Los medios de atención descritos en este capítulo ~~y~~, así como los adicionales que disponga el operador, **PCA e IT**, deben cumplir las siguientes condiciones:
>
> 2.1.25.1.1. Cuando el usuario presente una PQR (petición, queja/reclamo o recurso) el operador, **PCA e IT,** en ninguna circunstancia puede exigirle que se remita a un medio de atención distinto, (salvo cuando la respectiva interacción objeto de PQR haya migrado a la digitalización y se le haya informado previamente al usuario)».

Frente a la propuesta de modificación del artículo 6.4.3.2 CAUSALES DE RECUPERACIÓN DE LA NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD, considera que se deben incluir causales de recuperación aplicables a recursos de identificación diferentes a códigos cortos, por lo cual sugiere

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

«reemplazar (códigos cortos) por (Recursos de Identificación para SMS, USSD y Voz) en todo el Artículo 6.4.3.2 y sus sub artículos» (sic), de la siguiente forma:

> «ARTÍCULO 6.4.3.2. CAUSALES DE RECUPERACIÓN DE **Recursos de Identificación para SMS, USSD y Voz** ~~LA NUMERACIÓN DE CÓDIGOS CORTOS PARA SMS Y USSD~~. El Administrador de los Recursos de Identificación podrá recuperar total o parcialmente la numeración de **Recursos de Identificación para SMS, USSD y Voz** ~~códigos cortos para SMS y USSD~~ asignada conforme el procedimiento de recuperación establecido en el ~~numeral 6.1.1.8.1. del ARTÍCULO~~ artículo 6.1.1.8. ~~de la SECCIÓN 1 del CAPÍTULO 1 del TÍTULO VI~~, cuando el asignatario incumpla con alguno de los criterios de uso eficiente establecidos en el ARTÍCULO 6.4.3.1. de la SECCIÓN 3 del CAPÍTULO 4 del TÍTULO VI, o incurra en alguna de las siguientes causales de recuperación:»

Repuesta CRC

Tal como se indicó en el documento de respuestas a comentarios, que hace parte de las Resoluciones CRC 7810 y 7811 de 2025, las observaciones y sugerencias planteadas por **COMCEL**, **HABLAME**, **PTC**, **TELEFÓNICA** y el ciudadano **RODRIGO MONTUFAR** hacen referencia a diferentes modificaciones de fondo sobre los textos normativos de algunas medidas regulatorias vigentes en materia de recursos de identificación, y otras están relacionadas con adicionar obligaciones en cabeza de diferentes agentes intervinientes en la cadena de valor definida en función del flujo de la comunicación, esto es: los Proveedores de Redes y Servicios de Telecomunicaciones (PRST), Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT), como se explica en detalle en la sección 4.1.4 de este documento.

Por esta razón, dichos comentarios fueron trasladados a esta iniciativa regulatoria, con el fin de tenerlos en consideración en los diferentes análisis que se realicen en cada una de las etapas del proyecto, las cuales, además, serán puestas a disposición de todos los grupos de valor como parte de la discusión sectorial que esta Comisión ha implementado como buena práctica en el diseño y desarrollo de su regulación, reiterando su compromiso con el involucramiento de los interesados desde la etapa inicial de las iniciativas que desarrolla.

Así las cosas, en la medida en que mediante este documento no solo se presenta el problema identificado y los objetivos del proyecto, sino también una consulta pública con la que se pretende indagar sobre la viabilidad de posibles alternativas que esta Comisión ha identificado de manera preliminar para solucionar las diferentes aristas que conforman dicho problema, es claro que las observaciones y recomendaciones presentadas por la industria y el ciudadano fueron tenidas en cuenta en la construcción de cada uno de estos componentes y, de acuerdo con ello, definir el enfoque y alcance del proyecto.

De esta manera, se informa que, como se explica en detalle en la subsección 4.2, el problema identificado por esta Comisión es «ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto», el cual se construyó a partir de la contextualización que se realiza en la subsección 4.1, en el que se insertan varias de las sugerencias presentadas en sus comentarios y en la respuesta al requerimiento de

información particular que se realizó a asignatarios y usuarios del recurso de identificación de códigos cortos[6].

Como consecuencia de lo anterior, en la sección 7 se plantea una consulta pública que incluye la primera aproximación a diferentes alternativas de solución posibles que identificó la CRC para resolver las preocupaciones de los grupos de valor y las situaciones problemáticas que se describen en este documento. De esta manera, tomando propuestas como la de **TELEFÓNICA** y **HABLAME**, y a partir del estudio de las experiencias regulatorias de otros países que han abordado problemas relacionados con fraude cibernético, se plantean preguntas puntuales que buscan conocer la perspectiva de todos los grupos de valor sobre cada una de las opciones, las cuales incluyen soluciones tecnológicas disponibles en el mercado, que involucran, incluso, el uso de inteligencia artificial u otras tecnologías avanzadas, con el fin de hacer más exigentes los controles para prevenir la comisión de fraude.

En el mismo sentido, respecto de las solicitudes planteadas por **COMCEL, PTC** y el ciudadano **RODRIGO MONTUFAR**, se informa que dentro de los controles por los que se preguntan en la consulta pública como posibles alternativas de solución, tanto para el servicio de llamadas de voz como de SMS, esta Comisión está teniendo en consideración la imposición de consecuencias en aquellos casos en los que se identifique tráfico presuntamente fraudulento en las redes de telecomunicaciones.

Finalmente, como ya se mencionó, en atención a lo dispuesto en parágrafo del artículo 12.1.1.6 de la Resolución CRC 5050 de 2016, la CRC no admitió tres propuestas de experimentación en el marco de la convocatoria 2025 al Sandbox Regulatorio Convergente, ya que estas se encontraban relacionadas con la prevención del fraude mediante llamadas de voz y mensajes de texto, precisamente la temática objeto de análisis en el presente proyecto regulatorio.

Estas iniciativas fueron: i) *Creador de contenido responsable* por parte de Infobip Colombia S.A.S., ii) *Prevención y gestión del riesgo de fraude a través de mensajes PCA* por parte de Partners Telecom Colombia S.A.S., y iii) *Prevención y gestión del riesgo de fraude a través de llamadas LDI* también de Partners Telecom Colombia S.A.S.

A pesar de no haber sido habilitadas para participar en dicha convocatoria, las tres propuestas presentadas por los proponentes mencionados incluían elementos de experimentación relevantes. En particular, se planteaba el diseño y validación de metodologías dentro del Sandbox Regulatorio para mitigar riesgos de fraude en servicios de mensajería SMS A2P y llamadas LDI, así como la redefinición de responsabilidades en la gestión del consentimiento de usuarios en el ecosistema de contenidos. Estas iniciativas buscan mejorar la seguridad, la trazabilidad y la transparencia en los canales de comunicación digital, mediante la implementación de mecanismos técnicos y procedimentales innovadores, los cuales son tenidos en cuenta en los análisis que ha desarrollado y continuará desarrollando la CRC durante la ejecución del presente proyecto de regulación.

Es así como se acogen cada uno de los comentarios, sugerencias y solicitudes presentadas en el marco de este proyecto regulatorio. Esta Comisión agradece el interés de todos los grupos de valor respecto al desarrollo de esta iniciativa, la cual, es claro que afecta a toda la cadena de valor de las comunicaciones, tanto los agentes como a los usuarios de los servicios, como se presenta en detalle en

[6] CRC. Comunicación identificada con el radicado de salida No. 2025512256 del 23 de abril de 2025.

este documento. Por esta razón, invita a mantener su interés y participación en cada uno de los espacios de discusión que se pondrán a su disposición.

3. MARCO LEGAL Y REGULATORIO

A partir de las diferentes observaciones, comentarios y sugerencias planteadas por los grupos de valor en distintos escenarios de discusión dispuestos por esta Comisión, los cuales recaen directamente en los recursos de identificación dada su relevancia en la materialización de la comunicación con el usuario final, ya sea mediante los servicios tradicionales de voz o de SMS, se procede a efectuar un análisis integral del marco legal y regulatorio de estos recursos en Colombia, así como las competencias con las que cuenta la CRC para resolver las diferentes situaciones problemáticas previamente identificadas por esta Comisión y las preocupaciones que distintos agentes han puesto de presente.

De esta manera, en esta sección se realiza una breve descripción de la normativa vigente en materia de recursos de identificación; se presentan las facultades de la CRC que, en este caso, no solo se encuentran bajo la sombrilla de la regulación, sino también de la administración de tales recursos cuya característica esencial es que son limitados o escasos; y, al final, se efectúa un recuento de las principales decisiones regulatorias expedidas en ejercicio de dichas facultades.

3.1. Facultades de la CRC en materia de administración y regulación de recursos de identificación

De conformidad con los principios orientadores establecidos en el artículo 2[7] de la Ley 1341 de 2009, modificado por la Ley 1978 de 2019, en Colombia, el Estado no solo debe asegurar el acceso y uso de las Tecnologías de la Información y las Comunicaciones (TIC) y la prestación de los servicios de comunicaciones con calidad y de forma continua y oportuna; sino que debe fomentar el despliegue y uso eficiente de la infraestructura para su provisión y promover el óptimo aprovechamiento de los recursos escasos con el fin de generar competencia, calidad y eficiencia en beneficio de los usuarios.

Con el propósito de determinar el marco general que permita formular las políticas públicas que regirán las TIC, su ordenamiento general, el régimen de competencia, la protección al usuario y el uso eficiente de la infraestructura y los recursos escasos[8], mediante el mismo compendio normativo el legislador responsabilizó a la CRC de regular y administrar los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones.

En virtud de lo dispuesto en los numerales 12[9] y 13[10] del artículo 22 de la Ley 1341 de 2009, modificado por el artículo 19 de la Ley 1978 de 2019, la CRC es el órgano competente para regular y administrar

---

[7] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 de 2009. Numerales 1, 3, 4 y 10 del artículo 2, último numeral adicionado por el artículo 3 de la Ley 1978 de 2019. Publicada el 30 de julio de 2009. [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[8] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 de 2009. Artículo 1, modificado por el artículo 2 de la Ley 1978 de 2019. Publicada el 30 de julio de 2009. [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[9] «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 -.co-».

[10] «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».

los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones. Esto incluye la administración de los recursos de numeración, identificación de redes de telecomunicaciones y otros recursos escasos; y excluye el espectro radioeléctrico y el nombre de dominio de internet bajo el código del país correspondiente a Colombia -.co-, los cuales fueron otorgados expresamente al MinTIC por parte del legislador.

Aunado a lo anterior, mediante el Decreto 25 de 2002[11], compilado en el Decreto 1078 de 2015[12], el Gobierno Nacional, en ese momento facultado por la Ley 37 de 1993[13] para elaborar los planes de señalización, numeración, tarificación y enrutamiento necesarios para la interconexión de la red de telefonía móvil celular con la red telefónica pública conmutada[14], reiteró lo dispuesto en el Decreto 1130 de 1999[15], que expresamente indicaba que la CRC es la entidad competente para administrar y presentar proyectos al Gobierno Nacional sobre los planes técnicos básicos y las normas técnicas, referidos, entre otros, a transmisión, señalización, sincronización, enrutamiento, numeración y tarificación[16].

De esta manera, la compilación efectuada por el mencionado Decreto 1078, que continúa vigente, condiciona la administración de dichos planes técnicos básicos por parte de la CRC, a lo dispuesto en su Título 12 y a los principios de neutralidad, transparencia, igualdad, eficacia, publicidad, moralidad y promoción de la competencia, con el objetivo de garantizar el uso adecuado de estos recursos técnicos[17].

Una de las disposiciones más relevantes de dicho Título 12 establece que la administración del plan de numeración comprende «[…] las modificaciones y/o adiciones que se hagan a la estructura de la numeración, a los mapas de numeración, a los cuadros contenidos en el plan y a cualquier otro aspecto que requiera ser incluido dentro del mencionado plan»[18].

Finalmente, es importante indicar que con la compilación efectuada por el mencionado Decreto 1078 de 2015, se otorgó y se mantiene la naturaleza pública y de pertenencia al Estado a los recursos de numeración, esto es «[…] los números, bloques de numeración, códigos, prefijos, entre otros […]». Esta condición especial le permite al Estado «[…] asignarlos a los proveedores de redes y servicios de telecomunicaciones y recuperarlos cuando se den las condiciones que determine la CRC […]», por cuanto tal asignación no otorga derecho de propiedad alguno[19].

A partir de todo lo anterior, el marco regulatorio estipula expresamente que 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; y en caso de emitirse dicha autorización, el nuevo asignatario adquiere todas las obligaciones sobre los recursos de identificación cedidos o transferidos[20].

---

[11] «Por el cual se adoptan los Planes Técnicos Básicos y se dictan otras disposiciones».
[12] «Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones».
[13] «Por la cual se regula la prestación del servicio de telefonía móvil celular, la celebración de contratos de sociedad y de asociación en el ámbito de las telecomunicaciones y se dictan otras disposiciones».
[14] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 37 de 1993. Artículo 8.
[15] «Por el cual se reestructuran el Ministerio de Comunicaciones y algunos organismos del sector administrativo de comunicaciones y se trasladan funciones a otras entidades públicas».
[16] Decreto 1130 de 1999. Artículo 37, numeral 18.
[17] Decreto 1078 de 2015. Artículo 2.2.12.1.1.1.
[18] Ibid. Artículo 2.2.12.5.3.
[19] Ibid. Artículo 2.2.12.1.2.5.
[20] Resolución CRC 5050 de 2016. Artículo 6.1.1.6.2., numeral 6.1.1.6.2.3.

En aplicación de este marco normativo, y en ejercicio de sus funciones, la CRC ha expedido una serie de actos administrativos de carácter general en materia de administración de recursos de identificación, los cuales se encuentran compilados en el Título VI de la Resolución CRC 5050 de 2016[21]. A continuación, se realiza una breve explicación de cada uno de ellos.

3.1.1. Antecedentes regulatorios respecto de la administración de recursos de identificación

Teniendo en consideración la evolución de las competencias otorgadas a la CRC en materia de recursos de identificación y, por su puesto, al dinamismo tecnológico que ofrece la oportunidad de experimentar transformaciones en la forma en que se prestan y adoptan los servicios de telecomunicaciones, las decisiones regulatorias han venido adaptándose a las necesidades que la industria ha expresado. En este contexto, a continuación, se resumen los principales antecedentes regulatorios que esta Comisión ha desarrollado en el ejercicio de sus facultades de regulación y administración de los recursos de identificación esenciales para la operación de los servicios de telecomunicaciones.

Valga la pena aclarar que los antecedentes que aquí se presentan tienen énfasis en los recursos de numeración de códigos cortos para la provisión de mensajes cortos de texto (SMS) y el Servicio Suplementario de Datos no Estructurado (USSD), y la numeración E.164, que permite el uso de servicios tanto de llamadas de voz como de SMS, todo lo cual se encuentra compilado en la Resolución CRC 5050 de 2016.

Ilustración 1. Principales antecedentes regulatorios en materia de recursos de identificación.

Fuente: Elaboración CRC.

- **Resolución CRT 2028 de 2008**

Mediante este acto administrativo se expidieron por primera vez las reglas aplicables a los recursos de numeración. De esta manera, la entonces CRT definió los principios, criterios y procedimientos para la gestión uso, asignación y recuperación de la numeración nacional de los servicios de

[21] *"Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones"*

telecomunicaciones, aplicable también a la numeración geográfica y no geográfica en lo relativo a numeración de redes y numeración de servicios.

Con el objetivo de impregnar de imparcialidad y coherencia las reglas aplicables al plan nacional de numeración, se establecieron como principios aplicables tanto al administrador, como al proveedor solicitante y asignatario, los siguientes: disponibilidad, eficacia, eficiencia, imparcialidad y equidad, y transparencia. En el mismo sentido, se definieron las obligaciones que se debían cumplir por cada una de las partes intervinientes, incluyendo los criterios de uso eficiente verificables por el administrador.

Adicionalmente, se definieron los estados en los que se pueden encontrar estos recursos de identificación, con el objetivo de conocer aquellos que se encuentren en uso por parte de un usuario y la capacidad disponible, dada su naturaleza de escasez. En ese momento se definieron como estados de la numeración los siguientes: (i) asignada; (ii) en reserva; (iii) disponible; (iv) no asignable; (v) implementada en usuarios; (vi) implementada en otros usos; y (vii) no implementada.

Finalmente, se definieron los procedimientos de asignación, recuperación y devolución de los recursos de numeración, indicando expresamente los requisitos y criterios que se deben cumplir para cada caso.

- **Resolución CRC 3501 de 2011**

Con esta decisión la CRC reconoció, por primera vez, la importancia de los contenidos y aplicaciones en el sector TIC, así como el impacto que sobre el usuario estaban ejerciendo en áreas tales como servicios financieros, salud, educación y gobierno electrónico. Puntualmente, determinó las condiciones de las redes de telecomunicaciones por parte de proveedores de contenidos y aplicaciones mediante SMS y mensajes multimedia (MMS) sobre redes de telecomunicaciones de servicios móviles.

Así, en dicha resolución también se establecieron las definiciones, responsabilidades y obligaciones de los agentes intervinientes en la relación de acceso a las redes de telecomunicaciones móviles, a saber: PRSTM, PCA e IT. En el mismo sentido, se implementó el Registro de Proveedores de Contenidos y Aplicaciones e Integradores (RPCAI) y el reporte de uso o implementación de ese recurso de identificación.

Además, desde la perspectiva de la protección al usuario, se definió una estructura específica para la numeración de códigos cortos, con el objetivo de que le permitiera al usuario diferenciar criterios como: costos de los servicios (gratuito – cobro recurrente), modalidades de compra (única vez – suscripción), contenidos (servicios para adultos).

En suma, la expedición de esa resolución estableció los principios, criterios, condiciones, procedimientos de acceso y asignación de los códigos cortos para la provisión de contenidos y aplicaciones por medio de SMS y MMS sobre redes de telecomunicaciones móviles.

- **Resolución CRC 5826 de 2019**

Esta resolución modificó el Plan Nacional de Numeración y el Plan Nacional de Marcación que soporta los servicios de voz fija, previstos en el Decreto 1078 de 2015. De esta manera, se simplificaron las llamadas desde un teléfono fijo hacia otro teléfono fijo, así como en llamadas desde un teléfono móvil

a un teléfono fijo, y viceversa, teniendo en cuenta que para ambos casos las llamadas convergen a un abonado de 10 dígitos con independencia de la ubicación geográfica del usuario destinatario de la llamada. Asimismo, implementó la ampliación de la cobertura para la numeración E.164 -geográfica-, pasando de una cobertura municipal a una regional, conservando la agrupación de departamentos definida para cada Indicativo Nacional de Destino (NDC) geográfico desde el Decreto 25 de 2002.

- **Resolución CRC 5968 de 2020**

Mediante este acto administrativo 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 han venido aplicando durante los últimos años en la materia, 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, por los próximos 10 años.

Así mismo, 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 SMS Service Providers (SMS-SP) de los que trata el Reporte 212 del *Electronic Communications Committee* de la *European Conference of Postal and Telecommunications Administrations* (ECC Report 212)[22].

- **Resolución CRC 6522 de 2022**

Mediante esta última intervención regulatoria, la Comisión 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, en consonancia con lo establecido en la Ley 2300 de 2023[23], por medio de la cual se adoptó el Registro de Números Excluidos (RNE) cuyo objetivo es identificar a todos aquellos usuarios que no desean ser contactados para fines comerciales o publicitarios, tanto mediante SMS, como llamadas de voz.

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, estableció la obligación en

[22] Electronic Communications Committee of European Conference of Postal and Telecommunications Administrations (CEPT). *ECC Report 212. Evolution in the Use of E.212 Mobile Network Codes*. Aprobado el 9 de abril de 2014. [en línea]. Consultado en el siguiente enlace: https://docdb.cept.org/download/1152
[23] «Por medio de la cual se establecen medidas que protejan el derecho a la intimidad de los consumidores».

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.

Adicionalmente, en materia de protección de los usuarios que reciben mensajes SMS o USSD con fines publicitarios o comerciales, mediante el mismo acto la CRC implementó las siguientes disposiciones:

i. Para los PCA e IT asignatarios de códigos cortos:

   a. Contar con medios o mecanismos para la atención de usuarios; y, en consecuencia, responder de fondo las solicitudes que reciba en relación con los SMS enviados desde esa numeración, dentro de los quince (15) días hábiles siguientes a su recibo.
   b. Incluir en todos los SMS remitidos mediante este recurso: el nombre, marca o razón social del PCA responsable de la provisión de contenidos y aplicaciones. Esta información debe incluirse al inicio o al final de cada mensaje, sesión o grupo de mensajes, según corresponda.
   c. Implementar herramientas para prevenir fraudes haciendo uso de este recurso de identificación y realizar controles periódicos para determinar su efectividad.

ii. Derecho de los usuarios: utilizar la palabra clave «SALIR» o «CANCELAR» para restringir la recepción de esos SMS de un determinado PCA.

En la mencionada resolución también se incluyó dos nuevas causales de recuperación para los códigos cortos. La primera, consistió en que la CRC podrá recuperar el o los códigos cortos al asignatario cuando se envíen SMS a usuarios que se encuentren inscritos en el RNE; y, la segunda, estableció que cuando se envíen SMS a nombre de terceros que no han autorizado su envío o su contenido, se puede proceder con la recuperación.

Finalmente, como una medida de fortalecimiento del procedimiento de asignación de códigos cortos, se incluyó la prohibición de asignación de este recurso de identificación, a aquellos solicitantes que, en el año inmediatamente anterior, se les haya recuperado numeración por las causales dispuestas en los numerales 6.4.3.2.2., 6.4.3.2.8., 6.4.3.2.9., y 6.4.3.2.10. de la Resolución CRC 5050 de 2016.

4. IDENTIFICACIÓN DEL PROBLEMA

En esta sección se aborda la definición de la problemática junto con sus causas y consecuencias. Previo a ello, con el fin de entender el escenario objeto de estudio, se realiza una contextualización del fraude cibernético en Colombia, describiendo su magnitud a partir de la información aportada por todos los grupos de valor, haciendo énfasis en las que generarían impacto en los servicios de telecomunicaciones tradicionales de voz y SMS.

Acto seguido, se exponen los aspectos más relevantes desde la perspectiva técnica, que en este caso se enmarca en los recursos de identificación que existen en Colombia, con enfoque especial en la numeración E.164 y de códigos cortos esenciales para la comunicación con los usuarios finales. Luego, desde la perspectiva económica, se presentan las cadenas de valor construidas para los servicios tradicionales de voz y SMS, a partir de las funciones que cada agente desempeña para permitir la comunicación hasta el usuario final.

Por último, bajo ese contexto, se explica en detalle el árbol del problema identificado, todo ello soportado con evidencias e información que fundamentan las situaciones descritas.

4.1. Descripción y contextualización del fraude cibernético en Colombia y su relación con los recursos de identificación para la provisión de los servicios de telecomunicaciones

4.1.1 Contexto general del fraude cibernético en Colombia

Sea lo primero indicar que, como lo ha explicado esta Comisión en el desarrollo de otros análisis regulatorios[24], en el ordenamiento jurídico colombiano vigente no existe una definición para el término «fraude». A pesar de lo anterior, sí existen disposiciones normativas que tienen como propósito prevenir, contener e incluso sancionar conductas que puedan ser consideradas como fraudulentas en las distintas órbitas de la vida social.

Un claro ejemplo de ello es que en el código penal hay conductas tipificadas como delitos que comúnmente se conocen como comportamientos fraudulentos, dentro de los cuales están: el fraude procesal (C.P., art. 453), la estafa (C.P., art. 246), la falsedad personal o suplantación de identidad (C.P., art. 296). De hecho, directamente relacionados con el cibercrimen y los servicios de telecomunicaciones, existen ocho (8) conductas delictivas tipificadas en el código penal, adicionadas mediante la Ley 1273 de 2009[25], a saber: acceso abusivo a un sistema informático (C.P., art. 269A), obstaculización ilegítima de sistema informático o red de telecomunicaciones (C.P., art. 269B), interceptación de datos informáticos (C.P., art. 269C), daño informático (C.P., art. 269D), uso de software malicioso (C.P., art. 269E), violación de datos personales (C.P., art. 269F) y suplantación de sitios web para capturar datos personales (C.P., art. 269G).

A pesar de lo anterior, no existe en el marco normativo una disposición que tipifique –en el sentido de caracterizar sus elementos esenciales– y prohíba una conducta denominada «fraude».

Ahora bien, la jurisprudencia penal, al analizar las conductas tipificadas como delitos y que comúnmente se califican como fraudulentas, ha identificado ciertos elementos comunes predicables a este tipo de comportamientos, en particular al delito de estafa. Entre ellos se pueden destacar los siguientes:

> «[…]
>
> a) Despliegue de un artificio o engaño dirigido a suscitar error en la víctima; b) Error o juicio falso de quien sufre el engaño, determinado por el ardid; c) Obtención, por ese medio, de un provecho

[24] CRC. Documento de Respuestas a Comentarios de las Resoluciones CRC 7810 y 7811 de 2025. 16 de junio de 2025. Página 45 a 49. [en línea]. Consultado en: https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20respuesta%20a%20comentarios%20-%20Simplificaci%C3%B3n%20del%20marco%20regulatorio%202024/Documento-Respuesta-Comentarios-Simplificacion-Marco-Regulatorio-2024-VF.pdf

[25] Congreso de la República. Ley 1273 de 2009 «Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones». Diario Oficial No. 47.223 de 5 de enero de 2009. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_1273_2009.htm

> ilícito; d) Perjuicio correlativo de otro, y e) Sucesión causal entre el artificio o engaño y el error, y entre éste y el provecho injusto que refluye en daño patrimonial ajeno.
>
> […]»[26].

Por su parte, aunque tangencialmente, la jurisprudencia de la Corte Constitucional también ha hecho referencia a lo que se debe entender por «fraude». Mediante la Sentencia T-073 de 2019, dicho Alto Tribunal indicó que:

> «Un comportamiento puede calificarse como fraudulento cuando la actuación, que en apariencia se ajusta a la prescripción normativa, en la realidad conlleva una situación manifiestamente contraria a un principio del ordenamiento superior»[27].

En este punto vale la pena resaltar que el sentido antes indicado sobre lo que se conoce como «fraude» se alinea con el significado natural de la expresión[28], definida por la Real Academia Española como la «acción contraria a la verdad y a la rectitud, que perjudica a la persona contra quien se comete» o como el «acto tendente a eludir una disposición legal en perjuicio del Estado o de terceros»[29].

Bajo este contexto, la CRC reafirma que los términos «fraude», «conductas fraudulentas» o «fines fraudulentos» se deben entender, tanto en el marco de este proyecto como en las medidas regulatorias vigentes donde se utilizan, en concordancia con su significado natural. En otras palabras, no se deben interpretar de manera restrictiva como que se refieren exclusivamente a la comisión de las conductas delictivas tipificadas en la ley penal colombiana, sino de manera amplia, es decir, que se refiere a todos aquellos actos contrarios a las reglas o disposiciones establecidas en la normativa que generan perjuicios a terceros.

Aclarado lo anterior, no puede perderse de vista que, con la entrada en vigor de la Ley 1273 de 2009, en Colombia sí existen conductas punibles que se materializan por medio del uso de los servicios tradicionales de telecomunicaciones como lo son las llamadas de voz y el envío de SMS.

En protección de los bienes jurídicos tutelados de «sistemas de información y datos personales», los delitos de «violación de datos personales» y de «suplantación de sitios web para capturar datos personales», son claros ejemplos de ello. Ambos delitos se encuentran tipificados en el código penal de la siguiente manera:

> «Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes».

---

[26] Corte Suprema de Justicia, Sala Penal. Sentencia del 12 de diciembre de 2019, SP-53792019. Sentencia del 9 de agosto de 2017, SP-537922019, exp. 44071. Sentencia del 8 de marzo de 2017, SP-32332017, exp. 48279.
[27] Corte Constitucional. Sentencia T-073 de 2019. M.P. Carlos Bernal Pulido.
[28] Código Civil. «Artículo 28. Significado de las palabras. Las palabras de la ley se entenderán en su sentido natural y obvio, según el uso general de las mismas palabras; pero cuando el legislador las haya definido expresamente para ciertas materias, se les dará en éstas su significado legal».
[29] Real Academia Española. Diccionario de la lengua española. *Fraude.* [en línea]. Consultado en: https://dle.rae.es/fraude?m=form

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

> «Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.
>
> […]».

Por su parte, desde la perspectiva de garantía constitucional del derecho a la intimidad personal y familiar y a su buen nombre, con la expedición de la Ley 1581 de 2012[30] se definieron los principios, derechos, obligaciones garantías y procedimientos que se deben observar sobre los datos personales registrados en cualquier base de datos personales, que los haga susceptibles de tratamiento por parte de cualquier entidad pública o privada.

De esta manera, en aquellos casos en los que, como resultado de ataques de ingeniería social —tales como *phishing*, *smishing*, *spoofing* o *vishing*— se efectúe el tratamiento de datos personales y se evidencie el incumplimiento de alguna de las disposiciones de su régimen, la SIC, como autoridad de inspección, vigilancia y control en esta materia, está facultada para, en caso de encontrar mérito, llevar a cabo actuaciones administrativas sancionatorias, incluyendo la imposición de sanciones.

Así las cosas, algunas de las mencionadas actividades, delictivas o transgresores de derechos fundamentales, se pueden materializar mediante mecanismos de contacto a usuarios de servicios de telecomunicaciones, los cuales pueden involucrar la vulneración de distintos eslabones de las cadenas de valor del flujo de la comunicación[31]. Al respecto, la *Cartilla metodológica de atención de delitos informáticos* de la Fiscalía General de la Nación[32] define los siguientes modos utilizados para realizar acciones irregulares con fines de fraude:

- «*Phishing:* Es una técnica de ingeniería social que usan los ciberdelincuentes para obtener información confidencial de los usuarios de forma fraudulenta y así apropiarse de la identidad de esas personas. Mediante correos electrónicos que contienen enlaces, se enruta la conexión de una víctima a través de una página falsa hacia otras páginas WEB con el objetivo de obtener información (páginas web vistas, información de formularios, contraseñas etc.). Comúnmente utilizada para robar información personal» (sic).

- «*Smishing:* Modalidad consistente en el uso del phishing -métodos de engaño para obtener información personal confidencial o estafar a alguien- pero a través de SMS (mensajes cortos de celular) en lugar de correos electrónicos» (sic).

[30] «Por la cual se dictan disposiciones generales para la protección de datos personales».
[31] Las cadenas de valor de los servicios de llamadas de voz tradicional y la de mensajes cortos de texto se describe en la sección 4.1.4 denominada «Cadena de valor de los servicios de llamada de voz y de mensajes cortos de texto».
[32] Fiscalía General de la Nación. Cartilla metodológica de atención de delitos informáticos. [en línea]. Consultado en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

- «*Vishing:* El *Vishing* corresponde a llamadas que hacen para engañar a las personas con la promesa de falsos premios, oferta u ofrecimientos bancarios y de esta manera obtener información sensible».

- «*Spoofing:* Suplantación de identidad del remitente del mensaje de correo electrónico, IP o cualquier otra app con la finalidad de obtener información sensible».

En este contexto, es importante tener en cuenta que, si bien el tráfico de los servicios de mensajería y voz móvil 3G, así como del servicio de telefonía fija[33], han mostrado una tendencia decreciente en los últimos años[34], las afectaciones a los usuarios derivadas de acciones irregulares con fines de fraude presentan un crecimiento sostenido, incluso exponencial en algunos casos.

Esta disparidad evidencia que, a pesar de la reducción en el volumen de uso, los riesgos asociados a estos canales no solo persisten, sino que se intensifican en términos de su impacto económico, reputacional y social sobre los usuarios. Esta situación pone de manifiesto la necesidad de una intervención regulatoria oportuna y proporcional, orientada a mitigar dichas amenazas y a proteger los derechos de los usuarios dentro del ecosistema de comunicaciones móviles.

Con el propósito de dimensionar el problema desde la perspectiva de la tipificación de la conducta, existen fuentes institucionales que consolidan información relevante sobre los delitos informáticos en Colombia. En particular, el Observatorio de Derechos Humanos y Defensa Nacional[35] del Ministerio de Defensa Nacional realiza la consolidación de la información sobre el reporte de denuncias sobre delitos informáticos a partir del cruce de registros administrativos de fuentes como el Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo de la Policía Nacional (SIEDCO) y del Sistema Penal Oral Acusatorio (SPOA)[36].

La información del Observatorio[37] revela un crecimiento sostenido de las denuncias relacionadas con delitos informáticos. La Ilustración 2 presenta la evolución de las denuncias entre 2020 y 2024. En esta se puede ver que este fenómeno creció a una tasa promedio anual del 11,0%, pasando de 49.359 registros en 2020 a 74.845 en 2024. Este aumento se explica, en gran parte, por el comportamiento de ciertas tipologías que concentran la mayor prevalencia y aportan significativamente al total general.

---

[33] En el documento de consulta publicado por la CRC el 22 de marzo de 2024, se llevó a cabo una descripción detallada de la evolución del mercado de voz fijo desde la óptica de los ingresos, el tráfico y el número de líneas. Informe disponible en https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-38-3-20/Propuestas/consulta-remuneracion-fija-publicacion.pdf

[34] CRC. Documento de respuesta comentarios del proyecto regulatorio *Simplificación del marco regulatorio 2024*. [en línea]. Disponible en: https://crcom.gov.co/es/proyectos-regulatorios/2000-38-3-22

[35] Ministerio de Defensa Nacional. Observatorio de Derechos Humanos y Defensa Nacional. [en línea]. Disponible en: https://www.mindefensa.gov.co/defensa-y-seguridad/datos-y-cifras

[36] El Observatorio de Derechos Humanos y Defensa Nacional del Ministerio de Defensa Nacional realiza la consolidación de la información en coordinación con la Dirección de Investigación Criminal e INTERPOL (DIJIN) de la Policía Nacional, la Fiscalía General de la Nación y el Comité de Gerencia de la Información Estadística del Sector (CGIES). Para la consolidación de los delitos informáticos, se realiza cruce semanal con SPOA - Sistema Penal Oral Acusatorio de la Fiscalía General de la Nación. Con el fin de mejorar la calidad de la información, se realiza la validación de los registros existentes, el cruce de tipologías y la depuración que elimina registros por atipicidad del delito, inexistencia del hecho o querellante ilegítimo, lo cual confirma que no todos los registros corresponden a delitos tipificados o judicializados.

[37] Ministerio de Defensa Nacional. Delitos informáticos [Conjunto de datos]. Datos Abiertos Colombia. Consultada el 23 de mayo de 2025. [Información con corte de actualización al 20 de mayo de 2025] Disponible en: https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Por ejemplo, las denuncias por acceso abusivo a un sistema informático crecieron a una tasa anual promedio del 20,8% (ver Ilustración 3), pasando de 7.613 a 16.192 registros, llegando a ser la conducta de mayor crecimiento en este periodo.

Ilustración 2. Denuncias sobre conductas asociadas a delitos informáticos.

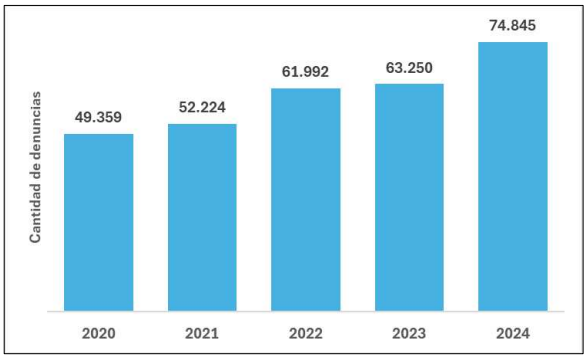
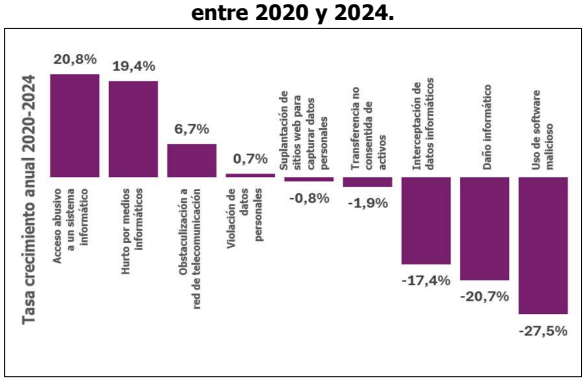


Ilustración 3. Tasa de crecimiento promedio anual entre 2020 y 2024.

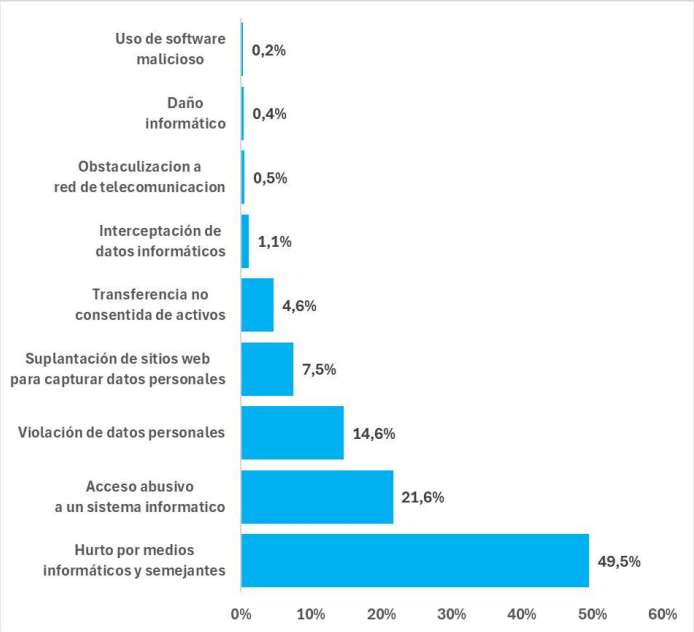


Fuente: Observatorio de Derechos Humanos y Defensa Nacional del Ministerio de Defensa Nacional.

Sin embargo, el hurto por medios informáticos y semejantes es la conducta más reportada a lo largo del periodo y el principal impulsor del crecimiento global del total de denuncias asociadas a delitos informáticos. En particular esta conducta presenta una tasa anual promedio del 19,4%, pasando de 18.244 a 37.045 casos y llegando a representar el 49,5% del total de las denuncias en el 2024 (ver Ilustración 4).

Adicionalmente, las violaciones de datos personales presentan un incremento moderado del 0,7% promedio anual, pero con niveles absolutos altos, 10.629 casos en 2020 y 10.977 en 2024. Por su parte, la cantidad de denuncias asociadas a la obstaculización ilegitima de sistema informático o red de telecomunicación muestran un crecimiento del 6,7%, llegando a representar el 0,5% del total de los casos.

Ilustración 4. Distribución de denuncias por tipificación de la conducta en 2024.



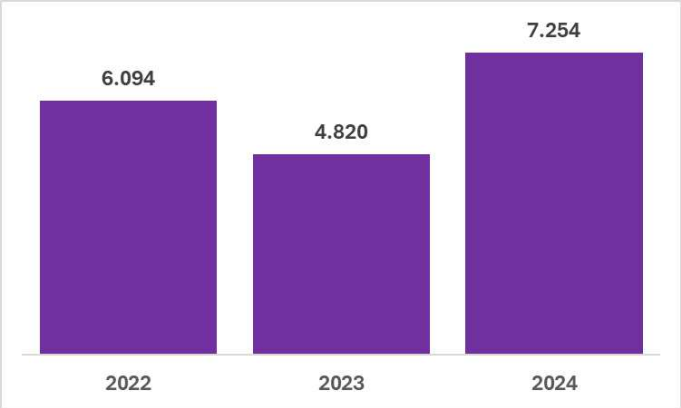
Fuente: Observatorio de Derechos Humanos y Defensa Nacional del Ministerio de Defensa Nacional.

En contraste, algunas conductas presentan una tendencia decreciente, como el daño informático (−20,7%), la interceptación de datos informáticos (−17,4%) y la transferencia no consentida de activos (−1,9%), lo que puede estar relacionado con una menor visibilidad por registro de denuncias, menor tipificación o mejoras en los controles técnicos.

Este panorama mixto refleja que, si bien algunas modalidades están contenidas o en descenso, las más frecuentes y de mayor impacto económico y social continúan en expansión, especialmente aquellas en donde los servicios de telecomunicaciones podrían llegar a actuar como vectores de estos delitos.

Otra fuente de información son las quejas relacionadas con posibles vulneraciones al tratamiento de datos personales que recibe la Delegatura para la Protección de Datos Personales de la SIC. De acuerdo con la Ilustración 5, entre los años 2022 y 2024 se recibieron 18.168 quejas, lo que refleja la persistencia y escala del fenómeno asociado al empleo de tácticas de ingeniería social dado el crecimiento del 19% en este periodo, al pasar de 6.094 quejas en 2022 a 7.254 en 2024.

Ilustración 5. Quejas sobre posibles vulneraciones al tratamiento de datos personales.



Fuente: Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC).

En términos generales, la tendencia creciente de las denuncias sobre conductas asociadas al fraude cibernético representa un desafío en materia de generación y adopción de herramientas para su mitigación. La magnitud y complejidad de esta problemática demanda de la intervención desde diferentes perspectivas, razón por la cual este proyecto regulatorio provee una visión integrada a los diferentes esfuerzos sectoriales para contribuir y dar alcance al objetivo propuesto.

4.1.2 Requerimiento de información sobre el fraude cibernético por medio del servicio de llamadas de voz y SMS.

Teniendo en cuenta la limitación de la información oficial para detallar con precisión la magnitud de cada uno de los modos específicos utilizados para ejecutar acciones irregulares con fines de fraude, esta Comisión realizó[38], entre el 23 de abril y el 9 de mayo de 2025, un requerimiento particular de información sobre el fraude cibernético por medio de llamadas de voz o del uso de mensajes cortos de texto.

Para el diligenciamiento de esta petición se remitió un listado de preguntas a 345 empresas registradas como usuarias o asignatarias de numeración de códigos cortos en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI) y en el Registro de Proveedores de Contenidos y Aplicaciones, e Integradores (RPCAI).

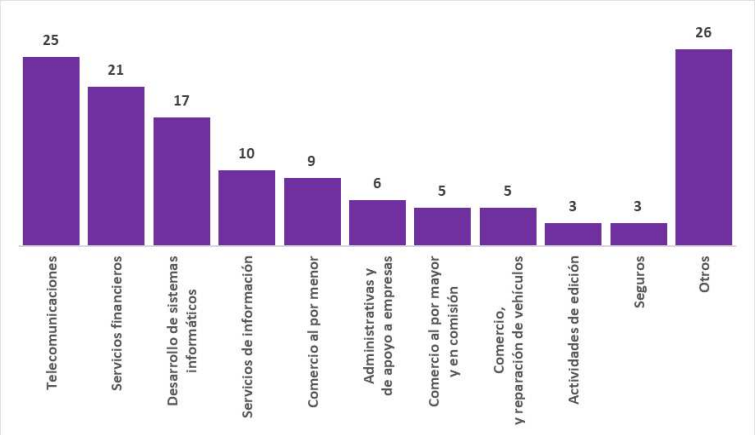
Entre las temáticas que integraron el requerimiento de información se encuentran:

- Magnitud y caracterización del problema del fraude cibernético.
- Medidas tecnológicas y de ciberseguridad implementadas para la prevención de fraude cibernético.
- Detección y reportes de fraudes.
- Medidas pedagógicas y de sensibilización.
- Costo asociado al fraude cibernético por medio del uso de códigos cortos.

[38] El requerimiento de información con asunto «Información relacionada con fraude cibernético por medio de servicios de telecomunicaciones móviles» se realizó mediante envío de comunicación a las empresas con número de radicado 2025200796.

De acuerdo con los resultados del requerimiento, se obtuvo una participación de 130 empresas, que pertenecen principalmente a sectores de la actividad económica relacionadas con telecomunicaciones, servicios financieros, desarrollo de sistemas informáticos, servicios de información, comercio al por menor, administrativas y de apoyo a empresas, entre otras actividades (ver Ilustración 6). Esta diversidad sectorial permite obtener una visión amplia desde la perspectiva empresarial sobre el fenómeno del fraude cibernético mediante el uso de servicios de llamadas de voz y mensajes cortos de texto.

Ilustración 6. Distribución de la participación de empresas por actividad económica.



Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

En cuanto a la prevalencia de las acciones irregulares, se identificó que el 26,9% de las empresas reportaron haber detectado incidentes de fraude cibernético mediante el uso de mensajes cortos de texto por parte de terceros con o sin autorización. Este hallazgo evidencia la relevancia de la trazabilidad y control de los recursos de identificación utilizados en la mensajería empresarial.

Es importante resaltar que, aproximadamente, 2 de cada 3 empresas que reportó haber detectado incidentes pertenece a los sectores de telecomunicaciones, servicios financieros y servicios de información, los cuales por la naturaleza de su objeto social gestionan altos niveles de tráfico con usuarios finales por medio de canales de servicios móviles. Este resultado permite sugerir que estos sectores pueden llegar a ser los más expuestos a los riesgos derivados del fraude cibernético, al menos en el conjunto de empresas usuarias o asignatarias de recursos de identificación.

La cantidad de incidentes detectados por las empresas, presentado en la Tabla 1, muestra una prevalencia de los casos de *smishing*. En particular, la información reportada por las empresas indica que esta modalidad de fraude presentó un crecimiento significativo entre el año 2022 y 2024. Mientras que para el 2022 se identificaron 40.902 incidentes, para el año 2023 los incidentes se multiplicaron aproximadamente por seis llegando a 259.973. Este patrón de crecimiento se mantuvo para el año 2024 debido a que los incidentes identificados llegaron a 570.144.

Tabla 1. Cantidad de incidentes de fraude cibernético detectados por las empresas.

Modo de Fraude	2022	2023	2024
Smishing	40.902	259.973	570.144
Vishing	2.291	3.552	17.429
Total	**43.193**	**263.525**	**587.573**

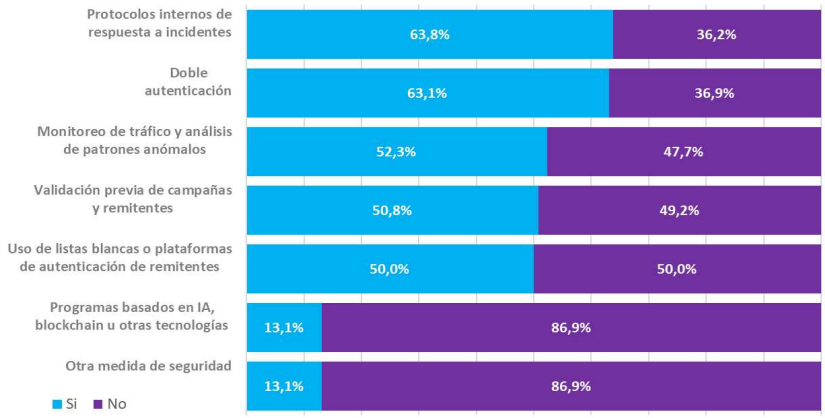
Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

Por su parte, los casos de *vishing* detectados por las empresas se mantuvieron en un nivel significativamente inferior en contraste a los casos de *smishing.* No obstante, también presentan un crecimiento acelerado para el mismo periodo de tiempo. En el año 2022 se identificaron 2.291 casos, mientras que para el año 2023 se presentó un crecimiento del 55% llegando a 3.552. Sin embargo, para el año 2024 los incidentes identificados de *vishing* aumentaron un 390,7% alcanzando 17.429 casos.

Estos resultados pueden estar asociados a un incremento inusual de los intentos de acciones irregulares con fines de fraude o a una mayor capacidad para detectar y reportar este tipo de amenazas. Así mismo, es importante señalar que la magnitud de este fenómeno puede estar subestimada dado que una parte de estas acciones no son identificadas por las empresas.En consistencia con la consulta sobre la cantidad de incidentes, se indagó por las medidas tecnológicas que han implementado las empresas consultadas para prevenir o mitigar el fraude cibernético mediante el envío de SMS o llamadas de voz. Los resultados de esta pregunta se muestran en la Ilustración 7.

El 63,8% de las empresas reportó contar con protocolos internos de respuesta a incidentes, los cuales están basados en procedimientos estandarizados que se activan de forma posterior a la detección de un incidente de fraude o ciberataque. Seguidamente, el 63,1% de estas manifestó contar con mecanismos de seguridad de doble autenticación, bajo esta medida de seguridad se asegura la identificación del usuario mediante el requerimiento de dos factores distintos de verificación para acceder a un servicio o confirmar una transacción.

Ilustración 7. Medidas tecnológicas y de ciberseguridad implementadas para la prevención de fraude cibernético.

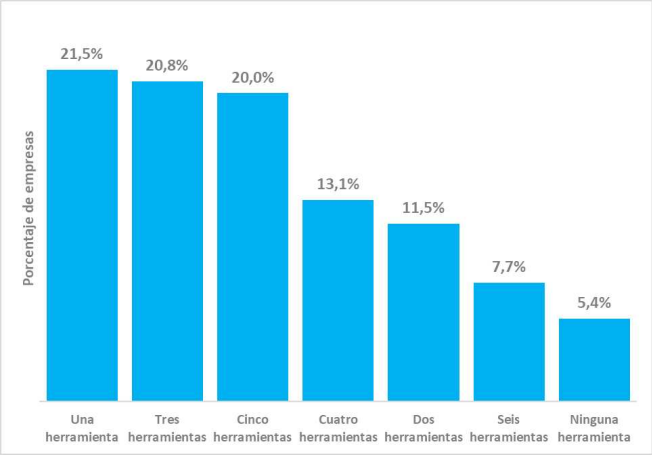


Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

Asimismo, el 52,3% de las empresas indicó implementar monitoreo de tráfico y análisis de patrones anómalos, bajo este mecanismo se emplean herramientas para observar de forma continua el comportamiento del tráfico digital (como el envío de SMS o transacciones), identificando comportamientos inusuales o sospechosos que podrían indicar un intento de fraude. De forma complementaria el 50,8% realiza la validación previa de campañas y remitentes con el fin de verificar la autorización de la empresa o de un tercero antes de permitir el envío de los mensajes cortos.

En este mismo sentido, el 50,0% hace uso de listas blancas o plataformas de autenticación de remitentes con el fin de realizar el envío únicamente desde remitentes autorizados o verificados. Por otro lado, un 13,1% reportó el uso de programas basados en tecnologías como Inteligencia Artificial (IA) o *blockchain*, y un mismo porcentaje indicó haber adoptado otras medidas de seguridad distintas a las listadas previamente.

Ilustración 8. Cantidad de medidas concurrentes para la prevención de fraude cibernético.



Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

La Ilustración 8 muestra la cantidad de medidas adoptadas de forma concurrente por las empresas. De acuerdo con los resultados, se observa que la mayoría de las empresas ha implementado múltiples estrategias de protección. Si bien el 21,5% de las empresas reportó haber adoptado al menos una medida, el 20,8% de las empresas reportó haber implementado al menos tres medidas en conjunto y seguida del 20,0% de las empresas que reportó contar hasta con cinco herramientas tecnológicas y de ciberseguridad.

En contraste, un grupo menor, compuesto por el 5,4% de las empresas, indicó no haber adoptado ninguna medida tecnológica para prevenir fraudes mediante llamadas de voz o por medio del servicio SMS, revelando que, aunque sea una baja proporción, existen empresas que tienen una mayor exposición a riesgos generados por acciones irregulares con fines de fraude.

Por otro lado, el 35,4% de las empresas manifiesta contar con mecanismos establecidos para el intercambio de alertas de fraude (ver Ilustración 9). Estos mecanismos permiten mantener una comunicación activa y oportuna con los PRSTM, otras empresas y autoridades competentes.

De acuerdo con la descripción de los procedimientos para el desarrollo de intercambio de dichas alertas, se encontró que el correo electrónico es el canal más comúnmente utilizado para enviar y recibir alertas relacionadas con contenido sospechoso, remitentes, códigos cortos o patrones anómalos de tráfico.

También se utilizan plataformas de gestión de incidentes que permiten la trazabilidad y el escalamiento de eventos. Adicionalmente, se mencionaron herramientas de comunicación directa como WhatsApp, Microsoft Teams y llamadas directas a contactos previamente definidos, así como cuentas centralizadas de reporte institucional.

Ilustración 9. Cuenta con procedimientos para intercambio de alertas de fraude con proveedores de redes y servicios de telecomunicaciones móviles (PRSTM) u otras entidades.

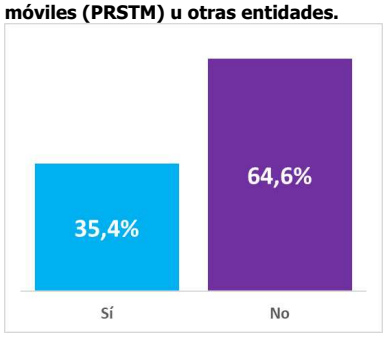


Ilustración 10. Considera que actualmente enfrenta dificultades para mantener o fortalecer sus medidas antifraude.

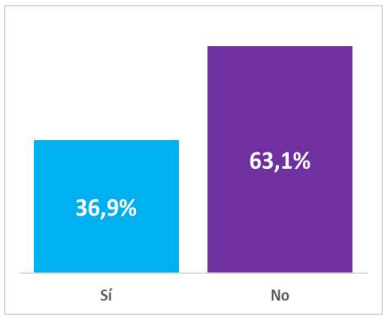
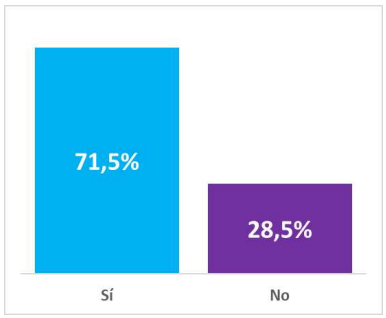


Ilustración 11. Desarrollo de campañas de educación a sus usuarios sobre prevención de fraudes cibernéticos en los últimos 3 años.



Fuente: Requerimiento de información de la CRC sobre el fraude cibernético por medio de llamadas de voz o mensajes cortos de texto.

En términos de procedimiento, algunas empresas describieron procesos estructurados que incluyen los siguientes pasos:

- Recepción de alertas por parte del PRSTM o del operador.
- Registro y clasificación de la alerta según su naturaleza (fraude por contenido, remitente, campaña).
- Validación interna y, si aplica, bloqueo de remitente o campaña.
- Escalamiento a proveedores, integradores o autoridades dependiendo del nivel de criticidad.
- Documentación del caso para análisis posteriores y retroalimentación de sistemas de prevención.

Respecto a la coordinación con PRSTM y otras entidades, se manifestó la colaboración con operadores como Claro, Tigo, Movistar, ETB, WOM y otros. Algunos operadores notifican sobre contenidos no autorizados o remitentes sospechosos, y las empresas definen plazos para responder. Varias empresas indicaron que también realizan intercambio de alertas y coordinación con autoridades y empresas externas, como la Policía Nacional (incluyendo CAI Virtual y Policía Cibernética), ColCERT, la SIC, y redes financieras como Redeban, ACH, Credibanco, entre otras.

No obstante, de acuerdo con los resultados, aproximadamente una de cada tres empresas manifiesta algunas limitaciones en sus procedimientos (ver Ilustración 10). Por ejemplo, algunas indican que no cuentan con canales directos para contactar a los PRSTM, así como la ausencia de estándares que

limitan la formalización de respuestas y la trazabilidad en la cadena de envío de los mensajes de texto (SMS) o de las llamadas de voz con contenido presuntamente fraudulento.

Desde la perspectiva del manejo del riesgo, una de cada tres empresas consultadas considera que actualmente enfrenta dificultades para mantener o fortalecer sus medidas antifraude. Las limitaciones descritas por estas organizaciones se clasificaron en cuatro categorías:

1. Dificultades presupuestales:
    - Altos costos de implementación y mantenimiento de soluciones antifraude (firewalls, inteligencia artificial, filtros avanzados, plataformas de monitoreo).
    - Costos asociados a procesos de judicialización de fraudes (honorarios, trámites, etc.).
2. Dificultades técnicas:
    - Falta de herramientas para la detección en tiempo real de fraudes por SMS o llamadas.
    - Evolución constante de las técnicas de fraude (variaciones lingüísticas, uso de ingeniería social, nuevos dominios).
    - Carencia de plataformas compartidas para validación y monitoreo.
3. Dificultades regulatorias:
    - Falta de exigencias claras a los PCA para registrarse, usar códigos cortos propios o responder ante alertas.
    - Inexistencia de un marco regulatorio que obligue a la cooperación entre PRSTM, PCA, entidades usuarias de los códigos cortos y autoridades.
4. Dificultades operativas:
    - Dependencia de terceros (integradores o proveedores) para tomar acciones.
    - Falta de cooperación entre los distintos actores del ecosistema (financieros, telecomunicaciones, autoridades).
    - Baja formalización de las denuncias por parte de los usuarios, lo que dificulta la trazabilidad.

La consulta pública también indagó sobre el desarrollo de campañas de educación a sus usuarios sobre prevención de fraudes cibernéticos. La Ilustración 11 muestra que el 71,5% de las empresas realizaron acciones pedagógicas en los últimos tres años, en las cuales se buscó principalmente generar conciencia sobre temas como *phishing*, *smishing*, *vishing*, *ransomware*, suplantación de identidad, seguridad de contraseñas, ingeniería social, y uso seguro de canales digitales.

Las estrategias implementadas incluyen cursos virtuales y presenciales, envío de mensajes informativos (por correo electrónico, SMS, redes sociales o plataformas internas), charlas con expertos, simulacros de ataques, cápsulas informativas (píldoras de seguridad), infografías y contenidos multimedia como videos y banners. Algunas empresas complementan estas acciones con programas estructurados de formación, simulaciones de ataques, e integración de la concienciación en procesos de inducción y capacitación continua.

Por último, la consulta pública también indagó sobre la valoración económica de las actividades y afectaciones atribuibles al fraude mediante el envío de SMS o llamadas de voz. Los resultados arrojaron que solo 16,9% de las empresas participantes cuenta con información sobre el fraude cibernético desde una perspectiva de costos.

Así mismo se encontró una alta dispersión de los valores reportados, particularmente en aquellos costos registrados por empresas del sector financiero. En este sentido, se empleó la mediana como estadístico

de tendencia central para analizar la información reportada y minimizar la influencia de la alta dispersión de los datos. En la Tabla 2 se presentan los valores que resultan del análisis de información desarrollado, expresados en millones de pesos.

La información de costos asociados al fraude cibernético mediante llamadas de voz o SMS solicitada en el requerimiento hizo énfasis en tres dimensiones: prevención, impacto y respuesta. En materia de prevención, los mayores recursos se destinaron al desarrollo e implementación de medidas técnicas, con una mediana anual que pasó de $85,15 millones en 2022 con un ascenso a $98,95 millones en 2023, para seguir aumentando en 2024 a $110,83 millones.

Las campañas pedagógicas y auditorías de ciberseguridad también representaron esfuerzos sostenidos, aunque con montos significativamente menores.

Tabla 2. Valoración económica de las actividades y afectaciones atribuibles al fraude mediante el envío de SMS o llamadas de voz. (En millones de pesos).

Prevención del fraude cibernético	**2022**	**2023**	**2024**
Desarrollo e implementación de medidas para la prevención del fraude cibernético	85,15	98,95	110,83
Campañas pedagógicas dirigidas a usuarios sobre prevención de *Smishing* o *vishing*	5,00	11,44	11,00
Auditorías de ciberseguridad y validación de campañas de SMS o llamadas de voz	80,00	16,50	40,90
Impactos del fraude cibernético	**2022**	**2023**	**2024**
Compensaciones económicas a clientes o aliados	748,84	574,69	985,06
Abandono de clientes / cancelación de servicios por pérdida de confianza	449,00	18,61	13,91
Pérdidas estimadas para los usuarios	791,74	363,13	1.691,96
Respuesta frente al fraude cibernético	**2022**	**2023**	**2024**
Recursos humanos asignados a equipos de atención de incidentes	50,00	54,00	70,00
Costo de sistemas de atención al cliente y soporte ante fraudes	16,95	19,37	22,00
Intervención de servicios externos técnicos o legales	195,64	38,83	103,13
Coordinación con operadores móviles o autoridades para gestionar casos	12,00	12,00	12,00
Otros	4,25	2,25	7,11

Fuente: Requerimiento de información de la CRC sobre sobre el fraude cibernético por medio de llamadas de voz o del uso de códigos cortos.

En cuanto a los impactos económicos del fraude cibernético, se destaca que la suma de las compensaciones a clientes, las pérdidas estimadas para los usuarios y la cancelación de servicios por pérdida de confianza implicaron los costos más altos reportados, con una mediana que alcanzó más de $985 millones en compensaciones y $1.691 millones en pérdidas para usuarios solo en 2024. En este

sentido, este se constituye en el rubro de mayor relevancia en términos de los costos derivados de las acciones irregulares con fines de extorsión.

Ahora, es importante resaltar que, si bien la cancelación de servicios por pérdida de confianza presenta una disminución significativa durante el periodo de análisis, al experimentar una caída del 96,9% entre el 2022 y el 2024, las compensaciones económicas a clientes y las pérdidas estimadas para los usuarios presentan un crecimiento positivo para el mismo periodo, 31,5% y 113,3% respectivamente, y además tienen una participación significativa dentro del valor total reportado para este rubro.

Los costos relacionados con la respuesta frente al fraude, como la asignación de recursos humanos, la intervención de servicios técnicos y la coordinación con autoridades, muestran un comportamiento variable, con amplias fluctuaciones y una tendencia decreciente a lo largo del periodo. Dentro de este rubro los costos de mayor relevancia son los relacionados con las actividades de «Intervención de servicios externos técnicos o legales», dado que llegó a representar el 48,1% del valor total reportado para el 2024.

Ilustración 12. Fraude cibernético en 2024 discriminado por categoría de costo y sector

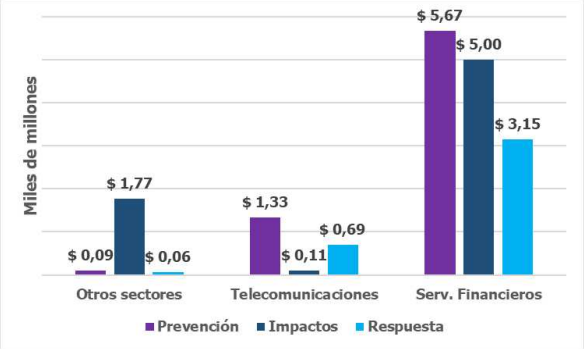
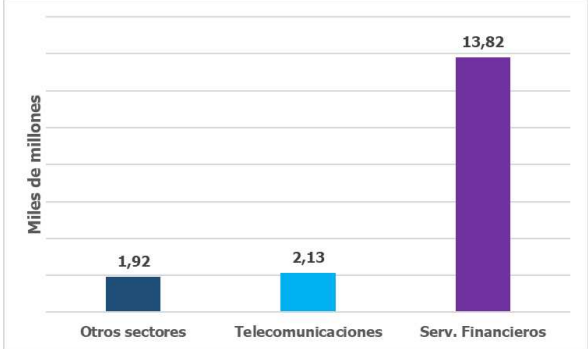


Ilustración 13. Valoración económica total del fraude cibernético en 2024 discriminado por sector



Fuente: Requerimiento de información de la CRC sobre sobre el fraude cibernético por medio de llamadas de voz o del uso de códigos cortos.

Al realizar la discriminación de la información reportada por sector económico se observa una alta heterogeneidad de las afectaciones económicas del fraude cibernético desarrollado mediante llamada de voz y mensajes de texto (SMS). Esto permite dimensionar con mayor precisión la magnitud y distribución del impacto económico del fraude cibernético, a partir de la información recolectada por esta Comisión mediante el requerimiento dirigido a distintos actores del ecosistema de comunicaciones móviles.

La Ilustración 12 discrimina el fraude cibernético en el año 2024 por categorías de costo (prevención, impactos y respuesta) y por sector afectado (otros sectores, telecomunicaciones y servicios financieros). Se observa que los servicios financieros concentran la mayor carga económica, con $13,82 mil millones en pérdidas totales, distribuidas principalmente en costos asociados a impactos directos del fraude ($5,67 mil millones) y a las acciones de respuesta institucional ($5,00 mil millones). Le siguen los costos de prevención ($3,15 mil millones), lo cual evidencia una alta inversión reactiva frente a la amenaza.

En comparación, el sector de telecomunicaciones reporta una carga económica significativamente menor, aunque no despreciable: $2,13 mil millones, concentrados también en impactos ($1,33 mil millones), seguidos de respuesta ($0,69 mil millones) y prevención ($0,11 mil millones). Por su parte,

los otros sectores suman $1,92 mil millones, con un patrón de mayor gasto en los impactos económicos posterior al incidente. La Ilustración 13 sintetiza la valoración económica total del fraude cibernético por sector, y reafirma que las entidades del sector financiero son las que reportan una mayor afectación, concentrando más del 77,3% del total reportado, lo que plantea un escenario de alta exposición a los efectos de este tipo de conductas irregulares.

De forma complementaria, también resulta relevante considerar las acciones irregulares con fines de fraude que se cometen por medio del uso del servicio de llamadas de voz. En este contexto, actualmente existen lineamientos normativos orientados a restringir las comunicaciones no autorizadas desde el interior de los Establecimientos de Reclusión del Orden Nacional (ERON). En particular, el Decreto 851 de 2024 indica en su parte considerativa que el gobierno cuenta con:

> «[…] medidas tendientes a articular mecanismos entre el INPEC, la Fiscalía General de la Nación y los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM), para que ante estos últimos puedan adelantarse solicitudes de bloqueo de Equipos Terminales Móviles (ETM) - a través de su número de identificación IMEI (International Mobile Station Equipment Identity) utilizados al interior de los establecimientos de reclusión penitenciaria y/o carcelaria para la planificación, comisión, ejecución y/o direccionamiento de delitos».

Este enfoque permite avanzar en la prevención de delitos que se originan desde establecimientos penitenciarios mediante el uso indebido de la red móvil, incluyendo la posible suplantación de identidad o la ejecución de esquemas de engaño telefónico, como el *vishing*.

Tabla 3. Bloqueos de líneas y equipos por llamadas no autorizadas en ERON.

PRSTM	Solicitudes bloqueo líneas telefónicas		Identificación de equipos y tarjetas SIM con llamadas no autorizadas	
	Pospago	Prepago	IMSI	IMEI
TIGO	21	132	153	214
CLARO	0	996	996	1290
WOM	40	63	104	153
MOVISTAR	0	16	16	13
SUMA	0	1	1	1
Total	**61**	**1208**	**1270**	**1671**

Fuente: Instituto Nacional Penitenciario y Carcelario (INPEC)

En este sentido, es importante señalar que, con base en la información del INPEC[39] que se encuentra en la Tabla 3, entre el mes de diciembre de 2024 y marzo de 2025 se ha solicitado el bloqueo de 1.269 líneas telefónicas vinculadas a llamadas no autorizadas desde Establecimientos de Reclusión del Orden Nacional (ERON). De estas, el 95% correspondieron a líneas prepago, siendo este el segmento predilecto como canal de origen para el desarrollo de este tipo de actividades irregulares.

[39] Respuesta al requerimiento de información con asunto «Información relacionada con presunto fraude cibernético por medio de servicios de telecomunicaciones móviles» mediante radicado de salida 2025200747.

De igual manera se observa que Claro y Tigo son los operadores con el mayor número de solicitudes en términos generales, mientras que WOM presenta un mayor número de solicitudes en el segmento pospago.

Adicionalmente, se han identificado 1.270 códigos[40] IMSI y 1.671 códigos IMEI asociados a equipos utilizados en llamadas no autorizadas desde los ERON, lo que demuestra un nivel de penetración de terminales móviles en contextos restringidos que sugiere un posible uso rotativo de SIMs en un mismo equipo, teniendo en cuenta que hay un 31,6% más de solicitudes de bloqueos de tarjetas que equipos.

Al igual que en las solicitudes de bloqueos de líneas, Claro con 1.290 y Tigo con 214 son los operadores con el mayor número de solicitudes de bloqueos de equipos y tarjetas SIM durante el periodo de referencia del requerimiento de información.

Por último, es importante resaltar que la información aportada por las diferentes empresas y entidades que participaron por medio del aporte de información constituye un insumo relevante para los análisis que se efectúen en las diferentes etapas del presente proyecto regulatorio. En este sentido, la construcción del árbol del problema y de la consulta pública descritas en las secciones 4.2 y 7 de este documento, respectivamente, se encuentran alineados con dichos insumos de información.

Por supuesto, estos análisis se plantean en el marco del alcance definido para esta iniciativa, de manera que se garantiza que tanto la problemática como las alternativas por las que se preguntan en la consulta se mantienen dentro de los límites de competencia establecidos y son concordantes con los objetivos específicos que fueron trazados.

No obstante, estos resultados también demuestran la necesidad de realizar esfuerzos conjuntos entre diferentes organismos públicos e incluso, entre las entidades de gobierno y los privados, con el fin de mitigar los riesgos del fraude cibernético por medio de los servicios de llamadas de voz y de envío de SMS.

Es importante reconocer que las prácticas fraudulentas no encuentran límites en las fronteras geográficas ni obstáculos en las modificaciones normativas, sino que, por el contrario, su carácter transversal, y de rápida y constante evolución les permite aprovechar la brecha que existe entre la expedición de regulación y los avances tecnológicos y de ingeniería social.

4.1.3 Recursos de identificación administrados por la CRC

Sea lo primero mencionar que los recursos de identificación hacen parte del conjunto de recursos físicos y lógicos utilizados en la prestación de servicios de telecomunicaciones, o en la explotación de las redes de telecomunicaciones que ofrecen dichos servicios. Si bien no existe una definición normativa de «recursos de identificación», a partir de diferentes recomendaciones expedidas por la Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés), la CRC ha indicado que estos recursos se pueden entender como todas aquellas series de cifras, caracteres y símbolos representados

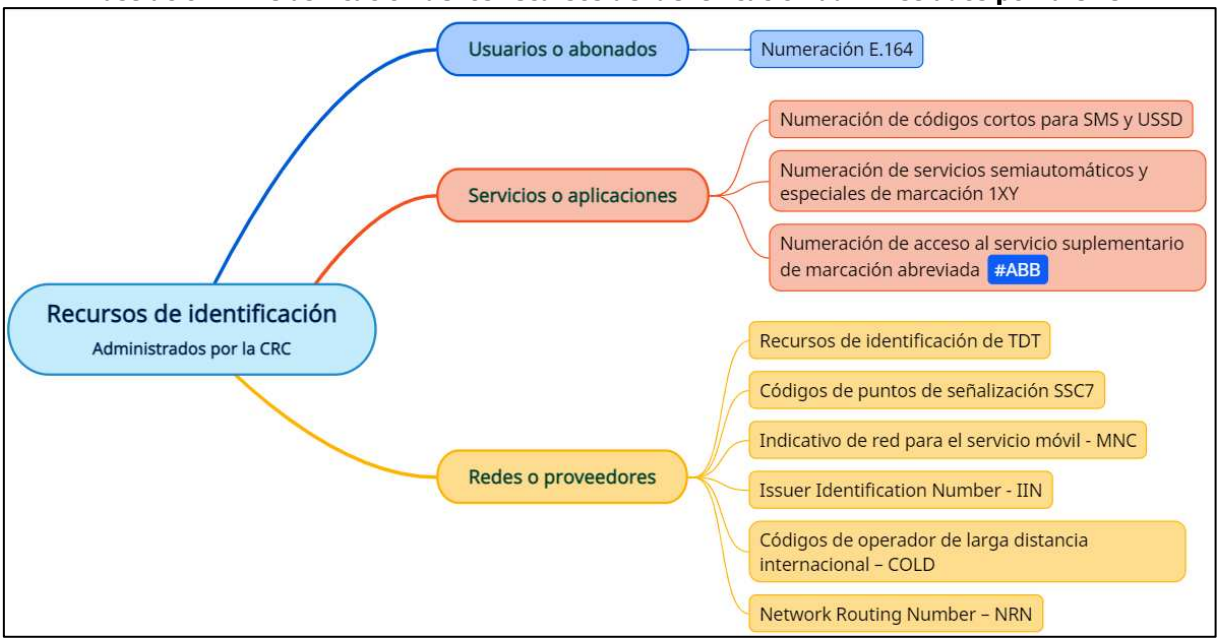
[40] De acuerdo con la Resolución CRC 5050 de 2016, la definición de código IMSI es:
IMSI: Código de Identificación Internacional del Abonado o Suscriptor Móvil (por sus siglas en inglés). Código único que identifica a cada abonado del servicio de telefonía móvil en el estándar GSM y en redes de nueva generación, y que adicionalmente permite su identificación a través de la red. El código se encuentra grabado electrónicamente en la tarjeta SIM.
IMEI: Identificador Internacional de Equipo Móvil, por sus siglas en Inglés.

en forma de indicativos, números, nombres, direcciones o identificadores, de dominio público o privado, utilizados en el proceso de registro y autorización en las redes de telecomunicaciones para identificar inequívocamente a un abonado, un usuario, un elemento de red, una función, una entidad de red, un servicio o una aplicación[41].

Como se explicó en la sección 3.1 de este documento, de conformidad con lo establecido en la Ley 1341 de 2009, la CRC cuenta con la competencia para regular y administrar los recursos de identificación utilizados en la provisión de redes y servicios de telecomunicaciones. Esta función incluye la planificación, asignación, devolución, verificación del uso y recuperación de dichos recursos, garantizando su disponibilidad general y uso eficiente debido a su naturaleza de recursos escasos.

En este contexto, los diez recursos de identificación administrados en la actualidad por la CRC, clasificados por aquellos destinados a identificar usuarios o abonados, redes o proveedores, servicios o aplicaciones, se muestran en la Ilustración 14.

Ilustración 14. Clasificación de los recursos de identificación administrados por la CRC.



Fuente: Elaboración CRC.

A continuación, se presenta una descripción breve de cada uno de los recursos de identificación previamente clasificados, a partir del marco regulatorio establecido para ello, compilado en el Título VI de la Resolución CRC 5050 de 2016. El propósito es contextualizar técnicamente la definición específica, destacar su función en el ecosistema digital y explicar sintéticamente su estructura, haciendo énfasis en los recursos denominados «códigos cortos» y «numeración E.164», debido al riesgo latente de que estos sean usados de manera irregular con fines de fraude durante el proceso de originación de

[41] CRC. Documento soporte de la propuesta publicada en el marco del proyecto *Revisión Integral del Régimen de Administración de Recursos de Identificación*. Julio de 2019. [en línea]. Consultado en el siguiente enlace: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-71-2/Propuestas/8_reqmenaripublicacion.pdf

comunicaciones, especialmente por medio de llamadas de voz tradicionales y mensajes cortos de texto (SMS).

- **Recursos destinados a identificar redes o proveedores**

a) Recursos de Identificación para Televisión Digital Terrestre (TDT)[42]

Se trata de una serie de identificadores asignados a operadores de TDT para permitir la transmisión ordenada de contenidos audiovisuales. Su función es asegurar la unicidad y trazabilidad de las señales digitales bajo el estándar adoptado en Colombia (DVBT2). Su estructura es alfanumérica y está definida por la CRC según el tipo de red, cobertura y servicio.

b) Códigos de Punto de Señalización (SSC7)[43]

Estos códigos se utilizan en la red de señalización por canal común número 7 para identificar nodos de red. Su función es permitir el enrutamiento de mensajes de señalización entre centrales de un mismo proveedor o incluso de distintos proveedores. Están estructurados en 14 bits divididos de tal manera que se puede identificar la zona, la red y el nodo de señalización.

c) Indicativo de Red para el Servicio Móvil (MNC)[44]

Es un código que identifica a un operador móvil dentro del IMSI. Su función es permitir la autenticación y localización del abonado en redes móviles a nivel mundial. Se estructura con tres dígitos que, junto con el código de país (MCC), forman el identificador de red internacional.

d) Issuer Identification Number (IIN)[45]

Este número identifica al emisor de una tarjeta SIM. Su función es asociar la tarjeta con un operador específico y permitir la autenticación del usuario. Está compuesto por el MCC, el MNC y el MSIN, formando el IMSI completo.

e) Códigos de Operador de Larga Distancia Internacional (COLD)[46]

Son códigos asignados a operadores para la prestación de servicios de larga distancia internacional. Su función es identificar al operador elegido por el usuario en el sistema de multiacceso para realizar una llamada de voz tradicional de larga distancia internacional. Su estructura es numérica, de una y tres cifras, precedida por el prefijo 00.

f) Network Routing Number (NRN)[47]

[42] Resolución CRC 5050 de 2016. Capítulo 11 del Título VI.
[43] Ibid. Capítulo 3 del Título VI.
[44] Ibid. Capítulo 5 del Título VI.
[45] Ibid. Capítulo 6 del Título VI.
[46] Ibid. Capítulo 8 del Título VI.
[47] Ibid. Capítulo 9 del Título VI.

Este número se utiliza para el enrutamiento de llamadas en redes móviles, especialmente en contextos de portabilidad numérica. Su función es identificar la red de un número portado para direccionar correctamente las llamadas hacia el operador que aloja el número. Está compuesto por una cadena de 10 dígitos que incluye el código de red y el número de abonado.

- **Recursos destinados a identificar servicios o aplicaciones**

a) Numeración 1XY para servicios semiautomáticos y especiales[48]

Estos códigos de tres cifras están reservados para servicios semiautomáticos y especiales, como el número único nacional de emergencias 123. Su función es garantizar a los usuarios el acceso inmediato a servicios de interés general y acceso universal. Su estructura es fija y comienza con el dígito 1, seguido de dos cifras que identifican el servicio específico. Los servicios de interés general que se pueden ofrecer mediante esta numeración se clasifican en cuatro modalidades en función de los costos asumidos por los operadores, los prestadores del servicio y/o por los usuarios.

b) Numeración de acceso al servicio suplementario de marcación abreviada (#ABB)[49]

Son números de marcación corta similares a los de estructura 1XY, pero con la diferencia esencial de que pueden ser usados para servicios comerciales y de interés general. Su estructura incluye el símbolo especial hashtag o numeral (#) seguido de una secuencia numérica de tres dígitos.

c) Códigos Cortos para SMS y USSD[50]

De conformidad con las definiciones establecidas en la Resolución CRC 5050 de 2016, los códigos cortos son un 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 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, por medio de un código numérico estructurado por cadenas de 5 y 6 dígitos, que busca informar desde su estructura el tipo de servicio, el contenido, la modalidad de compra y los costos asociados, y no está destinado para la creación de un canal de comunicación dedicado de SMS entre los usuarios finales del servicio de telefonía móvil y sus clientes.

Por lo tanto, la numeración de códigos cortos tiene la función de permitir la provisión de servicios de contenidos o aplicaciones, prestados por medio de SMS y USSD, por parte de proveedores de contenidos y aplicaciones e integradores tecnológicos, de tal manera que el usuario pueda distinguir mediante el número la modalidad de compra (única vez - suscripción), el tipo de servicio (concursos masivos-votaciones), el contenido específico (adultos - otros) y el costo del servicio (gratuito - pago).

Al respecto, es importante aclarar que el fundamento de la armonización de los códigos cortos es la orientación y protección al usuario final, destinatario del mensaje, y tiene por objeto facilitar procesos transparentes de información y publicidad permitiendo el posicionamiento de códigos únicos utilizables

[48] Ibid. Capítulo 7 del Título VI.
[49] Ibid. Capítulo 10 del Título VI.
[50] Ibid. Capítulo 4 del Título VI.

en las redes de todos los proveedores de redes y servicios que estén en capacidad de generar y recibir SMS.

Teniendo en cuenta lo anterior, para proveedores que no buscan el posicionamiento e identificación de un tipo de servicio de contenidos y aplicaciones para los usuarios mediante un código numérico que informe claramente el tipo de tarifa y el generador del contenido, sino la creación de un canal de comunicación dedicado de SMS entre los usuarios finales del servicio de telefonía móvil y sus clientes, la CRC ha identificado que dicha modalidad corresponde a la figura de prestación de servicios SMS enmarcada en la clasificación de «SMS Service Providers» propuesta en el Reporte 212 del *Electronic Communications Committee* de la *European Conference of Postal and Telecommunications Administrations* (ECC Report 212)[51], la cual debe utilizar la numeración E.164 no geográfica de servicios para su operación[52], teniendo en cuenta que ese tipo de números son de acceso universal y significancia nacional, y además permiten garantizar la disponibilidad y suficiencia de recursos en el mediano y largo plazo, como se describe a continuación.

- **Recursos destinados a identificar usuarios o abonados**

a) Numeración E.164[53]

De conformidad con la Recomendación UIT-T E.101[54], el número E.164 se define como una «(…) cadena de cifras decimales que cumple las tres características (a saber, estructura, longitud del número y singularidad) especificadas en [UIT-T E.164]. El número contiene la información necesaria para cursar la llamada hasta el usuario o el punto desde el que se presta el servicio».

En la misma línea, según el artículo 16 del Decreto 25 de 2002, compilado en el Decreto 1078 de 2015, la numeración E.164 es un conjunto de recursos lógicos que permiten acceder a las redes de telecomunicaciones y proporciona información sobre tarifas y servicios a fin de proteger al usuario. Estos números, definidos como cadenas de dominio público, permiten identificar a los abonados o usuarios para acceder a los servicios ofrecidos por los proveedores asignatarios.

Esta numeración está conformada por un código de país (57 para Colombia), un indicativo nacional de destino de tres dígitos y un número de abonado de siete dígitos, por lo que el número internacional tiene una longitud fija de 12 dígitos y se clasifica en la numeración geográfica (destinada a identificar servicios de voz fija) y la numeración no geográfica (destinada a identificar redes y servicios que no se circunscriben a delimitaciones político-administrativas).

La numeración no geográfica se divide en dos subcategorías: redes y servicios. La numeración de redes se utiliza para identificar a los usuarios de las redes móviles, mientras que la numeración de servicios se emplea para identificar los servicios ofrecidos por los PRST, como se detalla en la Tabla 4.

[51] Electronic Communications Committee of European Conference of Postal and Telecommunications Administrations (CEPT). *ECC Report 212. Evolution in the Use of E.212 Mobile Network Codes*. Aprobado el 9 de abril de 2014. [en línea]. Consultado en el siguiente enlace: https://docdb.cept.org/download/1152

[52] La CRC ha asignado numeración no geográfica de servicios bajo el NDC 940 a Proveedores de Redes y Servicios de Telecomunicaciones que ofrecen servicios SMS-SP conforme la descripción contenida en el SIGRI (https://pnn.gov.co/mapa/).

[53] Op. Cit. Resolución CRC 5050 de 2016. Capítulo 2 del Título VI.

[54] Definición de los términos utilizados en las Recomendaciones de la serie E para los identificadores (nombres, números, direcciones y otros) en redes y servicios públicos de telecomunicaciones.

Tabla 4. Subclasificación de la numeración de servicios.

NDC	Servicio	Descripción	Significancia
800	Cobro Revertido	Aplica para todos aquellos servicios en los cuales la llamada se carga al abonado destino	Nacional (1)
801 a 899	Reserva	Reserva	
900	Otros Servicios	Esquema de numeración para servicios que no tienen tarifa con prima	Nacional (1)
901 a 909	Tarifa con Prima	Esquema de numeración para servicios con cobro de tarifa con prima	Nacional (1)
910 a 919	M2M – IoT	Esquema de numeración para identificar comunicaciones M2M – IoT	Nacional (1)
920 a 939	Reserva	Reserva	
940	SMS-SP	Numeración para acceder a contenidos y aplicaciones soportados en SMS y USSD	Nacional (1)
941 a 946	Reserva	Reserva	
947	Acceso a Internet	Numeración para la prestación del servicio de acceso a Internet según lo dispuesto en la Res. 307 de 2000	Local (2)
948	Acceso a Internet por demanda	Acceso a Internet cuando no se usan los planes de tarifa reducida o plana	Local (2) / Nacional (1)
949 a 998	Reserva	Reserva	
999	Pruebas	Realización de pruebas de puesta en marcha de servicios o elementos de red al interior de las redes.	Nacional (1)

Fuente: SIGRI[55].

La numeración atribuida en el NDC 940 destaca dentro de esta subclasificación, siendo utilizada para identificar servicios de acceso a contenidos y aplicaciones soportados en SMS y USSD por parte de PRST. Esta numeración se diferencia de los códigos cortos principalmente en la longitud del número, ya que se trata de cadenas de 10 dígitos, y en que, al tratarse de numeración E.164, los asignatarios son exclusivamente los PRST y no los PCA e Integradores Tecnológicos.

4.1.4 Cadena de valor de los servicios de llamada de voz y de mensajes cortos de texto

Teniendo en consideración el enfoque especial que se otorga sobre los recursos de identificación de numeración E.164 y Códigos Cortos para SMS y USSD, debido al riesgo latente de que estos sean usados de manera irregular, desde la óptica económica y de mercado, resulta fundamental describir las cadenas de valor que soportan la prestación de los servicios de llamadas de voz y de envío de SMS, a fin de detallar las funciones que se generan en los diferentes eslabones, los agentes que intervienen en las comunicaciones y las potenciales vulnerabilidades en la cadena.

Las cadenas involucran a múltiples actores; incluidos operadores de red, proveedores de contenidos y aplicaciones, integradores tecnológicos, usuarios, entre otras, cuyas interacciones técnicas, comerciales y contractuales soportan la originación, transporte y entrega de las comunicaciones de voz y SMS. En

[55] Sistema de Información y Gestión de Recursos de Identificación disponible en el siguiente enlace: https://pnn.gov.co/mapa/

este sentido, resulta útil comprender la cadena de valor desde la perspectiva del flujo de la comunicación[56] con el fin de identificar los puntos críticos de vulnerabilidad.

Los servicios tradicionales de llamadas de voz y de envío de SMS cuentan con procesos de comunicación distintos, que, si bien comparten ciertos componentes técnicos estructurales, difieren en elementos propios de cada modelo de negocio, los cuales intervienen en el proceso de originación, transporte y terminación de la comunicación.

Estas diferencias impactan directamente la manera en que se configuran los flujos de información, los recursos de identificación utilizados, los actores involucrados, así como los riesgos asociados. Por esta razón, a continuación, se describe de forma separada la cadena de valor correspondiente a cada uno de estos servicios, con el fin de reflejar adecuadamente sus particularidades en el contexto del presente análisis regulatorio.

En primer lugar, una cadena de valor del servicio de llamadas de voz tradicional enfocada en el flujo de la comunicación iniciaría por el usuario que origina la llamada. Este usuario cuenta con un número telefónico E.164 que permite su autenticación en la red fija o móvil de origen, el cual es adjudicado por su operador de red, quien, para establecer la comunicación de voz con otro abonado fijo o móvil, debe conocer previamente el número telefónico E.164 que identifica al usuario de destino.

En el momento en que el usuario que origina la llamada marca el número E.164 del usuario de destino, la red del operador de origen transmite vía señalización tanto el número de origen como el número de destino, función que facilita tanto la identificación de la llamada del usuario que origina la comunicación, como el eventual filtrado de números que no se encuentren autorizados para generar o terminar una llamada específica. Esto permite a la red central enrutar las llamadas autorizadas a la ubicación del usuario de destino, ya sea dentro de la misma red o en la red de otro operador, habilitando así un canal de voz para el establecimiento de la comunicación.

Dado el caso que la comunicación de voz solicitada no tenga como destino la propia red del proveedor de origen, el enrutamiento de las llamadas se dirige hacia las diferentes interconexiones que se tengan establecidas en la red. Para este caso pueden presentarse tanto interconexiones directas[57], que son las que cuentan con acuerdos técnicos, jurídicos y económicos previos, como interconexiones indirectas[58], que son las que usan las redes de terceros para transportar su tráfico hacia el operador de destino dada la ausencia de una interconexión directa.

En esta línea, la cadena de valor del servicio de voz desde la óptica del flujo de la comunicación se conforma por el usuario de origen, por la red que soporta el servicio de dicho usuario, por el operador

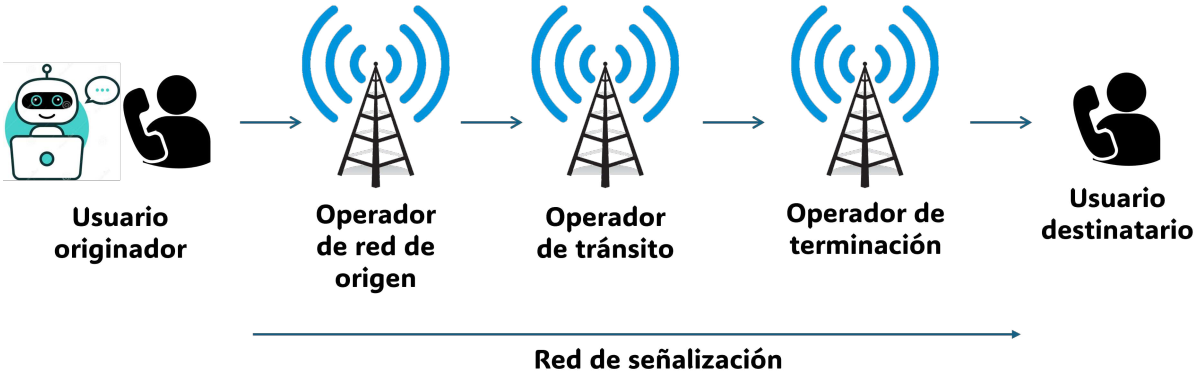
[56] Es importante resaltar que la cadena de valor desde la perspectiva del flujo de la comunicación se centra en las etapas técnicas y operativas que intervienen desde la originación de la comunicación hasta su recepción. A diferencia de una cadena de valor desde la perspectiva del valor agregado en donde se identifican cada una de las actividades que aumentan el valor percibido por el usuario final. Ver: Zamora, E. A. (2016). Value chain analysis: A brief review. Asian Journal of Innovation and Policy, 5(2), 116-128. DOI: http//dx.doi.org/10.7545/ajip.2016.5.2.116

[57] Resolución CRC 5050 de 2016. Título I. «INTERCONEXIÓN DIRECTA: Es la interconexión entre las redes de dos proveedores de redes y servicios de telecomunicaciones que comparten al menos un punto físico de intercambio de tráfico entre ellas, con el objeto de lograr el interfuncionamiento de redes y la interoperabilidad de plataformas, servicios y/o aplicaciones».

[58] Ibid. «INTERCONEXIÓN INDIRECTA: Es la interconexión que permite a un proveedor de redes y servicios de telecomunicaciones interconectar su red con la red de otro proveedor de redes y servicios de telecomunicaciones, a través de la red de un tercero que actúa como proveedor de tránsito cuya red tiene una interconexión directa con ambas redes».

de tránsito que ante una eventual interconexión indirecta lleva la comunicación hasta la red del abonado de destino, la red del abonado o usuario de destino y finalmente por el usuario que recibe la comunicación. Esta cadena de valor se muestra gráficamente en la Ilustración 15.

Ilustración 15. Cadena de valor general del servicio de voz.



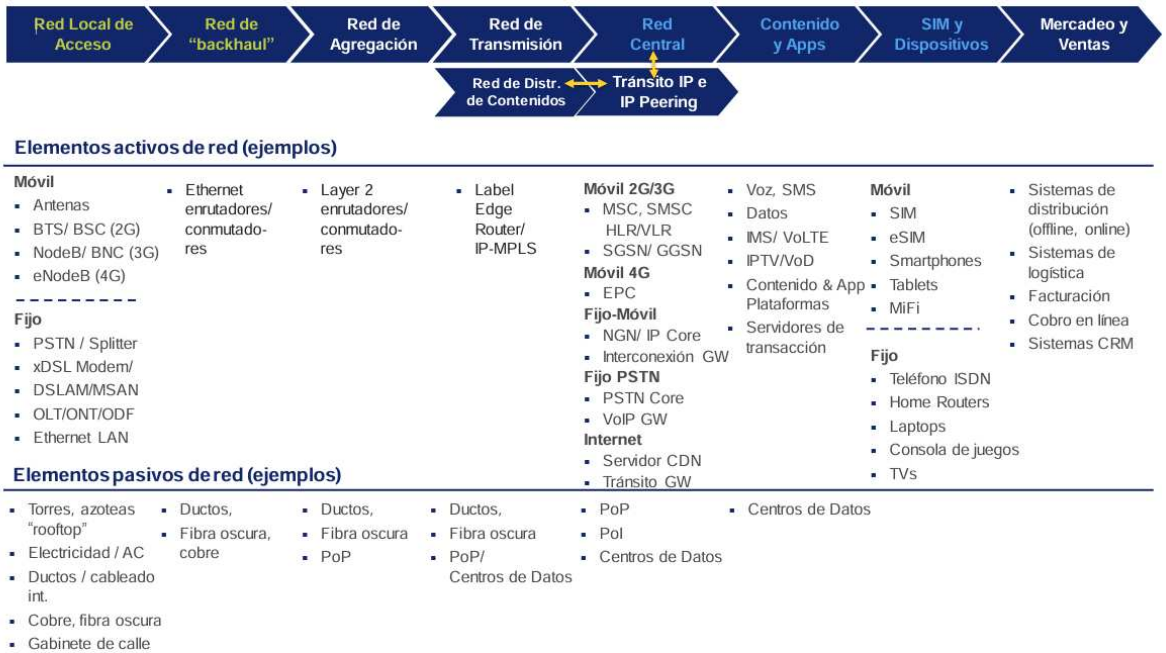
Fuente: Elaboración CRC.

En aras de dar un mayor detalle desde el punto de vista técnico y funcional de la cadena de valor del servicio de voz, vale la pena traer a colación la cadena de valor convergente construida por Detecon en el año 2017 para la CRC en el marco del estudio denominado «Cadena de valor y cadenas de acceso e interconexión en Colombia. Análisis de problemas de modelos de acceso existentes y conclusiones»[59], en donde se destacan los elementos de red activos y pasivos tanto para las redes fijas como para las redes móviles. Es importante mencionar que, bajo el enfoque convergente de los servicios de telecomunicaciones, la cadena de valor a la que se hace referencia también soporta el flujo de la comunicación de los servicios de mensajería de texto P2P o B2P, en la cual el recurso de identificación involucrado es la numeración E.164.

[59] Documento disponible en el siguiente vínculo https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-59-4/Propuestas/cadena-valor-redes.pdf y que hace parte de la revisión del régimen de acceso, uso e interconexión que culminó con la expedición de la Resolución CRC 6522 de 2022. La información del proyecto regulatorio puede ser accedida mediante el siguiente enlace: https://www.crcom.gov.co/es/proyectos-regulatorios/2000-59-4.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Ilustración 16. Elementos de red activos y pasivos a través de la cadena de valor convergente.



BTS = Base Transceiver Station; BSC = Base Station Controller; BNC = Base Network Controller; eNodeB = evolved NodeB; PSTN = Public Switched Telephony Network; xDSL = Digital Subscriber Line; DSLAM = Digital Subscriber Line Access Multiplexer; MSAN = Multi-service Access Node; OLT = Optical Line Terminal; ONT = Optical Network Termination; ODF = Optical Distribution Frame; LAN = Local Area Network; AC = Air Conditioning; PoP = Point of Presence; MPLS = Multiprotocol Label Switching; MSC = Mobile Switching Center; SMSC = Short Message Service Center; SGSN = Serving GPRS Support Node; GGSN = Gateway GPRS Support Node; EPC = Evolved Packet Core; GW = Gateway; CDN = Content Distribution Network; PoI = Point of Interconnection; IMS = IP Multimedia Subsystem; VoLTE = Voice over LTE; IPTV/VoD = TV over IP / Video on Demand; SIM = Subscriber Identification Module; eSIM = embedded SIM; MIFI = Portable Broadband Device; ISDN = Integrated Services Digital Network; TV = Television; CRM = Customer Relationship Management

Fuente: Detecon 2017 - Informe sobre cadena de valor y cadenas de acceso e interconexión en Colombia.

Por su parte, una cadena de valor del servicio de mensajes cortos de texto vista desde la perspectiva del flujo de la comunicación iniciaría cuando una entidad originadora decide enviar a sus usuarios finales un mensaje de texto. Estos mensajes pueden generarse, entre otras razones, con fines publicitarios o para atender necesidades operativas del negocio, como el envío de claves de autenticación o confirmaciones de transacciones. En algunos casos, las entidades originadoras delegan esta función en un socio comercial, generalmente una empresa especializada que opera plataformas de mensajería masiva y ejecuta campañas a su nombre.
En otros casos, esta relación se establece directamente con un Proveedor de Contenidos y Aplicaciones (PCA). En este sentido, a diferencia de la cadena de valor del servicio de llamada de voz, en este caso el flujo de la comunicación del servicio SMS es A2P y emplea el recurso de identificación de códigos cortos en su originación y la numeración E.164 en su terminación.

Es importante señalar que el PCA es el titular del código corto o número de origen, asignado por la CRC como administrador del recurso de identificación. Dicho actor debe cumplir con los requisitos establecidos en la regulación, incluyendo la inscripción en el Registro de Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos (RPCAI), y seguir el procedimiento de asignación definido por la Comisión en el Título VI de la Resolución CRC 5050 de 2016.

Así mismo, es relevante aclarar que, desde una perspectiva funcional o basada en atributos, una entidad originadora o un socio comercial puede registrase como PCA. Sin embargo, desde la visión del flujo de la comunicación, estas funciones deben entenderse como operativamente separadas, ya que implican distintos roles y responsabilidades dentro del proceso de originación.

En este eslabón de la cadena, el mensaje puede ser canalizado por medio de un integrador tecnológico, quien establece la conexión técnica entre el PCA y el Proveedor de Servicios de Telecomunicaciones Móviles (PRSTM). Este actor tiene un rol clave en el formato, control de tráfico y autenticación del mensaje, siendo además un punto potencial de vulnerabilidad si no se aplican medidas de seguridad robustas. Nuevamente, en este punto la relación entre el PCA y el PRSTM se puede dar directamente cuando el PCA cuenta con la capacidad de gestionar el tráfico sin intermediarios.

Ilustración 17. Eslabones de la cadena de valor de SMS.

Fuente: Elaboración CRC.

Por último, el mensaje es entregado al PRSTM, quien utiliza su infraestructura de red para terminar la comunicación en el equipo terminal móvil del usuario destinatario. El usuario, identificado por su número telefónico E.164, recibe el mensaje de texto en su dispositivo móvil. En cada eslabón, existen elementos técnicos de control, tales como validación del remitente, políticas anti-spam, autenticación de mensajes y trazabilidad del código corto utilizado. En la Ilustración 17 se presenta un esquema de la cadena de valor de servicios SMS, en el que se indica con color verde aquellos eslabones que pueden considerarse como opcionales en las relaciones comerciales entre los diferentes actores involucrados.

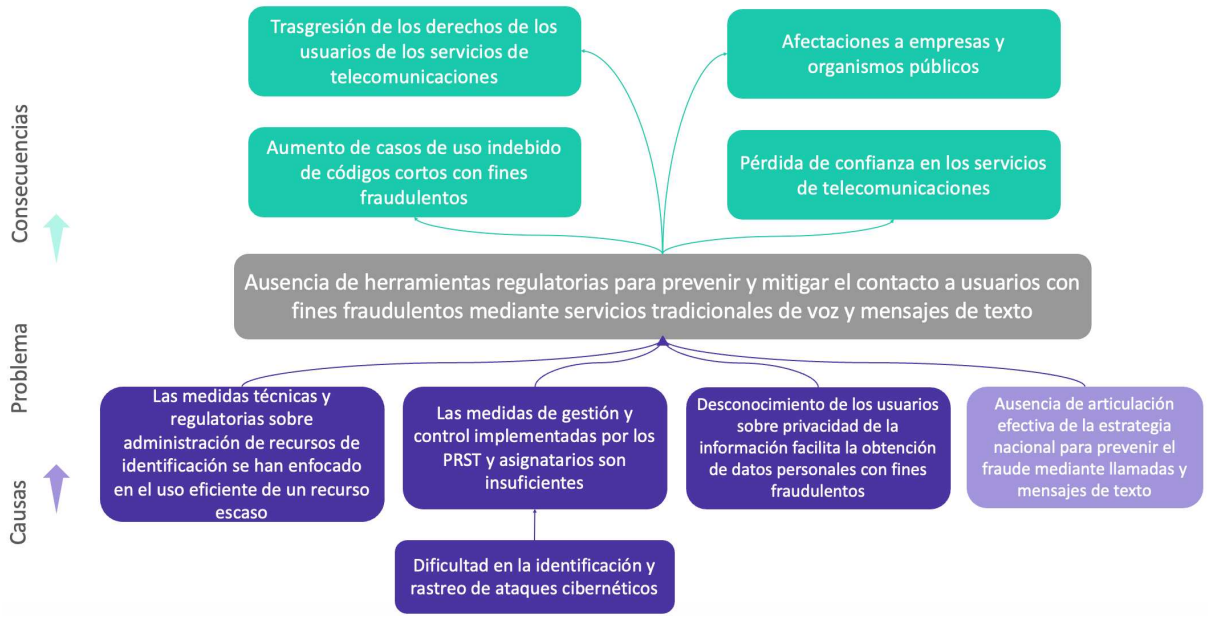
Así las cosas, en la cadena de valor del servicio SMS, los principales recursos de identificación involucrados son la numeración E.164 del usuario destinatario, utilizada para dirigir el mensaje de texto (SMS), y el código corto o número de origen asignado al PCA, que permite identificar al remitente de la comunicación.

Sin embargo, a lo largo de esta cadena se presentan diversas vulnerabilidades que pueden ser explotadas para ejecutar campañas irregulares con fines fraudulentos. Por ejemplo, si un PCA, en su rol de asignatario del código corto, presta servicios a un tercero sin realizar la debida autenticación del remitente o ejercer un control efectivo sobre la cesión del uso del código, se puede facilitar la suplantación de entidades legítimas, permitiendo así la circulación de mensajes engañosos o maliciosos hacia los usuarios.

4.2. Árbol del Problema

De acuerdo con lo expuesto hasta el momento, el problema a ser resuelto con ocasión del presente proyecto regulatorio es el siguiente: «Ausencia de herramientas regulatorias para prevenir y mitigar el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto». En la Ilustración 18, se presenta el correspondiente árbol de problema con sus respectivas causas y consecuencias.

Ilustración 18. Árbol del problema identificado.



Fuente: Elaboración CRC.

4.2.1. Causas del problema

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

Frente a esta causa es preciso mencionar que, si bien la Comisión ha venido definiendo en la regulación las condiciones para la administración de los recursos de identificación durante las últimas 2 décadas, dichas condiciones se han circunscrito al establecimiento de definiciones, parámetros, requisitos y procedimientos de asignación, uso eficiente y recuperación de estos recursos escasos.

Como se indicó en detalle en la subsección 3.1.1 de este documento, en esta línea se diseñó en su momento la Resolución CRT 2028 de 2008 «Por la cual se expiden las reglas para la gestión, uso, asignación y recuperación del recurso de numeración y se dictan otras disposiciones», la cual definió las condiciones para la administración y uso eficiente de la numeración E.164.

Otro gran hito regulatorio en materia de recursos de identificación es la Resolución CRC 5968 de 2020 «Por la cual se establece el Régimen de Administración de Recursos de Identificación, se da cumplimiento al artículo 7 del Decreto 555 de 2020 y se dictan otras disposiciones». Mediante este acto, si bien la Comisión amplió el alcance de la Resolución CRT 2028 de 2008 para los diez recursos de identificación que administra, implementó un sistema integral de administración cuyo objetivo fue la garantía de su disponibilidad para los próximos 10 años, por lo que incluyó condiciones de administración y uso eficiente de manera detallada y específica para cada recurso.

De esta manera, y a pesar de la relevancia de los recursos de identificación en el establecimiento de la comunicación con los usuarios finales, dentro del marco de la regulación y administración de dichos

recursos, no se ha explorado la definición de reglas específicas orientadas a generar información o a establecer condiciones regulatorias para mitigar el fraude, como la suplantación de identidad o el uso indebido de la numeración.

En todo caso, resulta pertinente indicar que, lo anterior no constituye una omisión de sus competencias toda vez que, desde la perspectiva de la protección de los derechos de los usuarios de los servicios de telecomunicaciones, esta Comisión ha implementado, aunque de manera general, los primeros avances en materia de prevención contra el fraude. De esta manera, por una parte, mediante el artículo 2.1.10.7[60] de la Resolución CRC 5050 de 2016, se obliga a los PRST a usar herramientas tecnológicas adecuadas para prevenir que se cometan fraudes al interior de sus redes, las cuales deberán someterse a controles periódicos para determinar su efectividad. Y, por la otra, puntualmente respecto al uso de códigos cortos, según el artículo 2.1.18.6[61] de la misma resolución, los otros agentes de la cadena de valor también tienen el deber de hacer uso de herramientas tecnológicas, a las cuales, además, deben efectuarles controles periódicos de efectividad, con el objetivo de prevenir el fraude.

A pesar de lo anterior, el contexto actual, caracterizado por un aumento en los casos de fraude digital y una mayor dependencia de los servicios móviles para transacciones sensibles, hace inocuas estas primeras aproximaciones generales y exige la ampliación tanto del alcance del régimen de administración de los recursos de identificación, como de su enfoque, reconociendo su relevancia en el contacto a usuarios finales mediante servicios tradicionales de voz y SMS. De esta manera, se contribuiría a la protección de los derechos de los usuarios, su seguridad y confianza en el ecosistema digital.

4.2.1.2. Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes

Otra causa del problema es la insuficiencia de las medidas de gestión y control implementadas por los PRST y los asignatarios de los recursos de identificación, las cuales no han sido diseñadas ni ejecutadas con un enfoque preventivo frente al fraude. Aunque los operadores cumplen con los lineamientos mínimos y generales establecidos por la regulación vigente, ya mencionados, en muchos casos estas medidas se limitan a aspectos operativos y administrativos, sin incorporar mecanismos robustos de verificación de identidad, trazabilidad del uso de los recursos o monitoreo proactivo de actividades sospechosas lo cual dificulta el actuar de las autoridades al momento de la investigación de una denuncia.

De acuerdo con los resultados del requerimiento de información descritos en la sección 4.1.2 de este documento, el uso de protocolos internos de respuesta a incidentes es la principal medida de ciberseguridad implementada para la prevención del fraude cibernético. El 63,6% de las empresas manifestó tener procedimientos estandarizados que se activan de forma posterior a la detección de un incidente de fraude o ciberataque. Sin embargo, este enfoque es una medida reactiva que se aplica una vez la acción irregular ha sido ejecutada.

---

[60] Resolución CRC 5050 de 2016. «ARTÍCULO 2.1.10.7. 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 […]».

[61] Ibid. «ARTÍCULO 2.1.18.6 PREVENCIÓN DE FRAUDES DE LOS PCA E INTEGRADORES TECNOLÓGICOS ASIGNATARIOS DE CÓDIGOS CORTOS. Los PCA e Integradores Tecnológicos que sean asignatarios de códigos cortos deberán hacer uso de herramientas tecnológicas para prevenir fraudes a través del envío de mensajes SMS o USSD y efectuar controles periódicos respecto de la efectividad de los mecanismos dispuestos para tal fin».

En este mismo sentido, se encontró que solo el 34,9% de las empresas cuenta con procedimientos para intercambio de alertas de fraude con proveedores de redes y servicios de telecomunicaciones móviles (PRSTM) u otras entidades. Así mismo, los hallazgos encontrados por medio del requerimiento de información muestran una alta heterogeneidad en las prácticas de los operadores, lo que dificulta la detección temprana de patrones de fraude y limita la capacidad de respuesta coordinada ante incidentes. Además, la falta de interoperabilidad entre sistemas y la escasa compartición de información entre actores del ecosistema de telecomunicaciones agravan la situación, permitiendo que los recursos de identificación sean utilizados de manera indebida sin una supervisión efectiva.

Teniendo en consideración que en la actualidad los recursos de identificación son utilizados como vectores de acceso a servicios financieros, gubernamentales y digitales, salta a la vista la ineficiencia de las medidas de autogestión y autocontrol que han implementado los diferentes agentes intervinientes en el flujo de la comunicación con los usuarios finales, sobre todo teniendo en cuenta que los rápidos avances tecnológicos dificultan aún más la identificación y rastreo de ataques cibernéticos, como se expone a continuación.

4.2.1.2.1. Dificultad en la identificación y rastreo de ataques cibernéticos

La insuficiencia de las medidas de gestión y control por parte de los PRST y asignatarios de recursos de identificación se agrava por la dificultad para identificar y rastrear ataques cibernéticos que comprometen a los usuarios. Esta limitación se debe, en gran parte, a la falta de articulación de medidas técnicas y operativas que permitan generar una trazabilidad de toda la cadena de comunicación, así como a la ausencia de sistemas integrados de prevención y alerta temprana.

Los ataques cibernéticos que afectan los servicios de telecomunicaciones —como el *SIM swapping*, la suplantación de identidad, el uso de numeración falsificada o el acceso no autorizado a plataformas de gestión— suelen ejecutarse de forma rápida y sofisticada, aprovechando brechas en los sistemas de autenticación y en la interoperabilidad entre operadores. La fragmentación de la información, la escasa estandarización de los registros de los diferentes actores de la cadena de comunicación, así como la falta de intercambio de datos entre actores del ecosistema, dificulta la reconstrucción de los hechos y la atribución de responsabilidades[62].

Esta situación no solo impide una respuesta oportuna ante incidentes, sino que también limita la capacidad de generar inteligencia preventiva en los operadores, y de fortalecer los mecanismos de control por parte de las autoridades competentes.

Por todo lo anterior, que las medidas de gestión y control de los agentes que intervienen en el flujo de la comunicación al usuario final adolezcan de insuficiencia, hace aún más gravoso el problema identificado, toda vez que, no solo no existen reglas específicas en el marco regulatorio, sino que tampoco se cuenta con controles desde la prestación de los servicios de telecomunicaciones en sí misma, lo que aumenta las brechas de vulnerabilidad y permite el contacto a usuarios con fines fraudulentos.

[62] Estas dificultades fueron puestas de presente en la mesa de trabajo llevada a cabo el 12 de febrero de 2025, en las instalaciones del MinTIC, en la que participaron la CRC, el ColCERT, el Cuerpo Técnico de Investigación (CTI) y el grupo de delitos informáticos de la Fiscalía General de la Nación y la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

4.2.1.3. Desconocimiento de los usuarios sobre privacidad de la información facilita la obtención de datos personales con fines fraudulentos

El derecho a la intimidad de las personas y de la familia es un derecho fundamental establecido en el artículo 15 de la Carta Política de Colombia. A partir de esta garantía constitucional, se han efectuado diferentes desarrollos normativos que buscan otorgar herramientas suficientes a los ciudadanos para exigir un tratamiento de sus datos personales acorde con los preceptos legales y constitucionales.

Tal es el caso de la Ley 1266 de 2008, la cual estableció las primeras reglas sobre privacidad de la información, específicamente enfocada al Habeas Data o información financiera, crediticia, comercial, de servicios y la proveniente de terceros países. Mediante este compendio normativo, el legislador estableció, principalmente, los siguientes derechos a los titulares de la información: (i) hábeas data, el cual hace referencia a «conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos»; y (ii) solicitar la prueba de la existencia de la autorización para el tratamiento de los datos personales. Estos derechos son exigibles tanto ante operadores de los bancos de datos como frente a las fuentes de información[63].

Posteriormente, con la expedición del régimen de protección de datos personales, por medio de la Ley 1581 de 2012, y su Decreto Reglamentario 1377 de 2013, el alcance de las prerrogativas en cabeza de los titulares de la información se amplió, otorgándoles las siguientes[64]:

(i) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento, cualquiera que sea la naturaleza de los datos, incluyendo aquellos datos cuyo tratamiento no haya sido autorizado;
(ii) Exigir la autorización previa, expresa e informada previo al tratamiento de los datos personales, lo cual incluye ser informado del uso que se dará a sus datos personales, antes de la solicitud; y
(iii) Revocar la autorización o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales;

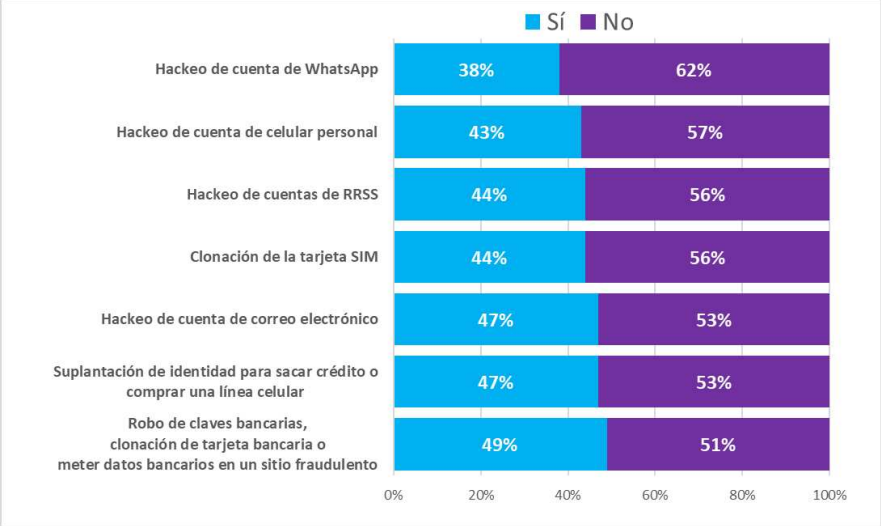
A pesar de que se han materializado estos desarrollos normativos, cruciales para la seguridad de la información personal de todos los ciudadanos, salta a la vista el desconocimiento de los titulares de los datos para ejercer sus derechos y exigir el cumplimiento de las obligaciones que tienen tanto responsables como encargados de la información. De esta manera, se ocasionan vulnerabilidades y espacios propicios para que los ciberdelincuentes lleven a cabo irregularidades por medio de los usuarios de servicios de telecomunicaciones móviles. Por ejemplo, según Kaspersky[65] las acciones irregulares con fines de fraude se aprovechan del desconocimiento de los usuarios respecto de la identificación de intentos de suplantación o solicitudes de datos engañosas, es decir, muchas personas no cuentan con la capacidad para distinguir cuáles acciones estarían por fuera del marco de las obligaciones de los responsables de custodiar la información sujeta de protección.

[63] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008. Artículo 6.
[64] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012. Artículo 8.
[65] Kasperky. What is Social Engineering?. Consultado el 28 de mayo de 2025. https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

En este mismo sentido, de acuerdo con la *Primera encuesta sobre seguridad digital en Colombia*, realizada por la Escuela de Ingeniería, Ciencia y Tecnología (EICT) de la Universidad del Rosario[66], los colombianos no dimensionan adecuadamente los riesgos que hay a nivel de seguridad digital. Mientras que los encuestados estiman que, en promedio, el 45% de las personas ha sido víctima de algún delito cibernético, la realidad es que el 78% afirmó haber experimentado al menos un incidente relacionado con seguridad digital. Este contraste pone de manifiesto un desbalance entre la percepción del riesgo y la experiencia real, lo que puede interpretarse como un sesgo cognitivo frente a la prevalencia de estos delitos, así como del nivel de exposición individual, lo cual incrementa la vulnerabilidad frente a prácticas de fraude cibernético.

Así mismo, la encuesta indagó si los usuarios sabrían cómo actuar en caso de ser víctimas de distintos incidentes de seguridad digital o pérdida de identidad. En todos los escenarios analizados, la mayoría de las personas encuestadas indicó no saber qué hacer (ver Ilustración 19), lo que revela un alto nivel de desconocimiento generalizado frente a la gestión de incidentes cibernéticos. Los resultados evidencian un bajo nivel de alfabetización digital en temas de seguridad y privacidad, lo que deja a los usuarios en un escenario de alta vulnerabilidad frente a fraudes como el *smishing*, el *vishing* o el *spoofing*.

Ilustración 19. ¿Sabría qué hacer para recuperar el control en caso de…?



Fuente: Universidad del Rosario (EICT). Primera encuesta sobre seguridad digital en Colombia.

En todo caso, se indica que este desconocimiento no puede ser óbice para reconocer que los usuarios de servicios de telecomunicaciones tienen la responsabilidad de mantenerse informados y actualizados respecto, tanto de los cambios normativos que buscan aumentar la protección y garantía de sus derechos, como de las medidas de seguridad digital básicas que pueden aplicar como mecanismos de auto control.

[66] Universidad del Rosario. Escuela de Ingeniería, Ciencia y Tecnología. Primera encuesta sobre seguridad digital en Colombia. Consultado el 29 de mayo de 2025. [En línea] Disponible en: Seguridad digital en Colombia: reflexiones y desafíos para proteger el futuro digital del país

No obstante, el desconocimiento de los usuarios sobre los mecanismos de protección que pueden implementar aumenta la criticidad del problema identificado, en tanto que el Estado no está brindando una protección adicional a aquellos usuarios de los servicios de telecomunicaciones que no tienen acceso a la normativa vigente o a información sobre condiciones de seguridad digital mínimas que pueden implementar de manera autónoma.

4.2.1.4. Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

Con la expedición del CONPES 3995 de 2020[67], por primera vez en Colombia se estableció una estrategia de múltiples partes interesadas con el objetivo de ampliar la confianza digital y mejorar la seguridad digital de manera que incremente la competitividad del país en el futuro digital. Además de reconocer la necesidad de fortalecer las capacidades en seguridad digital de todos los grupos de interés, se estableció como uno de los objetivos específicos la adopción de modelos, estándares y marcos de trabajo sobre seguridad digital, que incluya la seguridad y la privacidad de la información, impulsando así la implementación de controles físicos, lógicos y administrativos que protejan trámites, servicios, plataformas, sistemas de información e infraestructura institucional, tanto a nivel nacional como territorial.

Recientemente, la Presidencia de la República formuló la Estrategia Nacional de Seguridad Digital 2025–2027[68], concebida como una política integral para la protección del ecosistema digital nacional. Esta estrategia tiene como objetivo consolidar un entorno cibernético seguro, resiliente y confiable, que promueva el desarrollo económico, la inclusión social y la innovación tecnológica. Asimismo, busca robustecer las capacidades institucionales para la protección de infraestructuras críticas y servicios esenciales, garantizando la confidencialidad, integridad, disponibilidad y seguridad de la información de los ciudadanos, las empresas y las entidades públicas.

Esta estrategia adopta un enfoque basado en los derechos humanos, priorizando la protección de la privacidad, la libertad de expresión y la no discriminación, en concordancia con los lineamientos definidos en el Plan Nacional de Desarrollo 2022–2026 *Colombia, Potencia Mundial de la Vida.* Este enfoque refuerza el compromiso del Estado con la garantía de los derechos fundamentales en el entorno digital, alineándose con las directrices de los Documentos CONPES 3701 de 2011, 3854 de 2016 y el mencionado 3995 de 2020, así como la Estrategia Nacional Digital 2023–2026 y diversas políticas sectoriales como la Política de Gobierno Digital, la Política de Seguridad, Defensa y Convivencia Ciudadana, y el Plan Estratégico de Tecnologías de la Información y las Comunicaciones del sector defensa 2023–2026.

En la construcción de esta estrategia se identificaron cuatro ejes críticos: (i) la debilidad institucional y la limitada coordinación intersectorial; (ii) la creciente exposición a amenazas cibernéticas avanzadas y limitada capacidad para su identificación y mitigación; (iii) la escasez de talento humano especializado

[67] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL – DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital. 1 de julio de 2020. [en línea] Consultado e: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf

[68] PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Estrategia Nacional de Seguridad Digital de Colombia 2025-2027. Marzo de 2025. [en línea]. Consultado en: https://dapre.presidencia.gov.co/AtencionCiudadana/DocumentosConsulta/16052025-Estrategia-nacional-seguridad-digital_VF.pdf

en seguridad digital; y (iv) la necesidad de actualizar continuamente el marco normativo en materia de ciberseguridad frente a los riesgos emergentes.

Bajo este contexto, el MinTIC expidió recientemente nuevos lineamientos mediante el Modelo de Seguridad y Privacidad de la Información (MSPI). De acuerdo con su documento maestro, el objetivo principal de este modelo es fortalecer la implementación y mejora continua de controles de seguridad de la información en las Entidades del Estado y, a su vez, dar lineamientos sobre la implementación de seguridad digital que involucra la formalización de Sistema de Gestión de Seguridad y privacidad de la Información – SGSPI y seguridad digital.

Ahora bien, resulta importante indicar que además de estas políticas, a diversas entidades del Estado se les ha otorgado responsabilidades específicas que pueden aportar o no al desarrollo de la Estrategia Nacional de Seguridad Digital. En materia penal, se encuentra la Fiscalía General de la Nación, cuya responsabilidad mayor es el ejercicio de la acción penal y la realización de actividades de investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio.

Desde la perspectiva penal, en primer lugar, se encuentra la Fiscalía General de la Nación, cuya responsabilidad mayor es el ejercicio de la acción penal y la realización de actividades de investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querella o de oficio.

En complemento, la Dirección de Investigación Criminal e Interpol (DIJIN) de la Policía Nacional, tiene a su cargo el apoyo a la administración de justicia en el esclarecimiento de conductas punibles, para lo cual desarrolla las actividades de investigación judicial, criminalística, criminológica y la administración de la información criminal que permitan contribuir, a su vez, a demostrar la comisión del delito y la dirección de la investigación judicial en la Policía Nacional[69].

Adicionalmente, se encuentra el Ministerio de Justicia y del Derecho, como cabeza del sector administrativo, el cual fue definido como la autoridad encargada de adoptar, coordinar y ejecutar la política pública en materia de, entre otras cosas, lucha contra la criminalidad y la prevención y control del delito[70]. En esta misma línea, mediante el Decreto 851 de 2024, se le asignaron junto al Instituto Nacional Penitenciario y Carcelario (INPEC) competencias para coordinar con los Proveedores de Redes y Servicios de Telecomunicaciones Móviles (PRSTM) el bloqueo de equipos terminales móviles (ETM) dentro de los Establecimientos de Reclusión del Orden Nacional (ERON)[71], a fin de restringir comunicaciones no autorizadas. Esta labor se complementa con el uso de bases de datos que identifican dispositivos involucrados y, en caso necesario, permiten ejecutar acciones de control físico al interior del ERON[72].

[69] Decreto 113 de 2022. Artículo 11.
[70] PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1427 de 2017.
[71] Decreto 851 de 2024. Artículo 2.2.1.1.10.
[72] Ibid. Artículo 2.2.1.1.11.

En el mismo sentido, a los Grupos de Acción Unificada por la Libertad Personal (Gaula)[73], se les estableció el deber de remitir mensualmente a los PRSTM las bases de datos con denuncias asociadas a la comisión de delitos utilizando una línea telefónica para identificar comunicaciones no autorizadas en ERON[74].

Por su parte, desde un enfoque de apoyo y asesoría en la gestión de riesgos e incidentes de seguridad digital, mediante el Decreto 338 de 2022[75], se creó el Equipo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT) coordinado por el MinTIC, con el objetivo principal de asesorar, apoyar y coordinar a las múltiples partes interesadas para la adecuada gestión de los riesgos e incidentes digitales. Adicionalmente, este grupo es el punto único de contacto y respuesta nacional para responder de forma rápida y eficiente a los incidentes de seguridad digital y a gestionar de forma activa sus amenazas[76].

Desde el enfoque de protección al usuario, lo que involucra sus derechos como consumidor[77] y la garantía constitucional del tratamiento legítimo de sus datos personales[78], como ya se mencionó, la SIC se reviste como la autoridad de Inspección, Vigilancia y Control. De esta manera, dentro de sus facultades, el legislador definió que es un garante de la regulación en materia de protección de los derechos de los usuarios de servicios de comunicaciones, que expida la CRC, y del tratamiento adecuado de los diferentes tipos de datos personales, establecidos en la Ley.

Finalmente, la CRC, como autoridad regulatoria convergente del sector de las Tecnologías de la Información y las Comunicaciones (TIC), se encuentra facultada para, por un lado, expedir el régimen regulatorio para la maximización del bienestar social de los usuarios; y por el otro, como ya se indicó, regular y administrar todos los recursos de identificación en Colombia, con excepción del nombre de dominio -.co- y el espectro electromagnético.

De esta manera, pese a los esfuerzos adelantados por distintas instituciones involucradas y la definición de políticas públicas transversales que pretenden abordar los desafíos del cibercrimen y la ciberseguridad, aún persisten retos que requieren una estrategia nacional efectiva, coordinada y transversal. Es indispensable fortalecer la colaboración entre autoridades públicas, sector privado, sociedad civil y operadores de telecomunicaciones, a fin de generar respuestas integrales frente a fenómenos como el fraude digital y la ingeniería social, cuyas técnicas evolucionan de manera acelerada y requieren soluciones dinámicas, conjuntas y técnicamente sólidas.

4.2.2. Consecuencias del problema

4.2.2.1. Aumento de los casos de uso indebido de códigos cortos con fines fraudulentos

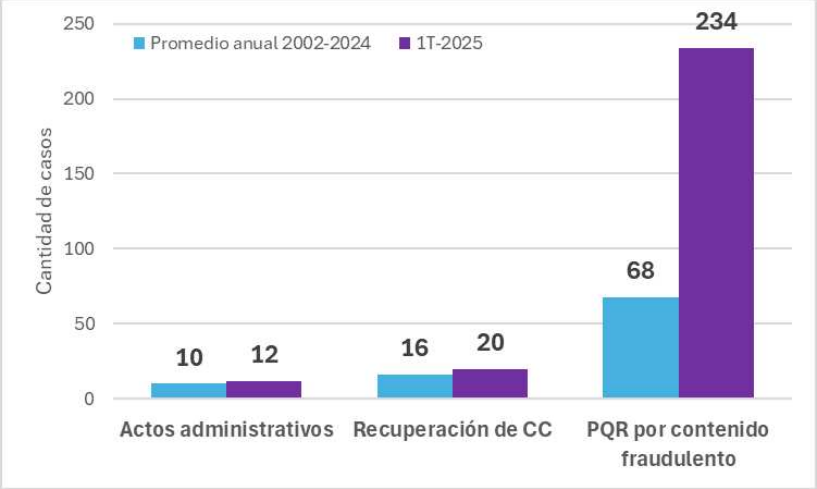
[73] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 282 de 1996.
[74] Op Cit. Decreto 851 de 2024. Artículo 2.2.1.1.13.
[75] «Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones».
[76] MINTIC. Decreto 338 de 2022. Artículo 2.2.21.1.5.2.
[77] CONGRESO DE LA REPÚBLICA. Ley 1480 de 2011. Artículo 59.
[78] CONGRESO DE LA REPÚBLICA. Ley 1581 de 2012. Artículo 19.

De acuerdo con el marco competencial en materia de recursos de identificación, la recuperación es una de las funciones que ejerce la CRC en su calidad de administrador, cuyo propósito es garantizar el uso eficiente de dichos recursos, prevenir su uso indebido y proteger los derechos de los usuarios de servicios de telecomunicaciones. En este marco, la recuperación se entiende como la decisión plasmada en un acto administrativo mediante el cual se revoca la autorización de uso previamente otorgada a un asignatario, cambiando el estado del recurso para su eventual reasignación a otro solicitante.

En el contexto de los servicios de envío de SMS o de servicios USSD, de conformidad con el artículo 6.1.1.8 de la Resolución CRC 5050 de 2016, esta entidad puede adelantar el procedimiento de recuperación de numeración de códigos cortos cuando se detecte la presunta configuración de alguna de las causales de recuperación establecidas en el artículo 6.4.3.2 o el presunto uso ineficiente de este recurso de identificación. Esta facultad, que responde tanto a criterios de legalidad como de eficiencia administrativa, se formaliza mediante la emisión de un acto administrativo que deja constancia de la causal de recuperación en la que se incurrió y habilita al administrador para modificar el estado del recurso indicando que se encuentra disponible[79].

Una de las causales de recuperación de numeración de códigos cortos establecida en la regulación se materializa al otorgarle un uso diferente al indicado en la solicitud de asignación del recurso. Precisamente la detección de la configuración de esta causal, también conocida como «uso indebido del código corto» ha presentado un incremento significativo en los casos el primer trimestre de 2025.

Ilustración 20. Comparativo de casos de uso diferente al indicado en el momento de la asignación de la numeración de códigos cortos.



Fuente: Elaboración propia.

Como se muestra en la Ilustración 20, mientras que entre 2022 y 2024 se registraron, en promedio anual, 16 recuperaciones de códigos cortos, 10 actos administrativos y 68 peticiones, quejas o reclamos

[79] Resolución CRC 5050 de 2016. «**ARTÍCULO 6.1.1.3. ESTADOS DE LOS RECURSOS DE IDENTIFICACIÓN.**
[…]
6.1.1.3.3. Recurso de identificación disponible: Corresponde al recurso de identificación atribuido al que puede acceder el solicitante.
[…]».

(PQR) por contenido fraudulento, es decir, por uso indebido del recurso; tan solo en los primeros tres meses de 2025 ya se reportan 20 recuperaciones, 12 actos administrativos expedidos, y un total de 234 PQR relacionadas con contenido fraudulento enviado por medio de SMS. Este aumento sugiere no solo una intensificación del uso irregular de estos recursos de identificación, sino también una mayor disposición de los usuarios para reportar este tipo de incidentes.

Este aumento significativo sugiere, además, la creciente prevalencia de prácticas indebidas como el *smishing* y la suplantación de identidad mediante numeración de códigos cortos, lo que a su vez pone en evidencia la necesidad de implementar medidas que prevengan el contacto a usuarios con fines de fraude, particularmente aquellas que se materializan por medio del uso indebido de servicios móviles como los mensajes SMS y las llamadas de voz.

4.2.2.2. Trasgresión de los derechos de los usuarios de los servicios de telecomunicaciones

Además de los bienes jurídicamente tutelados por la legislación colombiana, relacionados directamente con la prestación de los servicios de telecomunicaciones son los «datos personales» y «la integridad, confidencialidad y disponibilidad de la información», tanto pública como privada, mediante la Ley 1341 de 2009, el legislador definió un régimen mínimo y general de protección a los usuarios de servicios de telecomunicaciones.

En relación con la problemática identificada de contactabilidad con fines fraudulentos, se pueden identificar la posible vulneración delos siguientes derechos esenciales para una prestación de los servicios concordantes con la Constitución y la ley: (i) recibir protección en cuanto a su información personal, y que le sea garantizada la inviolabilidad y el secreto de las comunicaciones y protección contra la publicidad indebida, en el marco de la Constitución Política y la ley[80]; y (ii) protección contra conductas restrictivas o abusivas[81].

Bajo este contexto normativo, la CRC ha realizado esfuerzos importantes en la definición de derechos adicionales y de medidas para que garanticen su protección y su ejercicio en todo momento. Lo anterior, con el objetivo de materializar la maximización del bienestar social[82] y, específicamente, la protección de los derechos de los usuarios como uno de los principios orientadores de intervención del Estado en el sector TIC[83].

Uno de los principales derechos definidos por la CRC en el régimen de protección de los usuarios de los servicios de comunicaciones es «[r]ecibir protección de la información que cursa a través de la red del operador, quien debe garantizar la inviolabilidad de las comunicaciones»[84], el cual desarrolla la garantía constitucional de la intimidad personal y familiar y la prerrogativa legal dispuesta en el numeral 9 del artículo 53 de la Ley 1341 de 2009.

Este derecho establecido en el marco regulatorio se divide en dos partes, a saber, por un lado, para los PRST implica el cumplimiento del deber de solicitar el consentimiento previo, expreso e informado a los

[80] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 de 2009, modificada por la Ley 1978 de 2019. Artículo 53, numeral 9.
[81] Ibid. Artículo 53, numeral 10.
[82] Ibid. Artículo 4, numeral 1.
[83] Ibid. Artículo 2, numeral 4.
[84] Resolución CRC 5050 de 2016. Artículo 2.1.2.1, numeral 2.1.2.1.6.

usuarios y adoptar las medidas correspondientes para evitar accesos no autorizados a su información; y, por el otro, suscita la obligación de conservar la naturaleza privada de todas las interacciones y datos transmitidos mediante redes de telecomunicaciones, siendo concordante con la proscripción de la interceptación de las comunicaciones en Colombia, permitidas únicamente con la respectiva orden judicial y el cumplimiento de los demás requisitos legales[85].

Estas garantías constitucionales y legales, que son prerrogativas de los usuarios de dichos servicios, se pueden ver comprometidas al momento de involucrarse en el flujo de la comunicación, esto es, al utilizar cualquiera de los servicios tradicionales de voz o de SMS, más aún si se trata contacto para la presunta comisión de fraude.

Por consiguiente, como se indicó en la causa descrita en la subsección 4.2.1.2 y en la consecuencia 4.2.2.1, la ausencia de condiciones regulatorias específicas que prevengan el contacto a usuarios con fines fraudulentos posibilita la implementación de herramientas preventivas disímiles por parte de los agentes que hacen parte de la cadena de valor del flujo de la comunicación mediante llamadas de voz y SMS, por cuanto no se garantiza el mismo nivel de efectividad; lo que, a su vez, ha generado un aumento en los casos denunciados por los usuarios sobre este tipo de contacto; y, en últimas, profundiza el riesgo latente de la trasgresión de dichos derechos de los usuarios.

4.2.2.3. Afectaciones a empresas y organismos públicos

Resulta importante señalar que, si bien los usuarios y ciudadanos son los directamente afectados por incidentes de seguridad digital, no son los únicos, pues tanto las empresas como los organismos públicos a nivel mundial han sido víctimas de diversos tipos de ataques cibernéticos. Como ya se mencionó, en la legislación colombiana ya se contemplan conductas que desde la perspectiva penal y administrativa pueden generar sanciones por atentar contra la privacidad de la información y los datos personales, tanto de particulares como de entidades, como es el caso de la Ley 1273 de 2009, que introdujo el concepto de «delitos informáticos», y la Ley 1581 de 2012, que implementa el régimen general de protección de datos personales.

Ahora bien, a pesar de que la ley delega responsabilidades claras sobre el tratamiento de la información y busca prevenir y sancionar conductas asociadas al acceso indebido, uso no autorizado o filtración de datos personales, lo cierto es que este tipo de sanciones no han sido suficientes para persuadir a los delincuentes. De acuerdo con el *Informe Tendencias del Cibercrimen Primer Trimestre 2020*, elaborado por el Tanque de Análisis y Creatividad de las Tic (TicTac), en conjunto con la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y la Policía Nacional, en desarrollo de su programa de Seguridad Aplicada al Fortalecimiento Empresarial (SAFE), para el 2020, las entidades gubernamentales de Colombia con más casos reportados de suplantación fueron: la DIAN (57%), la Fiscalía General de

[85] CONSTITUCIÓN POLÍTICA DE COLOMBIA. «ARTÍCULO 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar.
[…]
La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley. […]».

la Nación (12%), Organismos de Transito (10%), la Policía Nacional (9%), y el Ministerio de Salud y Protección Social (7%)[86].

En ese momento coyuntural a nivel mundial ocasionado por la pandemia del Covid-19, en el país se presentó un incremento del 37% de ciberataques, siendo uno de los servicios y trámites del gobierno electrónico los más afectados, dado que fueron utilizados por organizaciones criminales para propagar *malware* (*software* malicioso)[87].

Por su parte, según Asobancaria, cerca de 50 entidades financieras se vieron afectadas por ciberataques durante 2023[88]; y, de acuerdo con los Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CI) de la Superintendencia Financiera de Colombia, para el 2024, se presentaron 36.000 millones de ataques cibernéticos, lo que representa un incremento del 29% con respecto al 2023[89]. Lo anterior, quiere decir que, durante 2024, los establecimientos bancarios pertenecientes al sistema financiero del país recibieron más de 98,6 millones de ataques cibernéticos a diario, cerca de 4,11 millones cada hora y aproximadamente de 68.500 por minuto[90].

Vale la pena indicar que, según la Superintendencia Financiera de Colombia en el primer semestre del 2024 las entidades financieras recibieron más de 242.000 quejas por fraude, siendo las modalidades de fraude más reportadas la ingeniera social -*phishing*, *vishing*, *smishing*, ataque CEO, y cambiazo- con el (27%) y la suplantación de identidad -uso no consentido de la información, *SIM swapping*, fraude amigo, pérdida de elementos y falsificación de documentos- con el (18%)[91].

La reincidencia en este tipo de ataques ha exigido a los establecimientos bancarios la implementación de una serie de herramientas de prevención y la definición de diferentes estrategias de seguridad digital, con el fin de proteger a sus consumidores. De acuerdo con los indicadores de seguridad SI y CI ya mencionados, para el año 2024, estas empresas invirtieron 510.000 millones de pesos en seguridad de la información y ciberseguridad -cifra que comparada con la del 2023 refleja un incremento del 16 por ciento-.

Ahora bien, las afectaciones a empresas y entidades públicas no solo se evidencian desde una perspectiva económica, sino también reputacional, teniendo en cuenta el impacto en su huella digital por ataques de ingeniería social. Este impacto en su reputación ha generado, además, desconfianza en el sistema financiero, llevando a algunos usuarios a optar por métodos de ahorro tradicionales, a pesar,

---

[86] TIC TAC, CCIT, POLICÍA NACIONAL. *Informe Tendencias del Cibercrimen Primer Trimestre 2020*. [En línea]. Publicado el 21 de abril de 2020. Consultado en: https://www.ccit.org.co/noticias/aumento-37-la-ciberdelincuencia-en-colombia-relacionada-con-el-covid-19/

[87] Ibid.

[88] BANCA & ECONOMÍA. *Discurso de Instalación 16° Congreso de Prevención de Fraude y Ciberseguridad.* Edición 1400 del 30 de octubre de 2023. [En línea]. Consultado en: https://www.asobancaria.com/wp-content/uploads/2023/10/1400-BE-3.pdf

[89] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CI). [en línea]. Consultado en: https://www.superfinanciera.gov.co/publicaciones/10115571/indicadores-de-seguridad-de-la-informacion-y-ciberseguridad-2024/

[90] EL TIEMPO. *Le contamos cuánto invirtieron los bancos en 2024 para proteger datos y recursos de sus clientes de ciberataques*. Columna escrita por Carlos Arturo García Mahecha. Fecha: 26 de marzo de 2025. [en línea]. Consultado en: https://www.eltiempo.com/economia/sector-financiero/le-contamos-cuanto-invirtieron-las-entidades-financieras-para-proteger-los-datos-y-recursos-de-sus-clientes-en-2024-3438724

[91] SUPERINTENDENCIA FINANCIERA DE COLOMBIA. *Retos importantes en seguridad y disponibilidad en el sector financiero*. [en línea]. Consultado en: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1072807

incluso, de que no se generen rendimientos; toda vez que sí otorga sensación de seguridad y control de su dinero[92].

De esta manera, que no existan herramientas regulatorias específicamente encaminadas a contactar usuarios con la finalidad de cometer fraude, genera graves afectaciones, en diferentes frentes no solo económicas, y de manera transversal, es decir, no son impactos exclusivos de la industria de telecomunicaciones, sino que también se generan a los agentes de los demás sectores de la economía e incluso a las entidades públicas.

4.2.2.4. Pérdida de confianza en los servicios de telecomunicaciones

De acuerdo con su definición, telecomunicación es toda emisión, transmisión y recepción de información por hilo, radiofrecuencia y, en fin, cualquier sistema electromagnético[93]; es decir, los servicios de telecomunicaciones como la telefonía fija y móvil, el acceso a internet y la mensajería de texto (SMS), son los que, en esencia, permiten a los usuarios enviar y recibir información, cualquiera sea su naturaleza.

Bajo este contexto, si bien los recursos de identificación de numeración de códigos cortos y E.164 se consideran un canal de comunicación e interacción entre personas (P2P) y entre usuarios y plataformas o empresas (A2P y B2P), lo cierto es que ante el reciente incremento de denuncias reportadas ante las diferentes autoridades competentes y la detección de contenido posiblemente fraudulento, se configure o no la comisión de delitos penales, es un fenómeno que está generando, más allá de daños al patrimonio, afectaciones psicológicas a sus víctimas.

De acuerdo con la edición 1256 de Banca & Economía de Asobancaria, en 2020, la Universidad de Portsmouth y algunas entidades gubernamentales de Reino Unido, realizaron un estudio mediante entrevistas a víctimas de hackeos o robos de información a través de medios informáticos con el objetivo de conocer los posibles impactos que generan los ataques cibernéticos en las personas[94].

Una de las principales conclusiones a las que se llegó a partir de los testimonios recolectados es que la comisión de «[…] delitos informáticos tienen un impacto en las personas [víctimas] similar, e incluso en algunas ocasiones, peor que delitos físicos como el robo», debido a que causan impactos directos en la salud, por altos niveles de estrés y ansiedad, así como psicológicos y emocionales como dificultad para dormir, depresión, autolesiones, pensamientos suicidas, aislamiento, etc.[95].

Este tipo de efectos psicológicos y en la salud de las personas víctimas de delitos cibernéticos genera una percepción de vulnerabilidad, lo que se traduce en desconfianza en el uso de los servicios de telecomunicaciones que permiten el contacto a los usuarios finales, ya sea mediante llamadas de voz o SMS e incluso en abandono de canales digitales para sus trámites y servicios. Por lo anterior, la ausencia

---

[92] Le contamos cuánto invirtieron los bancos en 2024 para proteger datos y recursos de sus clientes de ciberataques https://www.eltiempo.com/economia/sector-financiero/le-contamos-cuanto-invirtieron-las-entidades-financieras-para-proteger-los-datos-y-recursos-de-sus-clientes-en-2024-3438724

[93] Resolución MinTIC 202 de 2010, modificada por la Resolución 1272 de 2020. Artículo 1.

[94] Impacto económico y social del phishing y el smishing en Colombia y el Mundo https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

[95] BANCA & ECONOMÍA. *Impacto económico y social del phishing y el smishing en Colombia y el mundo*. Edición 1256 del 26 de octubre de 2020. [En línea]. Consultado en: https://www.port.ac.uk/news-events-and-blogs/news/new-home-office-funded-report-urges-greater-action-for-cybercrime-victims

de regulación que prevenga este tipo de contacto a usuarios, como ya se indicó, al generar el escenario perfecto para que se continúen desarrollando técnicas de ingeniería social que utilizan directamente la infraestructura de telecomunicaciones podría suscitar, incluso, una eventual disminución en la apropiación de las TIC en el país.

5. PLAN DE GESTIÓN DEL PROYECTO

5.1. Objetivos del proyecto

5.2.1. Objetivo general

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.

5.2.2. Objetivos específicos

a) Identificar aspectos del régimen de recursos de identificación que sean susceptibles de adecuación desde una perspectiva de prevención del contacto a usuarios con fines fraudulentos.
b) Evaluar la implementación de herramientas regulatorias que mitiguen el contacto a usuarios con fines fraudulentos, teniendo en cuenta su viabilidad técnica y económica.
c) Determinar la necesidad de implementar acciones educativas que aumenten el conocimiento de los usuarios en la prevención contra el fraude cibernético.
d) Definir líneas de acción de la CRC y recomendaciones a otras autoridades para la construcción conjunta de una estrategia nacional de prevención en el contacto a usuarios con fines fraudulentos.

5.2. Grupos de valor asociados al proyecto

De acuerdo con lo expuesto en relación con el alcance y objetivos del presente proyecto, el problema identificado impacta a los grupos de valor de la CRC definidos en la Tabla 5:

Tabla 5. Impacto e interés de los grupos de valor del proyecto regulatorio

No.	Grupo de valor identificado	Descripción	Interés en el proyecto	Impacto del proyecto
1	Proveedores de Redes y Servicios de Telecomunicaciones	Persona jurídica, debidamente habilitada, que ofrece a distintos agentes las redes y servicios tradiciones de voz y envío de mensajes cortos de texto.	Alto. El fraude mediante servicios de voz y envío de SMS afecta la confianza de los usuarios y la demanda de los servicios finales que ofrecen. Adicionalmente, al verse afectados por la problemática, en diferentes escenarios de participación han advertido su interés especial en que la regulación implemente medidas de seguridad más rigurosas.	Alto. En caso de que la CRC encuentre necesario expedir regulación, es posible que sobre estos agentes recaigan obligaciones, algunas de las cuales podría requerir implementación técnica de herramientas y control preventivo del fraude.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No.	Grupo de valor identificado	Descripción	Interés en el proyecto	Impacto del proyecto
2	Proveedores de Contenidos y Aplicaciones e Integradores Tecnológicos	Persona jurídica, debidamente registrada en el RPCAI, que ofrece distintos servicios de envío de mensajes cortos de texto.	Alto. El fraude mediante servicios de envío de SMS impacta en la confianza de los usuarios y en la demanda de los servicios mayoristas que ofrecen estos agentes. Al ser los autorizados por la CRC para utilizar el código corto, son los responsables de los diferentes usos, legítimos o no, que se otorgue al recurso.	Alto. En caso de que la CRC encuentre necesario expedir regulación, es posible que sobre estos agentes recaigan obligaciones, algunas de las cuales podría requerir implementación técnica de herramientas y control preventivo del fraude.
3	Entidades Gremiales	ANDESCO, ASOMÓVIL	Medio. Agrupan los intereses de sus agremiados, por lo que buscan propiciar cambios regulatorios que resulten convenientes para ellos. Así, los cambios regulatorios asociados a la mitigación del fraude, al fomentar la confianza de los usuarios y la competitividad de sus agremiados, son de igual interés para sus agremiaciones.	Medio. A pesar de que son interlocutores ante la CRC, y no destinatarios directos de las obligaciones regulatorias que pudieran ser modificadas, sus recomendaciones podrían ayudar en fortalecer la seguridad y confianza en la operación de todos sus agremiados.
4	Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC	Institución gubernamental encargada del diseño, formulación, adopción y promoción de la política general del sector de telecomunicaciones y postal; y facultada como Autoridad de Inspección, Control y Vigilancia de la regulación vigente para estos sectores.	Alto. MINTIC como entidad gubernamental de Inspección, Vigilancia y Control, verifica el cumplimiento de las normas vigentes en materia de calidad y seguridad de los servicios que regula CRC.	Alto. En caso de que se introduzcan cambios en la regulación, se impactarán sus funciones de inspección, vigilancia y control.
5	Superintendencia de Industria y Comercio – SIC	Entidad gubernamental que vela por el buen funcionamiento de los mercados por medio de la protección y vigilancia de la libre competencia económica, de los derechos de los consumidores en los sectores de telecomunicaciones y postal y de protección de datos personales.	Alto. Al ser la autoridad que vigila y controla, por un lado, los derechos de los consumidores, y por el otro, los datos personales, es la receptora de peticiones, quejas, reclamos y denuncias por afectación en la seguridad de estos servicios.	Alto. En caso de que se introduzcan cambios en la regulación orientada a la protección de los derechos de los usuarios de servicios de telecomunicaciones, se impactará el ejercicio de sus funciones de inspección, vigilancia y control.
6	Usuarios de servicios tradicionales de voz y envío de mensajes de texto	Persona natural o jurídica consumidora de los servicios tradicionales de voz y envío de mensajes de texto.	Alto. En la medida en que los usuarios finales de estos servicios han sido los directamente afectados al ser contactados con fines fraudulentos e, incluso por la comisión de delitos informáticos, son los principales interesados en el desarrollo de la presente iniciativa.	Alto. Son los beneficiarios directos del establecimiento de medidas para prevenir el fraude mediante servicios tradicionales de voz y mensajes de texto.
7	Agremiaciones de consumidores y sociedad civil	ONG y organizaciones privadas que trabajan para el adecuado desarrollo de políticas públicas y regulatorias para los ciudadanos.	Alto. En la medida en que los usuarios finales de los servicios tradicionales de voz y envío de mensajes de texto han sido los directamente afectados, las iniciativas que busquen promover la seguridad de los servicios para los consumidores beneficia a sus asociados.	Alto. En caso de que se introduzcan cambios en la regulación para prevenir el fraude, se impactará positivamente a las personas naturales y jurídicas que representan y cuyos intereses defienden.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

No.	Grupo de valor identificado	Descripción	Interés en el proyecto	Impacto del proyecto
8	OCDE, OMC, UIT	Entidades multilaterales conformadas por tres o más naciones que trabajan de forma conjunta en problemáticas y aspectos que involucran las TIC como parte fundamental del desarrollo económico, y el cumplimiento de los acuerdos comerciales.	Bajo. Las medidas que adopte la CRC para mitigar y prevenir el fraude, ponen de manifiesto el compromiso de Colombia por combatir este flagelo que es de escala mundial.	Bajo. Entidades como la UIT, el Banco Mundial y la OCDE podrán medir mediante los análisis comparativos entre países, la contribución que tenga el país en la prevención del fraude mediante llamadas de voz y mensajes de texto.
9	Entidades del sector financiero	Entidades bancarias que ofrecen servicios financieros y entidades gubernamentales encargadas de velar por la correcta prestación de los servicios financieros.	Alto. En los casos en que se lleve a cabo de manera exitosa un fraude, es decir, que se genere daño al patrimonio de un ciudadano, estos acuden directamente a las entidades financieras para reclamar sus derechos y definir responsabilidades.	Alto. En caso de que se introduzcan cambios en la regulación para prevenir el fraude, se beneficiará directamente la operación de las entidades financieras y a sus usuarios.

6. EXPERIENCIAS INTERNACIONALES

En el marco del presente proyecto regulatorio se efectuó una investigación minuciosa de las experiencias internacionales que consistió en conocer la problemática que fue identificada por las autoridades de regulación del sector TIC en otros países, relacionada con el fraude cibernético utilizando servicios de telecomunicaciones, e identificar las medidas que implementaron con el fin de solucionarlo.

En términos generales, la experiencia internacional sugiere que las estrategias implementadas para combatir el fraude requieren de la acción y coordinación conjunta entre diferentes actores, tanto gubernamentales como no gubernamentales, así como de la ciudadanía en general. Estas estrategias buscan reducir la incidencia de los ciberdelitos en cada uno de los países revisados.

Particularmente los organismos que regulan el sector de las TIC, tanto de manera autónoma como en coordinación con entidades que regulan otros sectores, han adoptado medidas orientadas a combatir este flagelo mediante la expedición de normativas que contienen directrices tanto para los PRST como para los proveedores de contenidos y aplicaciones.

Puntualmente, se revisaron y analizaron las experiencias de catorce (14) países en el mundo, a saber:

1. Australia
2. Brasil
3. Canadá
4. Chile
5. España
6. Estados Unidos
7. India
8. Irlanda
9. Jordania
10. Malasia
11. Polonia
12. Portugal
13. Singapur
14. Reino Unido

A partir de este análisis se pudo concluir que las problemáticas identificadas por las autoridades regulatorias del sector TIC y que buscaban solucionar por medio de la implementación de medidas, se pueden agrupar en tres grandes temáticas:

i. Evitar la suplantación de la identificación del número llamante de las comunicaciones de voz cursadas por medio de las redes de telefonía fija o móvil;
ii. Combatir el envío de mensajes cortos de texto por parte de estafadores; y,
iii. Ejercer control de contenidos.

Las estrategias implementadas para combatir la primera problemática se enfocan en validar que el número llamante no ha sido suplantado o enmascarado con otro número. Estas validaciones se realizan por medio de las siguientes tres metodologías:

1. **Verificación del CLI:** Consiste en revisar la información contenida en la funcionalidad del «Identificador de Línea Llamante» (Calling Line Identification o CLI) con el fin de bloquear llamadas que oculten el CLI, o cuyo CLI contenga números desde los cuales no se deben realizar llamadas (Do-Not-Originate list o DNO); o bloquear llamadas provenientes desde el extranjero que hacen uso de un números de origen del país de destino, con excepción de llamadas realizadas por usuarios que se encuentren en itinerancia.
2. **STIR/SHAKEN:** Radica en implementar el protocolo STIR/SHAKEN que permite verificar que el identificador de llamada transmitido coincide efectivamente con el número asignado al usuario llamante, usando técnicas de certificados digitales para verificar la identidad del proveedor de servicios que realiza la llamada.
3. **Cortafuegos (Firewall) de voz:** Consistente en implementar sistemas informáticos que permiten establecer patrones de llamadas fraudulentas a partir de herramientas de análisis de datos en tiempo real, aprendizaje automático e inteligencia artificial, con el fin de detectar y tomar medidas sobre patrones inusuales presentes en los datos de señalización de la llamada o sobre volúmenes inusuales de tráfico.

Por su parte, para obstaculizar el envío de SMS provenientes de estafadores, las autoridades reguladoras han implementado las siguientes medidas:

1. **Limitaciones de envío de SMS:** Restringe la cantidad de SMS que pueden ser enviados por un usuario dentro de un tiempo determinado.
2. **Verificación de Clientes:** Define las verificaciones que deben realizar los Agregadores de SMS sobre la identidad y los antecedentes de sus clientes.
3. **Registro de Identificación (ID) de Remitentes:** Las organizaciones legítimamente constituidas que deseen remitir SMS publicitarios o realizar algún tipo de notificación comercial a sus usuarios, deben registrarse y acceder a los identificadores alfanuméricos que utilizarán para su envío.
4. **Monitoreo de tráfico:** Despliegue e implementación de herramientas de monitoreo y análisis de tráfico que utilizan funcionalidades como escudos antispam y control de fraude para identificar y bloquear SMS sospechosos antes de su entrega a los consumidores.

Finalmente, para ejercer el control de contenidos, el regulador de Malasia implementó medidas consistentes en el trámite y la asignación de licencias a los proveedores de aplicaciones, por medio de las cuales se obligan a cumplir una serie de políticas y medidas orientadas a:

a) Controlar el acceso de contenidos a usuarios menores de edad.
b) Identificar y bloquear mensajes y contenidos maliciosos, tales como ciberacoso, estafa o captación de menores para fines sexuales.

c) Establecer políticas y medidas para la moderación de los contenidos.
d) Gestionar *deepfakes* y contenido malicioso generado por Inteligencia Artificial (IA).

En la Tabla 6 se presentan las principales medidas adoptadas por los países estudiados con el objetivo de combatir el fraude cibernético mediante el uso de servicios de telecomunicaciones:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 6. Principales medidas adoptadas para combatir el fraude cibernético mediante servicios de telecomunicaciones

País	Medidas contra la suplantación del ID del número llamante				Medidas de contra el envío de SMS Fraudulentos				Control de Contenidos
	DNO	Bloqueo a Llamadas Internacionales con Número Local	STIR/SHAKEN	Firewall de Voz	Limitación de envío de SMS	Verificación de Clientes	Registro de ID de Remitentes	Monitores de Tráfico	
Australia	Si	Si					Si	Si	
Brasil	Si		Si	Si					
Canadá			Si						
Chile	Si								
España[96]	SI	Si					Si	Si	
Estados Unidos			Si						
India[97]							Si		
Irlanda	Si	Si		Si		Si	Si		
Jordania[98]									
Malasia									Si
Polonia	Si	Si					Si	Si	
Portugal	Si	Si							
Singapur[99]							Si	Si	
Reino Unido	Si	Si[100]			Si	Si[101]	Si[102]	Si[103]	

[96] Además de las medidas señaladas en la tabla, en España se ordena la obligación de bloquear SMS enviados del exterior con números locales y prohíbe la utilización de numeración móvil para realizar llamada con propósito comercial.

[97] Además de la medida señalada en la tabla, en la India se ordena el bloqueo de SMS enviados desde el exterior con encabezados alfanuméricos o que tengan un código de país +91.

[98] Jordania reglamentó las condiciones para el envío de SMS de forma masiva.

[99] Además de las medidas señaladas en la tabla, Singapur expidió normativas donde las instituciones financieras o los operadores de servicios móviles respondieran por las pérdidas de sus usuarios, en los casos donde se comprobara el incumplimiento de alguna de las directrices definidas para combatir el fraude.

[100] Se hace excepción a las llamadas internacionales entrantes cuyo rango de numeración comience con el código +44.

[101] Esa exigencia es realizada voluntariamente por los operadores de redes móviles, incluyendo dentro de las cláusulas de los contratos que suscriben con los agregadores de SMS las validaciones mínimas que estos deben realizar a sus clientes.

[102] Las organizaciones legítimas remitentes de contenido realizan de manera voluntaria el registro de los ID alfanuméricos utilizados para el envío de mensajes de texto SMS.

[103] Los PRST móviles han implementado de manera voluntaria herramientas de monitoreo de tráfico para identificar y bloquear SMS fraudulentos.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

7. CONSULTA PÚBLICA

Teniendo en cuenta la metodología de AIN, con esta consulta la CRC se permite socializar con los agentes interesados los análisis realizados sobre la identificación y magnitud del problema, sus causas y consecuencias y los objetivos planteados en el marco del proyecto regulatorio denominado *Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles.* Así mismo, se busca conocer la perspectiva de cada uno de los grupos de valor respecto de la viabilidad de posibles alternativas de solución identificadas de manera preliminar por parte de esta Comisión, incluyendo sus facilidades y dificultades/costos en caso de que se defina su implementación.

Con el objetivo de orientar esta consulta, se solicita a los agentes interesados, a más tardar el **28 de julio de 2025**, contestar las siguientes preguntas mediante el formulario de Forms que se encuentra en el siguiente enlace https://forms.office.com/r/f0Qu3f3gHW o mediante el correo electrónico medidasantifraude@crcom.gov.co:

1. Sobre el problema planteado:

a) ¿Por qué considera que el problema definido en este documento involucra todos los elementos que evidencian las dificultades generadas por la comisión de fraude cibernético mediante la provisión de los servicios tradicionales de llamadas de voz y SMS? Dado el caso que considere que el problema definido no involucra todos los elementos necesarios, por favor justifique sus motivos, aporte evidencia al respecto y proponga un problema alternativo con sus respectivas causas y consecuencias.
b) Frente al problema planteado, ¿por qué considera que las causas presentadas en este documento son las que generan el problema definido? En caso de considerar lo contrario, por favor indicar las razones por las cuales no está de acuerdo con la relación que se establece entre tales causas y el problema definido, y proponga las causas que considere pertinentes.
c) Frente al problema planteado, ¿por qué considera que las consecuencias expuestas en el presente documento tienen relación directa con la materialización del problema? En caso de considerar lo contrario, indicar las razones por las cuales no está de acuerdo con la relación que se establece entre el problema definido y las consecuencias descritas, y proponga las consecuencias que considere pertinentes.

2. Respecto de los grupos de valor:

a) ¿Por qué considera que existen otros grupos de valor que deben tenerse en cuenta en el desarrollo del presente proyecto regulatorio? Por favor indíquelos, justificando la razón que tendría para incluirlos. En caso de considerar que se encuentran incluidos todos los grupos de valor, justifique también su respuesta.

3. Sobre posibles alternativas de solución a la problemática identificada:

a) <u>En relación con el uso indebido de la numeración de códigos cortos</u>:

a.1. ¿Cuáles beneficios o desafíos cree que podría tener la implementación de un registro de remitentes de mensajes cortos de texto, que haga uso de códigos alfanuméricos

para su identificación por parte de los usuarios, así como de la identificación de la campaña de comercialización o publicidad que se va a adelantar por parte del remitente?

a.2. ¿Cómo valora la creación de un registro de remitentes que utilice tanto numeración de códigos cortos como numeración no geográfica de servicios (Numeración E.164 del NDC 940), teniendo en cuenta la actualización de las categorías de atribución como requisito para su asignación? ¿Considera viable esta alternativa? ¿Qué pros y contras podría identificar?

a.3. ¿Qué efectos cree que tendría una medida regulatoria que prohíba la inclusión de enlaces o URL de cualquier tipo en el contenido de los mensajes cortos de texto? ¿Esta restricción podría mitigar riesgos de fraude? ¿Qué efectos tendría sobre el mercado de envío de SMS?

a.4. ¿Qué implicaciones considera que tendría la prohibición de la intermediación o reventa del uso de numeración de códigos cortos por parte de los asignatarios, estableciendo la identificación exclusiva de remitentes de mensajes de texto (SMS) a través de un único código corto atribuido a una modalidad y rango numérico exclusivo? Es decir, un código corto como canal dedicado de comunicación entre un originador de mensajes de texto y sus destinatarios, atribuido en la modalidad de servicios financieros. Ejemplo: código corto: 86000; modalidad: servicios financieros; uso: para uso exclusivo por parte de la entidad financiera: Banco X

¿Considera que la cantidad disponible de numeración de códigos cortos sería suficiente para atender la demanda de estos servicios, o sería necesario migrar a otro tipo de numeración con mayor disponibilidad de números?

a.5. ¿Qué beneficios o desafíos considera que podría tener la migración del uso de la numeración de códigos cortos a numeración E.164 no geográfica de servicios atribuida en el NDC 940 para acceder a contenidos y aplicaciones soportados en SMS y USSD, con reglas estrictas sobre exclusividad de uso y prohibición de compartición o tercerización del recurso?

a.6. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración de códigos cortos y el contacto a usuarios con fines presuntamente fraudulentos mediante el envío de mensajes cortos de texto.

b) <u>Respecto del uso inadecuado de la numeración E.164</u>:

b.1. ¿Qué beneficios y retos identifica en la implementación de un registro de originadores de llamadas comerciales y publicitarias, que permita su identificación por parte del usuario final mediante códigos alfanuméricos, y que se complemente con medidas como el uso exclusivo de rangos de numeración dedicadas, bloqueo de numeración no válida o extranjera sospechosa y el registro de campañas que se van a realizar por medio de llamadas de voz?

b.2. ¿Qué percepción tiene sobre la adopción de técnicas tecnológicas de filtrado (screening) para identificar y bloquear llamadas o mensajes sospechosos? ¿Considera que esta medida debe ser complementada con acciones regulatorias sobre el uso de numeración?

b.3. Por favor describa de manera detallada cualquier otra alternativa regulatoria que considere podría contribuir a prevenir el uso indebido de la numeración E.164 y el contacto usuarios con fines presuntamente fraudulentos mediante llamadas de voz.

c) <u>En relación con el desconocimiento de los usuarios sobre privacidad de la información técnicas de ingeniería social</u>:

c.1. ¿Cuál es su opinión sobre establecer obligaciones de divulgación pedagógica y de prevención en cabeza de los operadores móviles, PCA e integradores tecnológicos, complementadas con un portal de la CRC con información sobre remitentes denunciados?

c.2. ¿Qué efectos cree que tendría la creación de un portal que incluya una **lista negra** con los recursos de identificación más denunciados ante la CRC, e identificados de oficio por esta autoridad, que sean utilizados para contactar usuarios con fines presuntamente fraudulentos?

c.3. ¿Cómo valoraría la creación de un sistema intersectorial de trazabilidad de recursos de identificación, administrado por la CRC, que centralice las PQRD's presentadas por los usuarios y se complemente con campañas educativas conjuntas?

c.4. Por favor describa de manera detallada cualquier otra alternativa que considere útil para aumentar el conocimiento y empoderamiento de los usuarios frente a los riesgos del fraude cibernético por medio de servicios móviles.

d) <u>Sobre la revisión integral del Régimen de Recursos de Identificación</u>

d.1. ¿tiene alguna propuesta o recomendación para optimizar los procedimientos de asignación y recuperación de los recursos de identificación?

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

8. BIBLIOGRAFÍA

NORMATIVIDAD COLOMBIANA

COLOMBIA. Constitución Política de Colombia. Bogotá: Diario Oficial No. 47.091, 4 de julio de 1991. Artículo 15.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 84 de 1873. «Código Civil de los Estados Unidos de Colombia». Diario Oficial No. 2.867 de 31 de mayo de 1873. [En línea]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/codigo_civil.html#27

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 37 de 1993. «Por la cual se regula la prestación del servicio de telefonía móvil celular, la celebración de contratos de sociedad y de asociación en el ámbito de las telecomunicaciones y se dictan otras disposiciones». Diario Oficial 40.710 de enero 6 de 1993. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=290

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1266 de 2008. «Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.». Diario Oficial No. 47.219 de 31 de diciembre de 2008. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_1266_2008.htm

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009 «Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones». Diario Oficial No. 47.223 de 5 de enero de 2009. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_1273_2009.htm

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1341 de 2009. «Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.». Diario Oficial No. 47.426 de 30 de julio de 2009. [En línea] Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1480 de 2011. «Por medio de la cual se expide el Estatuto del Consumidor y se dictan otras disposiciones.» Diario Oficial No. 48.220 de 12 de octubre de 2011. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_1480_2011.htm

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1581 de 2012. «Por la cual se dictan disposiciones generales para la protección de datos personales.». Diario Oficial No. 48.587 de 18 de octubre de 2012. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_1581_2012.htm

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 2300 de 2023. «Por medio de la cual se establecen medidas que protejan el derecho a la intimidad de los consumidores». Diario Oficial No. 52.452 de 10 de julio de 2023. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_2300_2023.htm

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 282 de 1996. «Por la cual se dictan medidas tendientes a erradicar algunos delitos contra la libertad personal, especialmente el secuestro y la extorsión, y se expiden otras disposiciones». Diario Oficial No. 42.804 de 11 de junio de 1996. [En línea] Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/ley_0282_1996.htm

CORTE CONSTITUCIONAL. Sentencia T-073 de 2019. M.P. Carlos Bernal Pulido.

CORTE SUPREMA DE JUSTICIA, Sala Penal. Sentencia del 12 de diciembre de 2019, SP-53792019. Sentencia del 9 de agosto de 2017, SP-537922019, exp. 44071. Sentencia del 8 de marzo de 2017, SP-32332017, exp. 48279.

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 1078 de 2015. «Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones». Diario Oficial No. 49.523 de 26 de mayo de 2015. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/decreto_1078_2015.htm

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 1130 de 1999. «Por el cual se reestructuran el Ministerio de Comunicaciones y algunos organismos del sector administrativo de comunicaciones y se trasladan funciones a otras entidades públicas». Diario Oficial No 43.625, del 29 de junio. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/decreto_1130_1999.htm

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 25 de 2002. «Por la cual se adoptan los Planes Técnicos Básicos y se dictan otras disposiciones.» Diario Oficial No. 44.680, de 18 de enero de 2002. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/decreto_0025_2002.htm

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 338 de 2022. «Por el cual se adiciona el Título 21 a la Parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.» Diario Oficial No. 51.970 de 8 de marzo de 2022. [En línea] Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/decreto_0338_2022.htm

PRESIDENCIA DE LA REPÚBLICA DE COLOMBIA. Decreto 851 de 2024. «Por el cual se dictan disposiciones relacionadas con la restricción de comunicaciones no autorizadas al interior de Establecimientos de Reclusión del Orden Nacional (ERON), se adicionan unos artículos al Capítulo 1 del Título 1 de la Parte 2 del Libro 2 del Decreto número 1069 de 2015, y se modifican y derogan algunas disposiciones del Título 11 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015.». Diario Oficial No. 52.808 de 5 de julio de 2024. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/decreto_0851_2024.htm

PRESIDENCIA DE LA REPÚBLICA. Decreto 113 de 2022. «Por el cual se modifica la estructura del Ministerio de Defensa Nacional». Diario Oficial No. 51.928 de 25 de enero de 2022. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=176328

PRESIDENTE DE LA REPÚBLICA DE COLOMBIA. Decreto 1427 de 2017. «Por el cual se modifica la estructura orgánica y se determinan las funciones de las dependencias del Ministerio de Justicia y del

Derecho.» Diario Oficial No.50.340 de 29 de agosto de 2017. [En línea]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83275

COMISIÓN DE REGULACIÓN DE COMUNICACIONES (CRC). Resolución CRC 5050 de 2016. «Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones». [En línea] Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_5050_2016.htm

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (MINTIC). Resolución MinTIC 202 de 2010, modificada por la Resolución 1272 de 2020. Artículo 1. «Por la cual se expide el glosario de definiciones conforme a lo ordenado por el inciso 2o del artículo 6o de la Ley 1341 de 2009.». Diario Oficial No. 47.656 de 19 de marzo de 2010. [En línea]. Disponible en: https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_mintic_0202_2010.htm

DOCUMENTACIÓN TÉCNICA Y REGULACIÓN INTERNACIONAL

AUTORIDADE NACIONAL DE COMUNICAÇÕES – ANACOM. Início de procedimento de elaboração de um regulamento relativo à identificação da linha chamadora e do remetente de uma mensagem. 21 de marzo de 2023. [Información extraída de documento en línea].

COMREG. Combatting scam calls and texts: Response to consultation on network-based interventions. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.comreg.ie/publication/combatting-scam-calls-and-texts-response-to-consultation-on-network-based-interventions-to-reduce-the-harm-from-nuisance-communications

CULLEN INTERNATIONAL. Canadian Centre for Cyber Security publishes National Cyber Threat Assessment. 17 de diciembre de 2020. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. CEE Telecoms Update. 30 de septiembre de 2023. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. ComReg adopts measures to combat scam calls and SMS. 12 de abril de 2024. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. Countering online scams. 21 de mayo de 2023. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. Explainer: STIR/SHAKEN – a tool for combating scam calls. 11 de octubre de 2024. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. FCC mandates voice service providers to implement the STIR/SHAKEN caller ID authentication framework by 30 June 2021. 16 de abril de 2020. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. Malaysia introduces mandatory licensing for internet messaging and social media service providers. 26 de agosto de 2024. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. Singapore consults on initiatives to reduce scam SMS. 25 de agosto de 2022. [Información extraída de documento en línea].

CULLEN INTERNATIONAL. Singapore proposes shared liability scheme on phishing scams. 21 de noviembre de 2023. [Información extraída de documento en línea].

ELECTRONIC COMMUNICATIONS COMMITTEE OF EUROPEAN CONFERENCE OF POSTAL AND TELECOMMUNICATIONS ADMINISTRATIONS – CEPT. ECC Report 212. Evolution in the Use of E.212 Mobile Network Codes. [En línea]. 9 de abril de 2014. [Consultado el 28 de mayo de 2025]. Disponible en: https://docdb.cept.org/download/1152

GOBIERNO DE AUSTRALIA. Cybersecurity Strategy Summary 2024. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf

GOBIERNO DEL REINO UNIDO. Fraud Strategy: Stopping scams and protecting the public. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public

INTERNATIONAL TELECOMMUNICATION UNION. ITU-T Recommendation E.101: Definitions of terms used for identifiers (names, numbers, addresses and other identifiers) for public telecommunication services and networks in the E-series Recommendations. [En línea]. 2020. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.itu.int/rec/T-REC-E.101/en

KASPERSKY. What is social engineering? [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.kaspersky.com/resource-center/definitions/what-is-social-engineering

OFCOM. Call for input: Reducing mobile messaging scams. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams

OFCOM. Call for input: Reducing scam calls from abroad which spoof UK mobile numbers. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/186068-call-for-input-options-to-address-mobile-spoofing/associated-documents/cfi-reducing-scam-calls-from-abroad-which-spoof-uk-mobile-numbers.pdf?v=373415

OFCOM. Calling Line Identification. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/calling-line-identification

OFCOM. Good practice guide on sub-allocated and assigned numbers. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/good-practice-guide-on-sub-allocated-assigned-numbers

OFCOM. Improving Calling Line Identification (CLI) data accuracy. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/improving-cli-data-accuracy

SEJM – PARLAMENTO DE POLONIA. Proyecto de ley núm. 3069. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm

TELECOM REGULATORY AUTHORITY OF INDIA – TRAI. TCCC Public Consultation Documents. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://trai.gov.in/tcccpr

ZAMORA, E. A. Value chain analysis: A brief review. Asian Journal of Innovation and Policy, 2016, vol. 5, n.º 2, p. 116-128. DOI: http://dx.doi.org/10.7545/ajip.2016.5.2.116

DOCUMENTACIÓN DE LA COMISIÓN DE REGULACIÓN DE COMUNICACIONES

CRC. Agenda Regulatoria 2025–2026. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.crcom.gov.co/sites/default/files/agenda/agenda-regulatoria-2025-2026.pdf

CRC. Comunicación identificada con el radicado de salida No. 2025512256 del 23 de abril de 2025.

CRC. Documento de Respuestas a Comentarios de las Resoluciones CRC 7810 y 7811 de 2025. 16 de junio de 2025. Página 45 a 49. [en línea]. Consultado en: https://www.crcom.gov.co/system/files/Biblioteca%20Virtual/Documento%20de%20respuesta%20a%20comentarios%20-%20Simplificaci%C3%B3n%20del%20marco%20regulatorio%202024/Documento-Respuesta-Comentarios-Simplificacion-Marco-Regulatorio-2024-VF.pdf

CRC. Documento soporte del proyecto publicado en el marco del proyecto Revisión Integral del Régimen de Administración de Recursos de Identificación. Julio de 2019. [En línea]. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-71-2/Propuestas/8_regmenaripublicacion.pdf

CRC. Documento técnico sobre la cadena de valor de redes, en el marco del proyecto de revisión del régimen de acceso, uso e interconexión (Resolución CRC 6522 de 2022). [En línea]. Disponible en: https://www.crcom.gov.co/system/files/Proyectos%20Comentarios/2000-59-4/Propuestas/cadena-valor-redes.pdf

CRC. Política de mejora regulatoria de la Comisión de Regulación de Comunicaciones. p. 35. Agosto 22 de 2019. [En línea]. Disponible en: https://www.crcom.gov.co/sites/default/files/webcrc/noticias/documents/documento-politica-mejoraregulatoria-crc.pdf

OTRAS ENTIDADES NACIONALES

FISCALÍA GENERAL DE LA NACIÓN. Cartilla metodológica de atención de delitos informáticos. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

MINISTERIO DE DEFENSA NACIONAL. Delitos informáticos [Conjunto de datos]. Datos Abiertos Colombia. [Consultado el 23 de mayo de 2025]. [Información con corte de actualización al 20 de mayo de 2025]. Disponible en: https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

MINISTERIO DE DEFENSA NACIONAL. Observatorio de Derechos Humanos y Defensa Nacional. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.mindefensa.gov.co/defensa-y-seguridad/datos-y-cifras

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Indicadores de Seguridad de la Información (SI) y Ciberseguridad (CI). [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.superfinanciera.gov.co/publicaciones/10115571/indicadores-de-seguridad-de-la-informacion-y-ciberseguridad-2024/

SUPERINTENDENCIA FINANCIERA DE COLOMBIA. Retos importantes en seguridad y disponibilidad en el sector financiero. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.superfinanciera.gov.co/loader.php?lServicio=Tools2&lTipo=descargas&lFuncion=descargar&idFile=1072807

OTRAS REFERENCIAS

ASOBANCARIA. Impacto económico y social del phishing y el smishing en Colombia y el mundo. Edición 1256. 26 de octubre de 2020. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2020/10/1256VF.pdf

BANCA & ECONOMÍA. Discurso de instalación del 16° Congreso de Prevención de Fraude y Ciberseguridad. Edición 1400. 30 de octubre de 2023. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.asobancaria.com/wp-content/uploads/2023/10/1400-BE-3.pdf

EL TIEMPO. Le contamos cuánto invirtieron los bancos en 2024 para proteger datos y recursos de sus clientes de ciberataques. Columna de Carlos Arturo García Mahecha. 26 de marzo de 2025. [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.eltiempo.com/economia/sector-financiero/le-contamos-cuanto-invirtieron-las-entidades-financieras-para-proteger-los-datos-y-recursos-de-sus-clientes-en-2024-3438724

REAL ACADEMIA ESPAÑOLA. Diccionario de la lengua española. Entrada: "Fraude". [En línea]. [Consultado el 28 de mayo de 2025]. Disponible en: https://dle.rae.es/fraude?m=form

TIC TAC; CCIT; POLICÍA NACIONAL. Informe tendencias del cibercrimen – Primer trimestre 2020. [En línea]. [Publicado el 21 de abril de 2020]. [Consultado el 28 de mayo de 2025]. Disponible en: https://www.ccit.org.co/noticias/aumento-37-la-ciberdelincuencia-en-colombia-relacionada-con-el-covid-19/

UNIVERSIDAD DEL ROSARIO. Escuela de Ingeniería, Ciencia y Tecnología. Primera encuesta sobre seguridad digital en Colombia. [En línea]. [Consultado el 29 de mayo de 2025]. Disponible en: https://urosario.edu.co/escuela-ingenieria/seguridad-digital

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9. ANEXOS

ANEXO 1. EXPERIENCIAS INTERNACIONALES

Este anexo presenta el análisis detallado por país de las experiencias internacionales revisadas, con el objetivo de identificar la problemática y sus dimensiones desde un punto de vista estadístico. Además, se examinan las medidas implementadas en cada experiencia para evaluar su potencial en la generación de una estrategia nacional en Colombia, resaltando los mecanismos innovadores adoptados hasta la fecha.

9.1. Australia

En Australia, el fraude y las estafas representan un problema significativo que afecta tanto a consumidores como a empresas. En 2022, las estafas causaron pérdidas financieras superiores a los 3 mil millones de dólares australianos (aproximadamente 1.95 mil millones de dólares estadounidenses). Además, el 65% de los australianos fueron expuestos a intentos de estafa durante el mismo año. Estas cifras reflejan un aumento del 80% en comparación con las pérdidas registradas en 2021. La creciente sofisticación y coordinación de los estafadores, que utilizan tecnologías avanzadas y encuentran nuevas vulnerabilidades para explotar, agravan aún más la situación[104].

En 2023, 601,000 australianos reportaron pérdidas por un total de 2.74 mil millones de dólares australianos debido a estafas. Aunque esta cifra es ligeramente inferior a la de 2022, sigue representando un impacto significativo en la economía y en los individuos afectados.

Se identificó también que las estafas no solo causan pérdidas financieras, sino que también generan estrés indebido, daño psicológico y emocional a las víctimas. La necesidad de acción urgente se destaca para mantener a los australianos seguros en un entorno digital cada vez más complejo.

El marco propuesto para combatir las estafas en Australia[105] se basa en un enfoque de ecosistema completo, donde cada actor de dicho ecosistema (bancos, proveedores de telecomunicaciones, plataformas de comunicación digital, gobierno y reguladores, y empresas en general) tiene un papel que desempeñar. Este enfoque coordinado entre el gobierno, los reguladores y las empresas busca prevenir que los estafadores contacten a los consumidores, y educar a su vez a los consumidores para que reconozcan y reporten estafas.

Al respecto, este país cerró una consulta pública lanzada en noviembre de 2023[106] para recopilar opiniones sobre un marco de código para abordar el tema de las estafas. El marco tiene como objetivo establecer roles y responsabilidades claros para los diferentes actores del ecosistema a fin de combatir las estafas.

---

[104] Información extraída del documento disponible en el siguiente vínculo: https://treasury.gov.au/sites/default/files/2025-01/p2025-623966.pdf. Actualización del sitio web el 3 de febrero de 2025 https://treasury.gov.au/publication/p2025-623966

[105] El proyecto donde se fija el marco de prevención de estafas en Australia puede ser consultado en el siguiente enlace: https://treasury.gov.au/consultation/c2024-573813

[106] La consulta pública puede ser accedida mediante el siguiente vínculo: https://treasury.gov.au/sites/default/files/2023-11/c2023-464732-cp.pdf

Los bancos tienen la responsabilidad de implementar procesos para verificar la identidad del destinatario de los pagos y detectar transacciones de alto riesgo que puedan ser estafas. Deben tomar medidas para advertir a los consumidores, bloquear o suspender transacciones sospechosas y colaborar con otros bancos para deshabilitar cuentas de estafadores. Además, los bancos deben proporcionar métodos accesibles para que los consumidores tomen medidas inmediatas si sospechan que sus cuentas han sido comprometidas y ayudar a rastrear y recuperar fondos transferidos a estafadores.

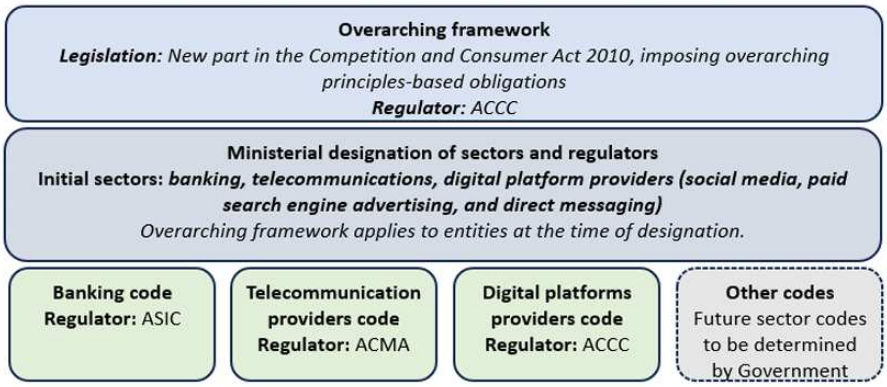
Los proveedores de telecomunicaciones están sujetos al Código de Reducción de Llamadas y Mensajes de Estafa, que les exige tomar medidas razonables para prevenir y bloquear llamadas y mensajes de texto de estafa. Deben verificar el origen de las llamadas y mensajes, monitorear sus redes para identificar características de estafas y actuar rápidamente para bloquear números o identificadores de remitentes fraudulentos. Hasta el 30 de junio de 2023, los proveedores de este país bloquearon aproximadamente 1.4 mil millones de llamadas de estafa y 257 millones de mensajes de texto de estafa bajo los lineamientos de este código.

Las plataformas de comunicaciones digitales deben implementar procesos para autenticar y verificar la identidad y legitimidad de los usuarios comerciales y anunciantes, prevenir que los usuarios vendan o anuncien productos y servicios fraudulentos, y detectar interacciones de alto riesgo. También deben actuar rápidamente sobre la información que identifica a un usuario o interacción como una estafa, incluyendo bloquear o deshabilitar cuentas utilizadas por estafadores.

El gobierno y los reguladores tienen un papel coordinador y de supervisión. La Comisión Australiana de Competencia y Consumo (ACCC) lidera el Centro Nacional Anti-Estafas (NASC), que coordina esfuerzos para prevenir estafas mediante la mejora del intercambio de inteligencia y la concienciación pública. La Comisión Australiana de Valores e Inversiones (ASIC) y la Autoridad Australiana de Comunicaciones y Medios (ACMA) también desempeñan roles clave en la supervisión y aplicación de las medidas anti-estafas.

Todas las demás empresas implicadas en el ecosistema de estafas tienen la responsabilidad de desarrollar, mantener e implementar una estrategia anti-estafas que incluya la prevención, detección, interrupción y respuesta a las estafas. Deben compartir información sobre estafas con otros negocios, el NASC y los reguladores relevantes, y actuar sobre la inteligencia recibida para detener estafas actuales y prevenir futuras.

Ilustración 21. Proposed scams prevention framework



Fuente: Documento de conjunto de reformas del tesoro Australiano[107].

Es de destacar que las autoridades australianas son conscientes de que el marco desarrollado debe ser flexible para responder a los cambios en el ecosistema de estafas, incluyendo nuevos tipos de estafas, tecnologías y canales de entrega explotados por los estafadores. Reconocen que dicha capacidad de respuesta dinámica es crucial para adaptarse a las tácticas en constante evolución de los estafadores.

El marco complementará y aprovechará los regímenes regulatorios existentes, como las regulaciones de privacidad, seguridad de identidad y financieras, que también combaten las estafas. Esto incluye la Estrategia Nacional de Resiliencia de Identidad y las reformas a la Ley de Privacidad de Australia.

En cuanto a las medidas específicas adoptadas para mitigar el fraude en este país, se destacan puntualmente las siguientes:

- **Establecimiento del Centro Nacional Anti-Estafas (NASC)**

El NASC, liderado por la Comisión Australiana de Competencia y Consumo (ACCC), se estableció el 1 de julio de 2023. Este centro coordina esfuerzos entre el gobierno y la industria para prevenir estafas mediante la mejora del intercambio de inteligencia y la concienciación pública. El NASC también trabaja en la construcción de capacidades de intercambio de datos para mejorar la calidad, oportunidad y cobertura de la información sobre estafas.

- **Medidas de la Comisión Australiana de Valores e Inversiones (ASIC)**

La ASIC ha tomado medidas para identificar y eliminar sitios web de estafas de inversión, habiendo eliminado más de 2,500 sitios web desde julio de 2023. Estas acciones buscan reducir la proliferación de estafas en línea y proteger a los consumidores de inversiones fraudulentas.

- **Registro de Identificación de Remitentes de SMS**

[107] El documento completo puede ser consultado en el siguiente enlace: https://treasury.gov.au/sites/default/files/2024-09/c2024-573813-summary.pdf

El Registro de Identificación de Remitentes de SMS es una iniciativa clave dentro del Marco de Prevención de Estafas (SPF) de Australia, diseñada por la Autoridad Australiana de Comunicaciones y Medios (ACMA) para proteger a los consumidores de mensajes de texto fraudulentos. Este registro tiene como objetivo prevenir que los estafadores imiten nombres de marcas confiables en los encabezados de mensajes de texto, una táctica comúnmente utilizada para engañar a los consumidores y hacer que caigan en estafas.

El principal objetivo del registro es asegurar que los mensajes de texto provengan de remitentes legítimos. Esto se logra mediante la autenticación y verificación de los remitentes de SMS, garantizando que solo las entidades autorizadas puedan enviar mensajes utilizando nombres de marcas reconocidas. Al establecer un registro centralizado, se dificulta que los estafadores puedan suplantar la identidad de marcas confiables, reduciendo significativamente la posibilidad de que los consumidores sean engañados por mensajes fraudulentos que aparentan ser de fuentes legítimas.

El funcionamiento del registro incluye varios pasos clave. Primero, las empresas que deseen enviar mensajes de texto utilizando nombres de marcas deben registrarse y verificar su identidad. Este proceso de verificación asegura que solo las entidades legítimas puedan utilizar nombres de marcas en los encabezados de sus mensajes. Además, el registro permite a los proveedores de telecomunicaciones implementar filtros anti-estafas que bloquean mensajes de texto con enlaces de phishing conocidos o características sospechosas. Estos filtros monitorean continuamente las redes para identificar y bloquear mensajes fraudulentos antes de que lleguen a los consumidores.

La colaboración entre proveedores de telecomunicaciones es esencial para el éxito del registro. Los proveedores deben cooperar entre sí para rastrear el origen de llamadas y mensajes sospechosos, permitiendo identificar y bloquear rápidamente los números o identificadores de remitentes fraudulentos. Este esfuerzo conjunto es crucial para mantener la integridad del sistema y proteger a los consumidores de posibles estafas.

Los beneficios para los consumidores son significativos. Al asegurar que los mensajes de texto provengan de remitentes legítimos, los consumidores pueden confiar más en la autenticidad de los mensajes que reciben, reduciendo el riesgo de caer en estafas y protegiendo su información personal y financiera. Además, la implementación del registro ha demostrado ser efectiva en la reducción de estafas, con una disminución significativa en el número de mensajes de texto fraudulentos que llegan a los consumidores.

En este orden de ideas, el Registro de Identificación de Remitentes de SMS es una medida innovadora y efectiva dentro del Marco de Prevención de Estafas de Australia. Al autenticar y verificar a los remitentes de SMS, prevenir la suplantación de identidad y bloquear mensajes fraudulentos, este registro juega un papel crucial en la protección de los consumidores contra las estafas.

- **Código de Reducción de Llamadas y Mensajes de Estafa**

El Código de Reducción de Llamadas y Mensajes de Estafa es otra parte integral del Marco de Prevención de Estafas (SPF) de Australia. Este código establece obligaciones específicas para los proveedores de servicios de telecomunicaciones con el objetivo de prevenir, detectar y bloquear llamadas y mensajes de texto fraudulentos antes de que lleguen a los consumidores.

El principal objetivo del código es prevenir las estafas mediante la implementación de filtros anti-estafas que bloqueen mensajes de texto con enlaces de *phishing* conocidos o características sospechosas. Estos filtros están diseñados para identificar y bloquear mensajes fraudulentos antes de que lleguen a los consumidores. Además, los proveedores deben monitorear activamente sus redes para detectar indicadores de estafas, como actividades de alto volumen y corta duración, y el uso de URLs maliciosas en mensajes de texto. Este monitoreo continuo permite a los proveedores identificar patrones sospechosos y tomar medidas rápidas para bloquear las comunicaciones fraudulentas.

Los proveedores de telecomunicaciones también tienen la responsabilidad de investigar y tomar medidas apropiadas para bloquear llamadas de estafa que se originan en sus redes. Esto incluye la cooperación con otros proveedores para rastrear el origen de una llamada sospechosa y bloquear números o identificadores de remitentes fraudulentos. La colaboración entre proveedores es esencial para el éxito del código, ya que permite una respuesta más rápida y efectiva para bloquear comunicaciones fraudulentas.

Además de las medidas técnicas, los proveedores de telecomunicaciones deben educar a los consumidores sobre las posibles estafas que pueden afectarles. Esto incluye proporcionar información sobre cómo identificar mensajes y llamadas fraudulentas y qué hacer si reciben una comunicación sospechosa. Las campañas de educación al consumidor ayudan a aumentar la concienciación sobre las estafas y proporcionan a los consumidores las herramientas necesarias para identificar y reportar comunicaciones sospechosas.

Los beneficios para los consumidores son significativos. Al bloquear llamadas y mensajes de texto fraudulentos antes de que lleguen a los consumidores, el código reduce significativamente el riesgo de que los consumidores sean víctimas de estafas. Esto protege tanto la información personal como financiera de los consumidores. La implementación del código ha demostrado ser efectiva en la reducción de estafas. Como ya se indicó, hasta el 30 de junio de 2023 se habían bloqueado aproximadamente 1.4 mil millones de llamadas de estafa y 257 millones de mensajes de texto de estafa bajo este código, lo cual demuestra su alto impacto.

- **Acuerdo Scam-Safe del Sector Bancario**

El Acuerdo Scam-Safe, lanzado en noviembre de 2023 por la Asociación Bancaria Australiana, incluye medidas como la confirmación del destinatario del pago, advertencias y retrasos para proteger a los clientes, y la expansión del intercambio de información. Este acuerdo busca mejorar la detección, prevención y respuesta a las estafas en el sector bancario.

Finalmente es importante destacar que desde el establecimiento del Centro Nacional Anti-Estafas (NASC), las pérdidas reportadas a Scamwatch han disminuido en un 41% en los primeros 12 meses. Esto indica que las medidas implementadas están teniendo un impacto positivo en la reducción de las estafas. Además, el Gobierno financiará una campaña en 2025 para mejorar la conciencia comunitaria sobre las estafas y ayudar a los australianos a identificarlas, evitarlas y reportarlas.

En síntesis, las estadísticas más recientes reportadas muestran que, aunque las pérdidas por estafas siguen siendo significativas en Australia, las medidas adoptadas están comenzando a tener un impacto positivo en la reducción de estas actividades fraudulentas. La implementación de mecanismos innovadores como el registro de identificación de remitentes de SMS y el Código de Reducción de

Llamadas y Mensajes de Estafa son pasos cruciales para proteger a los consumidores y hacer de Australia un objetivo menos atractivo para los estafadores.

9.2. Brasil

Entre 2022 y 2025, la Agencia Nacional de Telecomunicaciones (Anatel) de Brasil implementó un conjunto integral de medidas regulatorias y operativas con el objetivo de mitigar el volumen de llamadas inoportunas y combatir prácticas fraudulentas en el ámbito de las telecomunicaciones.

Adicionalmente vale la pena mencionar que esta Agencia publicó el 28 de abril de 2025 la Resolución Nº 777, que constituye el nuevo Reglamento General de los Servicios de Telecomunicaciones (RGST). La resolución revoca 42 normas anteriores y sustituye otras cinco, algunas de las cuales estaban vigentes desde la década de 1990.

Se destaca de la experiencia de Brasil la implementación de diversas medidas para combatir las comunicaciones indeseadas y el fraude en los servicios de telecomunicaciones, entre ellas las siguientes:

- **Bloqueo de llamadas masivas**

A través de sucesivos despachos cautelares, Anatel estableció límites estrictos para la realización de llamadas en masa. Se fijó un umbral de hasta 100 mil llamadas por día (Despacho 160/2022) y se introdujeron criterios de eficiencia, como el porcentaje máximo de llamadas de corta duración (hasta el 85% de las llamadas con duración inferior a 3 segundos, ampliado posteriormente a 6 segundos). Estas medidas permitieron identificar y bloquear a usuarios que realizaban intentos indiscriminados de llamadas.

- **Combate a la suplantación de identidad telefónica (Spoofing)**

Mediante el Despacho 262/2024, Anatel prohibió la comercialización de servicios que posibiliten la alteración indebida del número de origen de las llamadas.

Adicionalmente, el nuevo reglamento expedido en 2025 establece directrices para la autenticación obligatoria de llamadas telefónicas mediante numeración pública, alineada con la tecnología internacional STIR/SHAKEN, aunque el término no sea mencionado directamente en el texto.

Los operadores de telefonía fija y móvil deberán adoptar una solución técnica centralizada, coordinada por un grupo de trabajo bajo supervisión de la Anatel, con un plazo de hasta tres años para su adecuación. La medida busca frenar prácticas como el spoofing, aumentar la transparencia y combatir fraudes en llamadas de voz.

Asimismo, se determinó el bloqueo de rutas de interconexión que transportaran llamadas con numeración irregular, no asignada o inválida, haciendo uso de listas de no originación (DNO).

- **Autenticación e identificación de llamadas**

Se promovió el desarrollo e implementación de la tecnología denominada "Origem Verificada", orientada a la autenticación del origen de las llamadas. Esta solución, adoptada por el 99% de los accesos móviles

(SMP) y el 95% de los accesos fijos (STFC), permitió la identificación segura de más de 10 mil millones de llamadas.

- **Herramientas complementarias de transparencia y control**

En lo que respecta específicamente a las llamadas de telemarketing activas, los principales proveedores de servicios de telecomunicaciones han creado la plataforma «Não Me Perturbe» similar al Registro de Números Excluidos (RNE) creado en Colombia por la CRC. Con la autorización de Anatel, desde 2022, el sistema permite a los consumidores que no deseen recibir este tipo de llamadas telefónicas registrarse gratuitamente en la Lista Nacional de No Molestar.

Dentro de los 30 días siguientes a la solicitud de registro, el consumidor deja de recibir llamadas de los operadores participantes que le ofrezcan servicios de telefonía fija, telefonía móvil, banda ancha y televisión de pago. Los bloqueos también pueden utilizarse para evitar las promociones relativas a ventas y servicios mediante contacto telefónico para préstamos y tarjetas de crédito de nómina, a través de las instituciones financieras participantes.

En el caso de entidades financieras, el bloqueo de llamadas no aplica para cobro de deudas, refinanciamiento de deudas, solicitudes de portabilidad de servicios, confirmación de datos o prevención de fraude.

En la misma dirección, se creó un mecanismo de control ciudadano mediante la plataforma «Qual Empresa Me Ligou» con la intención de aportar al usuario la identificación de las empresas emisoras de las llamadas, y se habilitó un servicio de validación cruzada entre CPF y número telefónico, con el fin de optimizar los registros de usuarios en el sector de teleservicios.

- **Verificación adicional de llamadas**

Anatel exige a los operadores implementar medidas para evitar el uso de múltiples números aleatorios en llamadas realizadas desde una misma fuente. Esta práctica dificulta la identificación del origen de las llamadas, complicando así el bloqueo de comunicaciones no deseadas o fraudulentas por parte de los consumidores. Anatel señala que esta práctica se está implementando en el sector de teleservicios para llevar a cabo telemarketing abusivo.

- **Canal de denuncias para instituciones financieras**

Anatel también ordenó la creación de un canal específico para que las instituciones financieras reporten los números utilizados en fraudes. Con esta información, los operadores podrán identificar y bloquear el acceso a los usuarios que utilicen estos números para cometer delitos, además de informar a las autoridades competentes.

En caso de incumplimiento, los proveedores pueden ser penalizados con multas, y en casos más graves, perder su autorización para operar servicios de telecomunicaciones en Brasil.

- **Principios para el uso de Inteligencia Artificial**

Finalmente, resulta relevante mencionar que el nuevo reglamento general establece, por primera vez, principios específicos para el uso de Inteligencia Artificial (IA) en redes y servicios de

telecomunicaciones. Se exigen criterios como confiabilidad, no discriminación, responsabilidad, privacidad, transparencia y respeto a los derechos fundamentales.

Todas estas acciones forman parte de la estrategia diseñada por Brasil para proteger a los consumidores y restaurar la confianza en los servicios de telecomunicaciones, y como resultado de ellas, Anatel estima que se evitaron aproximadamente 196 mil millones de llamadas inoportunas entre junio de 2022 y febrero de 2025[108]. Asimismo, indica que se bloquearon 1.083 empresas por incumplimiento de los límites regulatorios, se instauraron 24 procesos administrativos y se aplicaron multas por un total de R$ 39 millones.

9.3. Canadá

De acuerdo con el Reporte Anual publicado por el Centro de Ciberseguridad de Canadá en 2020, el ciberdelito es la ciber-amenaza con mayor probabilidad de afectar a los canadienses. En efecto, para el año 2019 este centro estimó que los canadienses perdieron más de USD 32,28 millones por fraudes cibernéticos y que entre 2016 y 2019 se han presentado más de 1200 casos de fraude mediante correos electrónicos fraudulentos (modalidad conocida también como Compromiso de Correos Electrónicos Comerciales -BEC[109]) causando pérdidas por más de USD 33,78 millones. Adicionalmente en el año 2019 ocurrieron filtraciones de datos financieros que afectaron a más de 10 millones de canadienses[110].

Por su parte, en el año 2022 el Centro Canadiense Antifraude recibió denuncias de fraude y ciberdelincuencia causaron pérdidas por USD 391,85 millones, representando un aumento de casi el 40 % con respecto a 2021. La misma fuente estimó que solo entre el 5 % y el 10 % de las víctimas denuncian fraudes en Canadá.

Con el fin de hacer frente a estos flagelos, el gobierno canadiense ha adelantado las siguientes estrategias:

- En el año 2018, el Centro Cibernético publicó la primera Evaluación Nacional de Ciber amenazas 2018 y estableciendo las prioridades del Centro para mitigar las ciber amenazas;
- En agosto de 2019, el Instituto de Innovación, Ciencia y Desarrollo Económico (ISED), en colaboración con el Instituto de Seguridad de las Comunicaciones y el Consejo Canadiense de Normas, lanzó CyberSecure Canadá, el programa federal de certificación cibernética para pequeñas y medianas empresas
- En mayo de 2019, el ISED presentó la Carta Digital Canadiense, que traza las estrategias para aumentar la confianza y la seguridad de los servicios que se prestan en línea.

Teniendo en cuenta que las llamadas de voz fraudulentas generalmente suplantan el número identificador de la parte llamante para engañar a sus víctimas, la Comisión de Radio, Televisión y Telecomunicaciones de Canadá (*Canadian Radio-television and Telecommunications Commission* o

[108] Esta información fue proporcionada directamente por parte de Anatel a la CRC en una reunión sostenida el 28 de abril de 2025.
[109] BEC: Business Email Compromise
[110] Información extraída del documento *Canadian Centre for Cyber Security publishes National Cyber Threat Assessment*; Cullen International; 17 de diciembre de 2020

CRTC) estableció la obligación de implementar el protocolo STIR/SHAKEN[111], creado por el IETF (*Internet Engineering Task Force*), la ATIS (*Alliance for Telecommunications Industry Solutions*) y el SIP Forum[112].

Las llamadas VoIP utilizan el protocolo SIP (*Session Initiation Protocol*) para iniciar y enrutar llamadas. Uno de los componentes SIP es el encabezado SIP que incluye información sobre la persona que llama, la cual puede ser editada por la persona que llama. Aprovechando esta funcionalidad, los estafadores ocultan su identidad introduciendo información falsa de identificación de llamada en el software VoIP. Para evitar la suplantación de la identidad del llamante, STIR añade información al encabezado SIP para identificar con precisión el origen de la llamada a lo largo de toda su ruta.

El proveedor de VoIP examina el identificador de llamada, lo compara con los datos de su sistema e indica si la llamada se originó en un cliente verificado. Después de verificada el origen de la llamada, el proveedor desde donde se origina la llamada adjunta al encabezado del SIP la constatación, mediante una firma digital, que la identificación del llamante ha sido autenticada.

La adopción del STIR/SHAKEN por parte de la CRTC[113] y otras entidades regulatorias, como mecanismo para combatir el fraude, se ha visto afectada en consideración a las siguientes razones:

- El método solo puede ser eficaz si lo implementan todos los operadores involucrados en el origen, tránsito y terminación de una llamada.
- No funciona con las redes de telefonía pública conmutada tradicionales, y por lo tanto no es una solución eficaz en países que aún no han adoptado redes IP o que operan redes legadas.
- Los costos de implementación son elevados, especialmente para operadores pequeños.
- Se han encontrado dificultades para crear un ecosistema global de certificación confiable.

9.4. Chile

En el marco de la Agenda de Seguridad Digital impulsada por el Gobierno de Chile, la Subsecretaría de Telecomunicaciones (Subtel) ha implementado una serie de medidas regulatorias orientadas a fortalecer la protección de los usuarios frente a prácticas fraudulentas y comunicaciones no deseadas en el ámbito de las telecomunicaciones.

Estas acciones buscan garantizar la integridad de los servicios, resguardar la privacidad de los consumidores y fomentar un entorno digital más seguro y transparente. A continuación, se detallan las principales iniciativas:

- **Implementación obligatoria de verificación biométrica**

A partir de febrero de 2025, todas las empresas proveedoras de servicios de telecomunicaciones están obligadas a incorporar mecanismos de verificación biométrica para la realización de trámites sensibles

[111] STIR: Secure Telephony Identity Revisited; SHAKEN: Signature-based Handling of Asserted Information by toKENs.
[112] Información extraída del documento *Explainer: STIR/SHAKEN – a tool for combating scam calls*; Cullen International; 11 de octubre de 2024
[113] Ibid.

por parte de los usuarios[114]. Esta exigencia incluye, entre otros, procesos como la contratación de servicios, la portabilidad numérica y la reposición de tarjetas SIM.

La verificación biométrica puede realizarse mediante tecnologías como el reconocimiento facial, la huella dactilar o la firma electrónica avanzada, y tiene como objetivo principal prevenir delitos como la suplantación de identidad y el fraude por portabilidad, que han experimentado un aumento significativo en los últimos años.

- **Asignación de prefijos telefónicos para llamadas comerciales**

Con el propósito de transparentar el origen y la naturaleza de las llamadas telefónicas de carácter comercial, Subtel[115] ha dispuesto la implementación de nuevos prefijos numéricos que permitirán a los usuarios identificar de forma clara si una llamada ha sido solicitada o no. Esta medida entrará en vigor el 7 de agosto de 2025 y contempla lo siguiente:

- ✓ **Prefijo 600:** Identificará llamadas comerciales solicitadas, es decir, aquellas realizadas por empresas con las que el usuario mantiene una relación contractual o ha otorgado su consentimiento expreso para ser contactado.

- ✓ **Prefijo 809:** Corresponderá a llamadas comerciales no solicitadas, incluyendo aquellas de carácter masivo, automatizado o realizadas sin autorización previa del destinatario.

Esta diferenciación busca empoderar a los usuarios, permitiéndoles tomar decisiones informadas sobre la atención de llamadas y reduciendo la exposición a prácticas intrusivas o engañosas.

- **Herramienta "No Molestar" del SERNAC**

Complementariamente, los usuarios pueden acceder a la plataforma "No Molestar", administrada por el Servicio Nacional del Consumidor (SERNAC), la cual permite registrar números telefónicos, direcciones de correo electrónico y otros canales de contacto para evitar recibir comunicaciones promocionales no deseadas por parte de empresas. Esta herramienta es de carácter gratuito y está disponible a través del Portal del Consumidor de ese país.

9.5. España

En los últimos años, España ha experimentado un incremento exponencial en la cibercriminalidad, destacando particularmente las estafas de suplantación de identidad. Indican que estas estafas suelen iniciarse con una llamada telefónica o un mensaje de texto en los que el emisor suplanta la identidad de una organización de confianza, como una entidad bancaria, una administración pública o una empresa de transporte, con la clara intención de defraudar al consumidor. Los estafadores engañan a los consumidores para que proporcionen información personal y financiera confidencial, faciliten sus

[114] Subtel anunció el 4 de febrero de 2025 que todas las empresas deberán aplicar esta normativa que busca evitar las estafas por suplantación de identidad: https://www.subtel.gob.cl/mas-seguridad-y-menos-estafas-desde-hoy-todos-tus-tramites-con-empresas-de-telecomunicaciones-deberan-utilizar-biometria/
[115] Subtel anunció el 20 de marzo de 2025 la implementación de una numeración especial para identificar llamadas comerciales, como parte de la Agenda de Seguridad Digital del Gobierno https://www.subtel.gob.cl/gobierno-anuncia-implementacion-de-numeracion-especial-para-la-identificacion-de-llamadas-comerciales/

claves personales o realicen acciones como acceder a una web, llamar a un número telefónico, ordenar una transferencia o contratar un servicio.

Las estadísticas reflejan la magnitud del problema en España. Según la última Memoria de Reclamaciones del Banco de España (2022), las reclamaciones por fraude ascendieron a 10,361, duplicando su volumen respecto al año anterior, con la suplantación de identidad detrás de alrededor del 47% de las reclamaciones. El Informe sobre la Cibercriminalidad en España del Ministerio del Interior (2022) reporta un aumento del 22.7% en los ciberdelitos, alcanzando un total de 374,737, de los cuales el 90% corresponden a fraudes informáticos. Además, el Instituto Nacional de Ciberseguridad (INCIBE) registró 33,576 incidentes de suplantación de identidad durante el año 2022.

Mencionan que estas estafas causan importantes daños financieros y económicos a todos los sectores de la sociedad española, incluidos los consumidores, las empresas y los organismos públicos. Además, disminuyen la confianza de los consumidores en las comunicaciones electrónicas, provocando que desconfíen de contestar llamadas y leer mensajes de texto, lo que perjudica a aquellas empresas y organismos que utilizan legítimamente estos canales de comunicación para facilitar información u ofrecer sus servicios.

En cuanto a las medidas específicas adoptadas para mitigar el fraude en este país, se destacan puntualmente las siguientes:

- **Bloqueo de Llamadas con Numeración No Atribuida o No Asignada**:

Los operadores están obligados a bloquear las llamadas que presenten como identificador de llamada (CLI) un número de teléfono español que no esté atribuido a ningún servicio o cuyo formato no sea coherente con el plan nacional de numeración telefónica. Esta medida busca evitar que los estafadores utilicen números falsos para engañar a los consumidores.

- **Bloqueo de Llamadas con Origen Internacional:**

Se obliga a los operadores a bloquear las llamadas recibidas desde el extranjero que presenten como CLI un número de teléfono español, salvo en casos de itinerancia internacional. Esta medida es crucial para dificultar la operación de estafadores ubicados fuera del territorio nacional.

- **Bloqueo de Mensajes SMS/MMS con Origen Internacional:**

Los proveedores de servicios de mensajería deben bloquear cualquier mensaje SMS/MMS recibido desde el extranjero que presente como CLI un número de teléfono o un alias español, salvo en casos de itinerancia internacional. Esta medida es esencial para prevenir fraudes a través de mensajes de texto.

- **Registro de Alias y Bloqueo de SMS/MMS con Alias No Registrados:**

Los proveedores de servicios de mensajería que utilicen alias deben inscribir estos en un registro gestionado por la Comisión Nacional de los Mercados y la Competencia (CNMC). Los operadores deben bloquear los mensajes identificados mediante alias que no hayan sido inscritos en el registro o que no hayan sido emitidos por proveedores habilitados.

- **Prohibición de Utilización de Numeración Móvil para Llamadas Comerciales:**

Se prohíbe el uso de numeración móvil para la prestación de servicios de atención al cliente y para la realización de llamadas comerciales prospectivas. En su lugar, se permite el uso de numeración 800 y 900, asegurando que devolver las llamadas a estos números sea gratuito para los consumidores.

- **Aplicación de Técnicas de Inteligencia Artificial (IA):**

Se están explorando técnicas de IA para el tratamiento de mensajes SMS, generando un *hash* que permite identificar el envío de SMS masivos potencialmente fraudulentos. Esta técnica permite tanto una actuación reactiva como proactiva y preventiva, mejorando la capacidad de detectar y bloquear mensajes fraudulentos antes de que lleguen a los consumidores.

Estas medidas representan un esfuerzo significativo para mitigar el impacto de las estafas de suplantación de identidad, restaurar la confianza de los consumidores en las comunicaciones electrónicas y proteger los intereses de los usuarios.

9.6. Estados Unidos

En el año 2021, la Comisión Federal de Comercio (*Federal Trade Commission* o FTC) recibió 5,1 millones de denuncias de ciberdelitos asociados con el robo de identidad, estafas de telemarketing y estafas relacionadas con el coronavirus, entre otros delitos. Según la FTC, los consumidores reportaron pérdidas de casi USD 8.800 millones por estafas y fraudes en 2022, un 30% más que en 2021. Por su parte El Buró Federal de Investigaciones (*Federal Bureau of Investigation* o FBI) destacó que las pérdidas potenciales por ciberataques aumentaron en un 49% entre los años 2021 y 2022, llegando a los USD 10.300 millones[116].

Con respecto a las pérdidas reportadas por fraude, estas ascendieron a USD 3.310 millones en 2022 (un 128 % más que en 2021) de las cuales el 80 % correspondían a estafas relacionadas con inversiones en criptomonedas[117].

El 31 de marzo de 2020, la Comisión Federal de Comunicaciones (*Federal Communications Commission* o FCC) de Estados Unidos ordenó a los proveedores de los servicios de telecomunicaciones de voz implementar la autenticación de identificador de llamadas mediante el protocolo STIR/SHAKEN[118], a partir del 30 de junio de 2021 para las redes IP (*Internet Protocol*) y con excepción de las redes operadas por operadores pequeños, cuyo plazo venció el 30 de junio de 2023[119].

El protocolo STIR/SHAKEN[120] permite a los proveedores de los servicios de telecomunicaciones de voz verificar de manera segura que el identificador de llamada transmitido coincide efectivamente con el número asignado al llamante. El STIR autentica el identificador de llamada, mientras que SHAKEN estandariza la implementación de los protocolos STIR en el sector.

---

[116] Información extraída del documento *Countering online scams*; Cullen International; 21 de mayo de 2023
[117] Ibid.
[118] Información extraída del documento *FCC mandates voice service providers to implement the STIR/SHAKEN caller ID authentication framework by 30 June 2021*; Cullen International; 16 de abril de 2020
[119] Información extraída del documento *Explainer: STIR/SHAKEN – a tool for combating scam calls*; Cullen International; 11 de octubre de 2024
[120] Su sigla en inglés por *Secure Telephone Identity Revisited* (STIR) y *signature-based handling of asserted information using tokens* (SHAKEN).

Las obligaciones de los Proveedores de servicios de voz de acuerdo con el tipo de llamada se presentan en la Tabla 7.

Tabla 7. Requerimientos impuestos por la FCC de acuerdo con el tipo de llamada

Tipo de Llamada	Obligaciones del Operador desde donde se origina la llamada	Obligaciones del Operador donde se contesta la llamada
Llamadas originadas y terminadas dentro de la Red operada por el mismo Proveedor de Servicios de Voz	Debe autenticar y verificar la información de identificación de la persona que llama.	
Llamadas originadas en una Red no operada por el Proveedor de Servicios de Voz donde se contesta la llamada	Debe: ▪ Autenticar la información del ID Llamante; y ▪ Transmitir esta información autenticada al siguiente proveedor en la ruta de la llamada, en la medida en que sea técnicamente factible).	Al recibir una llamada debe verificar que la información del ID llamante ha sido autenticada.

Fuente: Elaboración CRC a partir de *FCC mandates voice service providers to implement the STIR/SHAKEN caller ID authentication framework by 30 June 2021*[121].

Adicionalmente la FCC también ha realizado consultas públicas, para adoptar medidas adicionales tendientes a combatir la suplantación ilegal de identidad.

9.7. India

En el año 2018, la Autoridad de Regulación de Telecomunicaciones de la India (TRAI, por sus siglas en inglés) expidió el Reglamento de Preferencias del Cliente en las Comunicaciones Comerciales de Telecomunicaciones. Este reglamento tiene por objetivo proteger a los usuarios de los servicios de telecomunicaciones móviles de recibir comunicaciones comerciales no solicitadas (*Unsolicited Commercial Communications* o UCC)[122].

Este reglamento establece que los usuarios de las redes móviles únicamente deben recibir comunicaciones comerciales deseadas y en consecuencia establece las condiciones para que los operadores de redes móviles envíen dichas comunicaciones de acuerdo con las configuraciones realizadas por sus clientes. Cualquier comunicación puede considerarse UCC si es recibida por un destinatario equivocado.

[121] Información extraída del documento *FCC mandates voice service providers to implement the STIR/SHAKEN caller ID authentication framework by 30 June 2021*; Cullen International; 16 de abril de 2020.
[122] Información extraída del documento disponible en el siguiente vínculo: https://trai.gov.in/tcccpr

De acuerdo con esta normativa cada persona, sea natural o jurídica, deberá registrarse ante los operadores de servicios móviles con el fin de que se les asigne un código de identificación alfanumérico de máximo once caracteres, denominado «encabezado».

Por su parte, con el fin de gestionar y administrar el envío de comunicaciones comerciales, los operadores de servicios móviles deben desarrollar un ecosistema que permita:

- Registrar, configurar y consentir el recibo de comunicaciones comerciales, por parte de sus suscriptores;
- Registrar a las entidades que deseen realizar actividades de telemarketing, donde se incluyan sus funciones y responsabilidades frente al envío de comunicaciones comerciales;
- Registrar a los remitentes de comunicaciones comerciales, verificando su identidad;
- Definir los procesos para el envío de comunicaciones comerciales por parte de los remitentes registrados;
- Definir los procesos y funciones de cada entidad con respecto a las comprobaciones que deben realizar antes del envío de comunicaciones comerciales y garantizar el cumplimiento normativo;
- Proporcionar a sus suscriptores las herramientas necesarias para presentar quejas contra los remitentes de comunicaciones comerciales, llevando registros del estado de resolución de las quejas;
- Responder las quejas, tomando las acciones del caso contra los infractores y adoptando las medidas correctivas para garantizar el cumplimiento de la normativa;
- Detectar, identificar y tomar las acciones que correspondan contra los remitentes de comunicaciones comerciales que no estén registrados;

De acuerdo con este reglamento, los proveedores de servicios móviles deben garantizar que cualquier comunicación comercial que se curse por su red se realice únicamente mediante los encabezados asignados a los remitentes. En consecuencia, los abonados que no estén registrados con algún proveedor de servicios móviles para el envío de mensajes con propósito comercial no podrán enviar este tipo de comunicaciones. En los casos donde abonados no registrados realicen envíos de comunicaciones comerciales podrán ser sancionados, incluso con la cancelación del contrato mediante el cual se les prestan los servicios móviles.

La normatividad también establece que los proveedores de servicios móviles tienen las siguientes obligaciones:

- Asegurar que los destinatarios de mensajes únicamente reciban las comunicaciones comerciales a las que hayan dado su consentimiento;
- Garantizar que por sus redes únicamente se realicen comunicaciones comerciales que cuenten con los encabezados autorizados y asignados a los remitentes registrados para tal fin;
- Entregar toda la información con los procedimientos para que sus clientes puedan registrarse y configurar cuales comunicaciones comerciales desean recibir o si desean recibirlas;
- Asegurar la confidencialidad, integridad y disponibilidad de los registros y datos almacenados dentro de la plataforma utilizada para gestionar y administrar el envío y recepción de comunicaciones comerciales.

Con respecto a mensajes provenientes de países extranjeros, el reglamento establece que los proveedores de servicios móviles y los operadores de servicios de telecomunicaciones de larga distancia no deben cursar por sus redes SMS con encabezados alfanuméricos o que tengan un código de país

+91. Adicionalmente, la TRAI se reservó el derecho de adoptar disposiciones adicionales con el fin de controlar SMS masivos provenientes del extranjero.

El incumplimiento de las disposiciones normativas relacionadas con las UCC podrá acarrear sanciones económicas a los proveedores de servicios de comunicaciones móviles, las cuales serán impuestas por la TRAI.

La implementación de esta normatividad por parte de los proveedores de servicios móviles tuvo algunas dificultades, por lo que la TRAI expidió el 20 de enero de 2020 una directiva que prorrogaba hasta el mes de febrero de 2020 la entrada en vigor de las disposiciones contenidas en la mencionada directiva.

9.8. Irlanda

De acuerdo con la Comisión para la Regulación de las Comunicaciones de Irlanda (ComReg), durante el periodo comprendido entre marzo de 2023 y marzo de 2024, el 91% de los clientes móviles recibieron llamadas o mensajes de texto provenientes de estafadores, causado perjuicios por más de EUR 300 millones a las víctimas de estos delitos[123].

Uno de los principales métodos utilizados por los delincuentes para realizar sus estafas es la suplantación de la identidad del llamante (*Spoofing*), la cual se realiza mediante la manipulación del "Número de Presentación", dato incluido dentro de la funcionalidad de Identificación de la Línea Telefónica Llamante (CLI). El Número de Presentación corresponde al número que puede ser visto por la parte llamada para identificar a la persona llamante.

Otro de los métodos utilizados por los estafadores para cometer fraudes consiste en suplantar la identidad (ID) de las organizaciones o empresas que envían mensajes de SMS utilizando una identificación de remitente alfanumérica, engañando a los receptores de estos mensajes haciéndoles creer que el mensaje es verdadero y confiable.

En el año 2023 ComReg lanzó una consulta pública con una la propuesta normativa para combatir las llamadas y mensajes de texto fraudulentos[124]. Como resultado de estas consultas, ComReg adoptó las siguientes decisiones regulatorias con el fin de combatir las llamadas y SMS fraudulentos:

- **Listados de No Originación (*Do-not-originate list* o DNO)**

  De acuerdo con las medidas regulatorias adoptadas, ComReg administrará la lista de No Originación (DNO) consistente en una base de datos con los números desde los cuales nunca se realizan llamadas salientes y por lo tanto si se detecta una llamada originada desde estos números, esta debe ser bloqueada.

  La norma obliga tanto a los operadores de servicios de telecomunicaciones de voz que cursan llamadas locales como a los operadores de llamadas internacionales a:

[123] Información extraída del documento *ComReg adopts measures to combat scam calls and SMS*; Cullen International; 12 de abril de 2024.
[124] Información extraída del documento disponible en el siguiente vínculo: https://www.comreg.ie/publication/combatting-scam-calls-and-texts-response-to-consultation-on-network-based-interventions-to-reduce-the-harm-from-nuisance-communications

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Bloquear todas las llamadas donde el Identificador de la Línea Llamante (CLI) indique que están siendo realizadas desde un número listado en la DNO;
- Actualizar sus sistemas de bloqueo en un término de cinco días hábiles siguientes a la recepción de la actualización de la DNO enviada por ComReg; y
- Registrar la cantidad diaria de llamadas bloqueadas y completadas, remitiendo esta información al ComReg en los Informes mensuales que el operador debe presentar dentro de los diez días hábiles siguientes a la finalización del mes de reporte.

- **Números Protegidos**

La ComReg administrará la lista de números protegidos, los cuales no han sido asignados a los operadores. Las llamadas cuyo CLI indica que la llamada se origina desde un número perteneciente a esta la lista deben ser bloqueadas.

La norma obliga tanto a los operadores de servicios de telecomunicaciones de voz que cursan llamadas locales como a los operadores de llamadas internacionales a:

- Bloquear las llamadas donde el Identificador de la Línea Llamante (CLI) indique que están siendo realizadas desde un número protegido;
- Actualizar sus sistemas de bloqueo, en un término de cinco días hábiles siguientes a la recepción de la actualización de la lista de números protegidos enviada por Comreg; y
- Registrar la cantidad diaria de llamadas bloqueadas y completadas, remitiendo esta información al ComReg en los Informes mensuales que el operador debe presentar dentro de los diez días hábiles siguientes a la finalización del mes de reporte.

- **Bloqueo a CLI con números fijos**

Los operadores de servicios de voz que cursan llamadas internacionales deben bloquear las llamadas que se originan desde el extranjero cuyo CLI indica que son originadas por un número fijo geográfico o no geográfico de Irlanda.

Bajo estas directrices los operadores de servicios de voz que cursan llamadas internacionales deben:

- Bloquear las llamadas internacionales entrantes cuyo Número de Presentación del CLI indique que están siendo realizadas desde un número fijo irlandés;
- No bloquear las llamadas internacionales entrantes donde la parte llamada corresponde a un número de itinerancia asignado a una estación móvil (*Mobile Station Roaming Number* o MSRN);
- No bloquear las llamadas internacionales entrantes donde el Número de Presentación del CLI es un número de Irlanda dentro del rango del bloque de numeración asignado para aplicaciones Máquina a Máquina (*Machine-to-Machine* o M2M); y
- Registrar la cantidad diaria de llamadas bloqueadas y completadas, remitiendo esta información al ComReg en los Informes mensuales que el operador debe presentar dentro de los diez días hábiles siguientes a la finalización del mes de reporte.

Los operadores internacionales que también son proveedores de servicios móviles deben informar a la ComReg, con tres meses de anticipación, cualquier cambio en los rangos de numeración de las MSRN.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- **Bloqueo a CLI con números móviles**

  Esta medida tiene como objetivo identificar y bloquear llamadas fraudulentas originadas en redes internacionales y cuyo Número de Presentación del CLI corresponda a un móvil irlandés, con excepción que el numera corresponda al asignado a una persona que se encuentra en el extranjero.

  Bajo estas directrices los operadores que cursan llamadas internacionales (*International Gateway Operators* o IGOs) deben:

  - Bloquear las llamadas internacionales entrantes cuyo Número de Presentación del CLI indique que están siendo realizadas desde un número móvil irlandés que no se encuentre en Itinerancia internacional;
  - No bloquear las llamadas internacionales entrantes si el usuario del número móvil se encuentra en itinerancia internacional;
  - No bloquear las llamadas internacionales entrantes donde la parte llamada corresponde a un número de itinerancia asignado a una estación móvil (*Mobile Station Roaming Number* o MSRN);
  - No bloquear las llamadas internacionales entrantes donde el Número de Presentación del CLI es un número de Irlanda dentro del rango del bloque de numeración asignado para aplicaciones Máquina a Máquina (*Machine-to-Machine* o M2M); y
  - Registrar la cantidad diaria de llamadas bloqueadas y completadas, remitiendo esta información al ComReg en los Informes mensuales que el operador debe presentar dentro de los diez días hábiles siguientes a la finalización del mes de reporte.

  Los operadores internacionales tienen la obligación de establecer si el usuario del número móvil se encuentra en itinerancia internacional, verificando esta información con el proveedor de servicios móviles del usuario. Para lleva a cabo esta verificación los proveedores de servicios móviles deben:

  - Proporcionar una función de verificación de itinerancia;
  - Informar a la ComReg, con tres meses de anticipación, cualquier cambio en los rangos de numeración de las MSRN; e
  - Implementar el servidor proxy de itinerancia.

- **Cortafuegos (*Firewall*) de voz**

  Otra de las medidas adoptadas por ComReg consiste es obligar a los proveedores de servicios de voz a implementación cortafuegos (*Firewall*) de voz, para establecer patrones utilizados para realizar estafas. Por medio de estos cortafuegos se realizan análisis avanzados de datos en tiempo real, aprendizaje automático e inteligencia artificial para detectar y actuar sobre patrones inusuales presentes en los datos de señalización de las llamadas y sobre volúmenes inusuales de tráfico.

  Bajo estas directrices los operadores de servicios móviles y fijos que originar y terminar una llamada de voz en una red pública y que tengan más de 330.000 abonados deberán:

  - Implementar un cortafuegos de voz para identificar las llamadas de voz que tengan una probabilidad de ser una llamada fraudulenta;
  - Boquear las llamadas de voz que tengan una muy alta probabilidad de ser una llamada fraudulenta;

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Realizar seguimiento a las llamadas de voz con probabilidades de corresponder a llamada fraudulenta y realizar recategorizaciones a partir de los patrones encontrados;
- Registrar la cantidad diaria de llamadas bloqueadas y completadas, remitiendo esta información al ComReg en los Informes mensuales que el operador debe presentar dentro de los diez días hábiles siguientes a la finalización del mes de reporte.

- **Registro de Identificación (ID) de Remitentes**

Con el fin de combatir la suplantación de la identidad (ID) de SMS por organizaciones o empresas legítimamente constituidas y permitir a los usuarios finales una identificación inequívoca del remitente del mensaje, la ComReg ha adoptado una medida basada en un registro de ID de Remitente. Esta medida aplica a:

- Proveedores de Servicios Móviles (*Mobile Service Pro*vider o MSP) que tengan más de 270.000 abonados (sin incluir abonados de M2M y banda ancha móvil), quienes se deben registrar ante el ComReg como MSP participantes; y
- Agregadores de SMS que transmiten o reenvían ID de remitentes de SMS asignados a un número irlandés, quienes se deben registrarse ante el ComReg como agregadores participantes.

La administración del registro de ID de Remitente estará a cargo de ComReg y contendrá los Propietarios de ID de Remitente (*Sender ID Owners* o SIDOs) con el respectivo ID asignado, los agregadores participantes y otros datos relevantes.

Para la implementación de esta medida la ComReg definió un período de transición, entre el 28 de junio al 28 de septiembre de 2025, donde los MSP y agregadores participantes solamente podrán catalogar los ID de Remitente sospechosos de suplantación como "*LikelyScam*", en lugar de bloquear los SMS. Después del 28 de septiembre de 2025, las MSP y agregadores participantes deberán bloquear todos los SMS con un ID de remitente que:

- No sea un ID de remitente registrado; o
- Sea un ID de remitente registrado, pero enviado por una fuente distinta a la permitida.

Para un MSP una fuente permitida puede ser otro MPS participante o un agregador participante. Para un agregador participante las fuentes permitidas pueden ser otro agregador participante o un Propietario de ID de Remitente (SIDO) registrado con el cual se tenga una conexión directa y cuyo ID se haya autenticado de manera segura.

Los MSP participantes deben bloquear el ID del remitente de SMS no registrados, excepto para los enviados a:

- Visitantes en Irlanda que estén en itinerancia; y
- Usuarios irlandeses en itinerancia en otro país, siempre que sea técnicamente viable.

Todas las empresas deben registrar diariamente la cantidad de SMS con ID del remitente destinados a números irlandeses, discriminando los bloqueados y no bloqueados, y presentar informes mensuales a ComReg.

Adicionalmente, los MSP deben bloquear cualquier SMS remitido desde un número irlandés (fijo, móvil o corto) cuando su entrega se realice desde un centro de SMS (SMS *Center* o SMSC) que no sea operado por un MSP irlandés.

9.9. Jordania

La Comisión de Telecomunicaciones y Regulación de Jordania (TRC) adoptó el 10 de junio de 2021 el reglamento para el envío de SMS masivos. El reglamento establece que las empresas que realicen envíos de SMS masivos deben estar autorizadas por la TRC, así como las condiciones regulatorias que deben cumplir tanto este tipo de compañías como los operadores de telecomunicaciones que gestionan y cursan este tipo de tráfico. Esta autorización aplica para empresas jordanas y extranjeras y tienen una vigencia de un año, la cual debe renovarse anualmente.

Para establecer las condiciones del envió los SMS se clasifican en dos categorías:

1. SMS Publicitarios: Corresponden a mensajes enviados para promocionar productos o servicios comerciales, independientemente de su remitente o destinatario. Para este tipo de SMS aplican las siguientes condiciones:

    - Debe comenzar con las siglas «ADV», seguidas de la Identificación (ID) del remitente.
    - Por medio de los datos del servicio USSD, el proveedor de servicios móviles debe garantizar[125] que los suscriptores tengan un mecanismo que les permita dejar de recibir SMS publicitarios.
    - No se deben enviar SMS publicitarios entre las 9:00 p.m. y las 7:00 a.m., ni los fines de semana ni los días festivos, a menos que la TRC lo autorice.
    - Solo se puede enviar un número limitado de SMS por día a un suscriptor móvil. Este número es definido por la TRC.

2. SMS de Servicios: Corresponden a mensajes que se envían a un segmento específico de destinatarios con el objetivo es prestar un servicio y no incluyen contenido publicitario. A este tipo de mensajes les aplican las siguientes condiciones:

    - Debe comenzar con las iniciales que representan el tipo de servicio, seguidas del nombre del remitente. La TRC publicó una lista con las iniciales asociadas a diferentes servicios, la cual puede ser modificada para incluir iniciales de nuevos servicios.
    - El proveedor de SMS masivos debe proteger los datos de remitentes y destinatarios debe cumplir con la normatividad de protección de datos personales y en consecuencia no debe explotarlos ni compartirlos con terceros.
    - No existen restricciones horarias para el envío de este tipo de mensajes.

Por último, el reglamento establece que las entidades del orden gubernamental no están obligadas a cumplir con esta normatividad.

[125] USSD: Unstructured Supplementary Service Data.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

9.10. Malasia

De acuerdo con reportes publicados por la Comisión de Comunicaciones y Multimedia de Malasia (MCMC) los principales impactos de los ciberdelitos sobre la población malaya son los siguientes:

- Se estima que más de 100.000 niños corren el riesgo de ser víctimas de explotación y manipulación sexual en línea.
- Entre los años 2019 y 2022 se duplicaron las transacciones sospechosas asociadas con los juegos de azar en línea, alcanzando un total de más de 42.000 transacciones. El valor de estas transacciones también aumentó superando los USD 5.500 millones, representando un aumento del 273% durante el mencionado periodo.
- De acuerdo con un informe de la UNICEF, el 28% de los niños malasios han sido víctimas de violencia o ciberacoso en línea; adicionalmente, según reportes del MCMC este organismo recibió 9.483 denuncias de ciberacoso entre enero de 2022 y julio de 2024.
- Los casos de fraude en línea en Malasia han aumentado, pasando de 17.668 casos en 2019 a 34.495 en 2023. Adicionalmente las pérdidas totales derivadas de las estafas ascendieron a USD 295,95 millones en 2023.

Con el fin de hacer frente a estas problemáticas, el 1 de agosto de 2024 la MCMC expidió un marco regulatorio dirigido a los proveedores de servicios de mensajería por internet y redes sociales, donde se establecía que los proveedores de servicios, que contaran con al menos 8 millones de usuarios en Malasia, debían solicitar a la MCMC una licencia de Proveedor de Servicios de Aplicaciones (*Applications Service Provider class licence* o ASP (C) *licence*). De manera general, los principales proveedores de servicios de aplicaciones como Facebook, Facebook Messenger, Instagram, TikTok, WhatsApp, Telegram, WeChat, X y YouTube, quedaron obligados a cumplir con este requisito[126]. La norma estableció que su entrada en vigor sería a partir del 1 de enero de 2025.

Desde la fecha de expedición hasta su entrada en vigor, la MCMC realizó una consulta pública para reglamentar las directrices y obligaciones que deberían cumplir los proveedores de servicios de aplicaciones obligados a tramitar y obtener la licencia. Dentro de las obligaciones propuestas se encontraban las siguientes:

- Políticas y medidas para la protección de datos de los usuarios.
- Medidas de seguridad infantil, incluyendo garantías de edad para restringir el acceso de los usuarios menores de 13 años a las plataformas operadas por los proveedores de servicios.
- Políticas y medidas para abordar los daños en línea, incluyendo el ciberacoso, las estafas en línea y las actividades de captación de menores con fines sexuales.
- Políticas y medidas de moderación de contenido.
- Transparencia publicitaria y restricción de anuncios que promuevan estafas.
- Medidas para proteger a los menores de contenido dañino y publicidad engañosa.
- Medidas para simplificar los procedimientos de queja para los usuarios y reducir el tiempo de respuesta.
- Medidas para gestionar deepfakes y contenido dañino generado por inteligencia artificial (IA).

[126] Información extraída del documento *Malaysia introduces mandatory licensing for internet messaging and social media service providers*; Cullen International; 26 de agosto de 2024.

- Presentación de informes periódicos por parte de los Proveedor de Servicios de Aplicaciones donde reporten el estado del cumplimiento de las leyes y los requisitos de conducta de Malasia.

Con la entrada en vigor de la obtención la ASP (C) *licence*, se obligó a los proveedores de servicios de aplicaciones a cumplir con la Ley de Comunicaciones y Multimedia (*Communications and Multimedia Act* o CMA), y sus respectivas normativas reglamentarias, así como con los códigos de consumo registrado bajo la CMA y la Ley de Protección de Datos Personales.

En Malasia a las licencias de clase les aplica una normativa flexible, orientada promover el crecimiento y el desarrollo de la industria. Para solicitar una ASP (C) *licence*, los proveedores de servicios de aplicaciones constituidos en Malasia deben realizar un pago de registro y presentar los documentos requeridos que incluyen, entre otros aspectos, un formulario de solicitud, descripción del perfil de la empresa e información sobre el servicio que se está prestando. Igualmente, la regulación malaya establece que uno de los requisitos para solicitar cualquier tipo de licencia, consiste en que las organizaciones se constituyan legalmente en el país, sin embargo, la normatividad también estableció que la MCMC cuenta con la discrecional de permitir que una empresa extranjera, sin sede en el país, se le pueda otorgar una licenciataria de clase, previo estudio del caso. Las licencias de clase otorgadas a los proveedores de servicios de aplicaciones tienen una vigencia de un (1) año, la cual debe ser renovada a su vencimiento.

Adicionalmente, la normatividad establece que a partir del 1 de enero de 2025 los proveedores de servicios de aplicaciones cobijados por esta medida, serán objeto de sanciones si:

- Prestan servicios sin tramitar la ASP (C) *licence*; y
- Habiendo tramitado la licencia, incurren en incumplimientos a las obligaciones establecidas en la normatividad.

Las sanciones abarcan desde una advertencia administrativa hasta la suspensión del acceso a la plataforma del proveedor de servicios de aplicaciones, o la revocación del registro de ASP (C) *licence* y acciones penales.

De acuerdo con algunos reportes, el Ministerio de Comunicaciones de Malasia afirmó que las plataformas de redes sociales han respondido positivamente a la necesidad de licencias para garantizar un uso más seguro de Internet por parte de los niños y las familias, sin embargo, algunas organizaciones de la sociedad civil afirman que esta normatividad es autoritaria y amenaza la libertad de expresión. Algunos economistas también sostienen que regular las redes sociales puede ser perjudicial para las empresas.

9.11. Polonia

EL 28 de julio de 2023, el ente Regulador de las Comunicaciones (UKE) y el Instituto Nacional de Investigación (NASK) de Polonia expidieron la Ley Contra el Abuso de las Comunicaciones Electrónicas. Con esta ley se adoptaron medidas contra *Smishing* (envío de SMS donde el remitente suplanta la identidad de una entidad con fines de engañar o estafar al receptor) y la suplantación de la Identificación de la Línea Telefónica Llamante (*Calling Line Identification* o CLI)[127].

[127] Información extraída del documento "*CEE Telecoms Update*"; Cullen International; 30 de septiembre de 2023

La normativa expedida estableció que el Grupo de Respuesta a Incidentes de Seguridad Informática del Instituto Nacional de Investigación de Polonia (CSIRT NASK) será el organismo encargado de controlar y prevenir el *Smishing*, a partir de la implementación de una plataforma informática que permitirá la definición de patrones presentes en los SMS fraudulentos. Para la definición de estos patrones, tanto los usuarios como los operadores de servicios de telecomunicaciones móviles, podrán reportar SMS maliciosos con los que se pretenden realizar estafas. Estos reportes pueden ser enviados a la CSIRT NASK por medio de un número abreviado gratuito establecido en la norma[128]. También se obliga a los Operadores de Redes Móviles realizar la identificación y el bloqueo automático de SMS considerados como *Smishing*.

Estas medidas igualmente contemplan que el CSIRT NASK mantenga disponible en su sitio web una lista con los nombres y abreviaturas reservadas a entidades públicas para permitir el bloqueo de mensajes que suplantan sus identidades, así como las variantes de nombres y abreviaturas que puedan inducir a error al destinatario del mensaje. La norma también establece que el encabezado de los mensajes enviados por las entidades públicas debe finalizar con los caracteres «#RP», prohibiendo su uso por parte otro tipo de organizaciones.

Con respecto a las medidas adoptadas para combatir la suplantación de la Identificación de la Línea Telefónica Llamante, la norma establece que los operadores de servicios de telecomunicaciones tendrán la obligación de bloquear las llamadas de voz que ocultan su identificación en el CLI. Asimismo, establece que la UKE mantendrá una lista de números utilizados para recibir llamadas de voz la cual será publicada en su sitio web.

9.12. Portugal

La Autoridad Nacional de las Comunicaciones (ANACOM), ente regulador de las comunicaciones de Portugal, ordenó a las empresas que ofrecen servicios de acceso a Internet o servicios de comunicaciones interpersonales basados en números públicos, permitir la presentación de la identificación de la línea llamante. Esta medida aplica, para llamadas y mensajes provenientes de otros países. Adicionalmente, determinó que las empresas que ofrecen servicios de comunicaciones interpersonales basados en números y operadores públicos deberían adoptar las medidas técnicas pertinentes para garantizar la integridad de los datos de identificación de la línea llamante, a fin de evitar que el número o recurso asociado a la identificación de la línea llamante o del remitente de un mensaje sea suplantado[129].

Para los casos en que no se envíe la identificación de la línea llamante o no se evidencia que esta información no sea válida, la llamada no deberá ser cursada.

9.13. Reino Unido

Para el año 2021 se estima que en el Reino Unido las víctimas de crímenes relacionados con fraude perdieron £2.35 mil millones en 2021 y para el año 2022 este tipo de delitos representaba más del 40%

[128] Información extraída del documento disponible en el siguiente vínculo: https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm
[129] Información extraída del documento "*Início de procedimento de elaboração de um regulamento relativo à identificação da linha chamadora e do remetente de uma mensagem*"; Autoridade Nacional de Comunicações; 21 de marzo de 2023

de los crímenes cometidos en Inglaterra y Gales. Asimismo, en el año 2022, uno (1) de cada quince (15) adultos fue víctima de fraude y el 18 % de las víctimas lo fue en más de una ocasión[130].

Entre los años 2019 y 2020, el costo total de los delitos relacionados con fraude en Inglaterra y Gales se estimó en al menos £6.800 millones, el cual incluye el dinero perdido por las víctimas, el coste de su atención y los costes de recuperación, investigación y enjuiciamiento de los estafadores.

Entre los meses de marzo de 2020 y 2021, las víctimas por este tipo de delitos reportaron pérdidas totales que ascendían a £2.350 millones. Por otra parte, la Encuesta de Delitos Económicos estimó que para el año 2020, el 18% de empresas había sido víctima de fraude durante los últimos tres años. Igualmente, para este mismo periodo, mediante la encuesta sobre delincuencia en Inglaterra y Gales (*Crime Survey for England and Wales* o CSEW), se pudo establecer que ocurrieron más de 250.000 incidentes de fraude, de los cuales el 36 % no generaron pérdidas financieras (intentos de fraude que no fueron exitosos) [131].

Otra problemática identificada en el Reino Unido con respecto a este tipo de delitos está relacionada con la forma cambiante en que los delincuentes cometen las estafas. Históricamente, la principal forma de fraude eran estafas no autorizadas, realizadas por medio de bancos y tarjetas de crédito, donde los estafadores extraían el dinero de las cuentas bancarias de las víctimas sin su autorización o conocimiento. Con la mejora en los controles implementados por los bancos para prevenir este tipo de fraude, impulsados también por los avances tecnológicos, los delincuentes han adoptado técnicas mediante las cuales persuaden o convencen a las víctimas para que autoricen transacciones monetarias o pagos. De acuerdo con los reportes recibidos por el Centro Nacional de Reportes de Fraude (*Action Fraud*), entre los meses de marzo de 2020 y 2021, en promedio, las pérdidas sufridas por cada una de las víctimas que voluntariamente aprobaban una transferencia o pago ascendían a casi £3.000[132].

Estos delitos conllevan también un costo considerable para las empresas. La asociación comercial del sector bancario y financiero del Reino Unido (UK Finance), estimó que en el año 2021 sus miembros perdieron más de £1.300 millones por fraude, acarreando en consecuencia un aumento en los costos de prestación de servicios financieros[133].

Además de las pérdidas económicas que conllevan este tipo de delitos, a partir de los resultados de la CSEW, se pudo establecer que aproximadamente el 25% de las personas que fueron víctimas de estafas entre los meses de marzo de 2019 y 2020, experimentaron algún tipo de impacto emocional. En este mismo sentido, el Centro Nacional de Reportes de Fraude (*Action Fraud*) estimó que, en más de 300 llamadas recibidas por víctimas de este tipo de delito, podían estar catalogadas en riesgo de suicidio[134].

Uno de los principales vectores del incremento de los delitos relacionados con estafas, identificado en el Reino Unido, es el desarrollo tecnológico y la adopción de nuevas tecnologías por parte de consumidores, empresas y de los mismos estafadores, permitiéndoles a estos últimos tener un mayor acceso a las víctimas y a los datos, en consideración a los siguientes factores:

---

[130] Información extraída del documento disponible en el siguiente vínculo: https://www.gov.uk/government/publications/fraud-strategy/fraud-strategy-stopping-scams-and-protecting-the-public
[131] Ibid.
[132] Ibid.
[133] Ibid.
[134] Ibid.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- A medida que se almacenan más datos en línea, las filtraciones de datos a gran escala permiten a los estafadores acceder y utilizar información personal robada para cometer sus fraudes;
- La disponibilidad de comunicaciones masivas, tales como los servicios de mensajería de texto, permiten a los estafadores dirigirse a miles de personas a la vez. La suplantación de números permite a los estafadores hacerse pasar por un número o empresa legítima y engañar a las personas para que respondan llamadas que, de otro modo, podrían ignorar;
- La aparición y el desarrollo de la inteligencia artificial y herramientas inteligentes de aprendizaje automático, permite a los estafadores dirigir y adaptar sus estafas para que sean más efectivas.

Estos avances tecnológicos también han permitido que la mayoría de los fraudes que se perpetran actualmente en el Reino Unido, se realicen por medio de las plataformas en línea, tales como las redes sociales, siendo los mensajes la forma más común de contacto de los estafadores con sus víctimas. Los avances también han permitido a los estafadores el desarrollo de nuevos métodos de fraude al presentar personas o información falsa de una manera que resulta imposible distinguirla de la real. Un estudio realizado por el organismo que regula las telecomunicaciones en el Reino Unido (Ofcom), encontró que más de 40 millones de adultos fueron víctimas de al menos un mensaje de texto o una llamada fraudulenta sospechosa en tan solo tres meses de 2022 y, por su parte, la organización británica Citizens Advice ha estimado que cada 2 de 3 adultos han sido víctimas de fraudes en línea en el Reino Unido.

Con el fin de hacer frente a este flagelo, en el año 2023, el Reino Unido lanzó la Estrategia Antifraude (*Fraud Strategy*) que establece acciones coordinadas que deben desarrollarse entre el gobierno, las fuerzas del orden, los reguladores, la industria y las organizaciones benéficas para reducir en un 10%, al finalizar el periodo parlamentario, los incidentes relacionados con fraudes con respecto a los niveles previos a la pandemia de Covid-19. Para su implementación esta estrategia se centra en tres elementos clave[135]:

1. **Perseguir a los Estafadores:** Consistente en desarticular sus actividades y llevarlos ante la justicia con mayor frecuencia y rapidez mediante el desarrollo de las siguientes acciones:

   - Establecer un Escuadrón Nacional Antifraude (National Fraud Squad), incorporando 400 investigadores especializados en este tipo de crímenes;
   - Crear una nueva Unidad de Inteligencia Antifraude;
   - Reemplazar el Centro Nacional de Reportes de Fraude (Action Fraud) por un sistema de reporte antifraude con tecnología de punta;
   - Encarcelar más defraudadores;
   - Liderar la cooperación a nivel internacional para perseguir a los defraudadores en todo el planeta impulsando una mayor cooperación internacional, creando grupos de trabajo conjuntos que permitan enfrentar el flagelo del fraude, fortaleciendo las relaciones con otros países para emprender acciones conjuntas contra los estafadores, la comprensión compartida de la naturaleza y el alcance de los fraudes, la identificación de las mejores prácticas para prevenir y responder al fraude de manera articulada y la propuesta de desarrollar un plan de acción coordinado para desmantelar las redes que cometen este tipo de crímenes.

[135] Ibid.

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

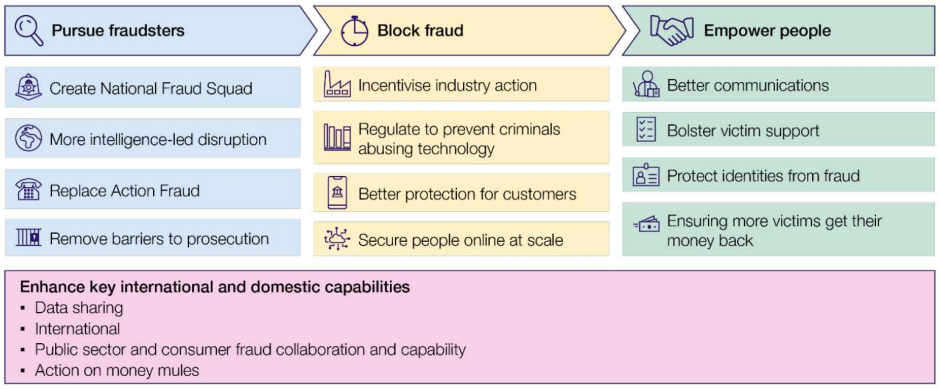
2. **Bloquear los Fraudes:** Centrándose en la reducción de la cantidad de comunicaciones relacionadas con fraude y estafa que llegan a la población en general, ejecutando las siguientes estrategias:

   - Designar a un líder de lucha contra el fraude;
   - Parar el abuso de las redes de telecomunicaciones por parte de los criminales mediante: (i) La prohibición de llamadas no solicitadas relacionadas con productos financieros; (ii) La prohibición de Granjas SIM; (iii) Revisión del uso de agregadores de texto masivos (o plataformas de SMS masivos); y (iv) Detener la suplantación de identidad en las llamadas.

3. **Empoderar a las Personas:** Desarrollando estrategias y herramientas que les permitan a las personas reconocer, evitar, denunciar y manejar situaciones fraudulentas de una manera más fácil y apropiada, mediante la implementación de las siguientes acciones:

   - Apoyar a una mayor cantidad de víctimas de fraudes;
   - Implementar nuevas tecnologías y promover el desarrollo de normativas orientadas a disminuir el robo y la venta de datos y el robo de la identidad digital de los ciudadanos. Estas normativas deben estar orientadas a recuperar y restituir la identidad a los ciudadanos que han sido víctimas del robo de su identidad, el establecimiento de ordenanzas que restrinjan la creación y venta de identidades y a establecer el tratamiento que se le debe de dar a datos copiados u obtenidos mediante acceso no autorizado
   - Resarcir a una mayor cantidad de víctimas que hayan caído en estafas;
   - Expedición de normativas que impidan a los estafadores esconderse tras empresas falsas, donde se incluyan mejoras a la información solicitada en el registro mercantil y promover un mayor uso.
   - Mejorar las campañas de comunicación sobre cómo protegerse, reportar y qué hacer si la persona ha sido víctima de acciones fraudulentas.

Ilustración 22. Estrategia para Disminuir el Fraude en el Reino Unido



Fuente: Reducing scam calls from abroad which spoof UK mobile numbers[136].

Como se puede observar, una de las principales estrategias que está implementando el Reino Unido para hacer frente a este flagelo es implementar medidas que bloqueen el fraude. Esta estrategia

[136] Id.

contempla la ejecución de acciones coordinadas entre los actores que participan en diferentes sectores económicos, el gobierno, las fuerzas del orden y las entidades reguladoras y en particular la adopción de medidas regulatorias que impactan directamente al sector de las TIC. Dentro de las medidas adoptadas en el marco de esta estrategia se encuentran las siguientes[137]:

- La designación de un líder de lucha contra el fraude para que coordine las acciones y controles que se deben establecer para combatir el fraude, garantizando el trabajo conjunto y la colaboración entre los diferentes sectores sociales, económicos y gubernamentales.
- La suscripción voluntaria por parte de las empresas que prestan servicios de telecomunicaciones del Memorando de Telecomunicaciones, donde se comprometen a implementar soluciones de filtrado de SMS.
- La revisión continua del Memorando Contra el Fraude en Línea con las empresas del sector TIC, con el fin de establecer controles adicionales para enfrentar nuevas modalidades de fraude utilizando herramientas de inteligencia artificial y otros desarrollos tecnológicos utilizados por los estafadores para cometer sus delitos.
- Implementación de controles por parte de empresas del sector TIC para verificar y garantizar que las organizaciones que promocionan inversiones financieras estén registradas ante la Autoridad de Conducta Financiera (FCA).
- Promover y mejorar el intercambio de información (datos) entre el gobierno y los actores de los sectores financieros, de las Tecnologías de la Información y las Comunicaciones y otros sectores económicos para identificar y bloquear fraudes y, en la medida de lo posible, realizarlo en tiempo real.
- La adopción de medidas regulatorias orientadas a prevenir que los criminales usen las tecnologías para cometer fraudes, tales como:
  - Exigir responsabilidades a las empresas del sector TIC para reducir el fraude en línea e imponer multas a quienes no lo hagan, mediante la aprobación e implementación del Proyecto de Ley de Seguridad en Línea, obligando la implementación de sistemas que eviten la aparición de contenido fraudulento en plataformas de redes sociales y de servicios de búsqueda en internet.
  - Extender la prohibición de las llamadas no solicitadas a todos los productos financieros y de inversión. Actualmente, mediante la Ley de Orientación Financiera y Reclamaciones de 2018 (*Financial Guidance and Claims Act 2018*) se prohibieron las llamadas no solicitadas provenientes de firmas de abogados especializadas en daños personales a terceros[138] y proveedores de pensiones (a menos que el consumidor haya aceptado explícitamente ser contactado)
  - Prohibir las granjas de tarjetas SIM para dificultar el envío de mensajes de texto y la realización de llamadas fraudulentas.
  - Revisar el uso de agregadores de mensajes de texto masivos y revisar la implementación de un registro de los usuarios en estos servicios. En el Reino Unido, estos servicios son utilizados, entre otras, para reservas en restaurantes, recordatorios de citas y actualizaciones de pedidos, por lo cual se está realizando una revisión sobre el mercado para tomar medidas que disminuyan las cantidad de fraudes que se efectúan utilizando esta herramienta.
  - Bloquear las capacidades que utilizan los estafadores para falsificar números de teléfono del Reino Unido. Los delincuentes suelen falsificar sus números para ocultar su identidad

[137] Ibid.
[138] Firmas de abogados especializadas en representar a clientes que han sufrido algún tipo de accidente que involucra un tercero.

al llamar y enviar mensajes de texto a sus posibles víctimas, haciéndose pasar por una organización legítima, como bancos, agencias gubernamentales u otras organizaciones reconocidas por los usuarios. Ofcom revisa periódicamente las normas que obligan a los operadores que prestan servicios móviles a bloquear llamadas que suplantan números, de acuerdo con los avances tecnológicos y a futuro se espera que los operadores implementen un proceso para responder denuncias relacionadas con usos indebidos de numeración. Adicionalmente, Ofcom puso a consideración del sector de las telecomunicaciones, la normativa que obliga a los operadores a implementar la tecnología de autenticación de Identificación de Línea Llamante (CLI, por sus siglas en inglés) para que los prestadores de servicios de telefonía móviles y fijos puedan certificar la legitimidad del número utilizado para realizar una llamada.

- Implementar el Programa de Publicidad en Línea que tiene como fin evitar la materialización de fraudes y otros perjuicios por medio de servicios de telecomunicaciones. Esta iniciativa está a cargo del Departamento de Cultura, Medios de Comunicación y Deporte (DCMS), entidad que está preparando una serie de reformas legislativas y no legislativas que tienen como objetivo reducir los perjuicios causados por propaganda fraudulenta o maliciosa.

- Bajo la supervisión de los organismos reguladores, el sector financiero ha invertido recursos para incorporar nuevas tecnologías para mejorar la identificación y bloqueo de pagos sospechosos. Las principales iniciativas que se han puesto en marcha para ayudar a prevenir el fraude por parte de las entidades financieras son:

  - **Autenticación Reforzada del Cliente:** Cuando los clientes compran un producto o realizan un pago en línea, el Reglamento de Servicios de Pago exige que todos los Proveedores de Servicios de Pago (PSP) verifiquen la identidad de sus clientes con el fin de evitar que los estafadores realicen pagos no autorizados con datos de terceros.
  - **Confirmación del Beneficiario:** Este servicio le permite al pagador comprobar si el nombre del beneficiario coincide con los datos de la cuenta de la persona a la que cree estar enviando dinero.
  - **Protocolo Bancario:** Iniciativa del sector financiero, liderada por UK Finance, donde se capacita al personal bancario para detectar cuándo un cliente está a punto de ser víctima de un fraude autorizado y colaborar con la policía para convencerlo de que no realice el pago.

- Ampliar las competencias del Centro Nacional de Ciberseguridad (NCSC) para colaborar con instituciones financieras y empresas tecnológicas en la Identificación y eliminación de páginas web fraudulentas. Actualmente, el NCSC colabora con proveedores de servicios de internet y operadores de redes móviles para rastrear en internet sitios web maliciosos y compartiendo los hallazgos en tiempo real con organizaciones financieras y tecnológicas para reducir la cantidad de fraudes, permitiendo la eliminación de nombres de dominio y direcciones IP de sitios maliciosos.

De manera específica, el organismo que regula las telecomunicaciones en el Reino Unido (Ofcom) ha adoptado las siguientes medidas con para prevenir el fraude:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. Bloqueo de Llamadas Fraudulentas Mediante las Funcionalidades Identificación de la Línea Telefónica Llamante (CLI)

La implementación de este servicio ha permitido la adopción de medidas para disminuir las llamadas utilizadas por los estafadores para cometer fraudes. Como se mencionó anteriormente, una práctica común utilizada por los estafadores es suplantar los números de teléfono para ocultar el origen de la llamada o hacer que parezca provenir de una persona u organización de confianza. Para reducir la cantidad de estafas que realizan utilizando este método, el Reino Unido ha implementado las siguientes medidas[139]:

- Obligar a los operadores a bloquear números que no están destinados a realizar llamadas salientes y que están registrados en la lista de No Originar (*Do Not Originate* o DNO);
- Obligar a los operadores que identifiquen y bloqueen las llamadas desde el extranjero que suplanten un número de red fijo del Reino Unido; y
- Obligar a los operadores que apliquen la debida diligencia al sub-asignar números a otros operadores del Reino Unido.

Las dos primeras medidas corresponden a disposiciones y requerimientos establecidos sobre la funcionalidad de Identificación de la Línea Telefónica Llamante (*Calling Line Identification* o CLI). Para implementar la tercera medida se estableció una guía con el fin de que los proveedores de servicios de telecomunicaciones realicen verificaciones más exhaustivas al momento de entregar a un tercero la numeración que le ha sido asignada[140].

Las funcionalidades de Identificación de la Línea Telefónica Llamante proporcionan información sobre la identificación de la línea de la persona que realiza la llamada. La información contenida en el CLI incluye el punto de entrada a la red ("Número de Red") y puede contener el número de teléfono llamante que se muestra al destinatario de la llamada, el cual se denomina "Número de Presentación". En la mayoría de los casos, el Número de Red y el Número de Presentación son el mismo número. Los destinatarios de las llamadas ven el número de presentación cuando reciben una llamada. El Número de Red se comparte con los proveedores para identificar el origen de la llamada[141].

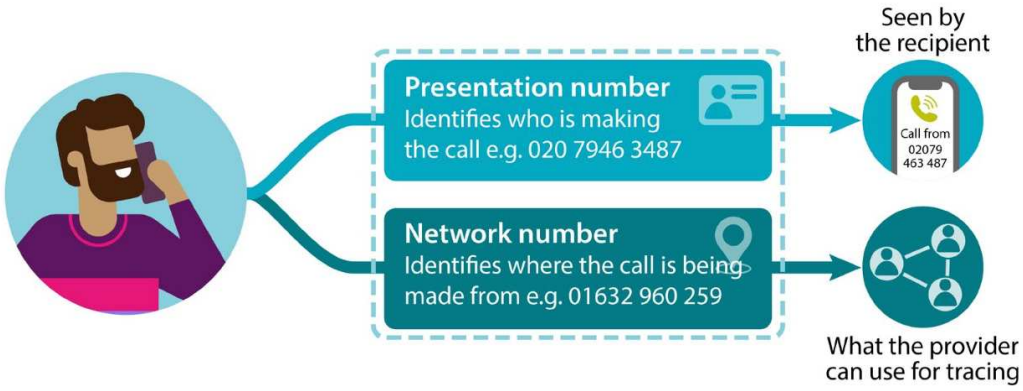
---

[139] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/186068-call-for-input-options-to-address-mobile-spoofing/associated-documents/cfi-reducing-scam-calls-from-abroad-which-spoof-uk-mobile-numbers.pdf?v=373415

[140] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/good-practice-guide-on-sub-allocated-assigned-numbers

[141] Extraído del documento disponible en el siguiente vínculo https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/improving-cli-data-accuracy

Ilustración 23. Número de Presentación y Número de Red



Fuente: Improving the accuracy of Calling LineIdentification (CLI) data[142]

Dentro de los datos contenidos en el CLI también se pueden incluir un campo opcional para mostrar el nombre del llamante. Adicionalmente, con el fin de dar cumplimiento a la normatividad relacionada con la protección de datos personales, el CLI contiene una marca de privacidad que indica si el número se puede compartir con el destinatario de la llamada, sin embargo, es importante notar que todas las personas que realicen llamadas de telemarketing se obligan a permitir la presentación de un número válido de la línea desde donde se origina la llamada[143].

Los requisitos de la visualización de los datos de Identificación de la Línea Telefónica se establecen en el documento Condiciones Generales de Titularidad (*General Conditions of Entitlement* o CG), expedido por Ofcom. De acuerdo con la normatividad establecida, se obliga a los proveedores de servicios de comunicaciones (*Call Providers* o CP), dependiendo de la viabilidad técnica y económica, a proporcionar los servicios de Identificación del Número Llamante. Esta norma también especifica que el CP se obliga a que el número incluido dentro del CLI debe corresponder a un número telefónico válido y que pueda ser marcado, permitiendo identificar de forma única al llamante. Cuando los CP identifiquen una llamada en la que los Datos CLI proporcionados no sean válidos, es decir no identifiquen de forma única al llamante o no contengan un Número de Teléfono que pueda ser marcado, exigen que el CP impida, siempre que sea técnicamente viable, que las llamadas se conecten al número marcado.

El Número de Red identifica el punto de entrada de la llamada y debe corresponder a un número asignado o portado al CP de origen cumpliendo con los formatos definidos en la Recomendación UIT-T E.164 y permitir la identificación de: (i) El punto de terminación de red (*Network Termination Point* o NTP); (ii) El suscriptor o terminal con acceso no fijo a una Red Pública de Comunicaciones; o (iii) El código del primer nodo conocido utilizado por la llamada al ingresar a las redes de comunicaciones del Reino Unido; cuando esta información no se encuentre contenida dentro del CLI o existan dudas sobre su veracidad, la marca de privacidad debe indicar que la presentación del número no está habilitada. Si el Número de Presentación incluido dentro del CLI corresponde a un número que pueda ser marcado por el usuario, no es necesario que el Número de Red sea un número que se pueda marcar.

[142] Id.
[143] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/phone-numbers/calling-line-identification

El Número de Presentación es el asignado la llamante y para su identificación y utilizarse para devolver la llamada. Si el usuario a la que se le ha asignado un número autoriza a varias personas a utilizarlo, se espera que mantenga un registro de las personas autorizadas a utilizarlo, para facilitar las solicitudes de rastreo de llamadas. Este número debe cumplir con las siguientes condiciones: (i) Debe ser un número válido; (ii) Debe ser un número que se pueda marcar; y (iii) Debe identificar de manera inequívoca a la persona que llama, sea esta un individuo o una organización. Por último, es importante señalar que, a diferencia de un Número de Red, un Número de Presentación no identifica necesariamente el punto de entrada de una llamada a una Red Pública de Comunicaciones.

Los datos del CLI se comparten entre los diferentes proveedores de servicios de comunicaciones (*Call Providers* o CP) que participan en la conexión de la llamada. Para que la información se comparta de forma fiable, es necesario que los datos de la línea telefónica llamante se proporcionen correctamente y que esta información se transmita guardando su integridad.

Siempre que sea técnicamente factible, los CP de tránsito deben garantizar que los datos de CLI sean válidos y que el CP de destino presente CLI válidos con números que puedan ser marcados por el usuario final.

Para las llamadas originadas en redes que se encuentran por fuera de la jurisprudencia del Reino Unido, la responsabilidad de verificar la validez de los datos CLI recae en el CP por donde ingresa la llamada a las Redes de Comunicaciones Públicas del Reino Unido Teniendo en cuenta lo anterior, este CP es responsable de tomar alguna de las siguientes acciones, según sea el caso:

- Bloquear las llamadas donde: (i) El Número Presentación no es válido o no se puede marcar; (ii) No se informe el Número de Presentación y el Número de Red falta o no sea válido, con excepción que se hayan reportado previamente causales técnicas que impidan la entrega de esta información.
- La llamada puede conectarse si el CP considera de manera fundada que es una llamada legítima siempre y cuando el CLI suministre un Número de Presentación válido a pesar de que el campo de Número de Red se encuentre vacío.
- Si la llamada contiene un Número de Presentación válido, pero el Número de Red se considera inválido por no cumplir con el plan de numeración de la recomendación UIT-T E.164, la llamada debe bloquearse, a menos que el CP esté investigando la causa por la cual el CLI está suministrando datos inválidos.
- Si la llamada se conecta a pesar de que existe un Número de Red inválido o inexistente, el CP debe insertar un CLI de un rango asignado para este fin como Número de Red e indicar en el campo correspondiente a la marca de privacidad que la presentación del número no está habilitada.

Sin perjuicio de lo anterior, estas medidas han sido insuficientes para prevenir la suplantación de números del Reino Unido por llamadas internacionales, debido a las excepciones contempladas para las llamadas provenientes del extranjero en el rango del bloque de numeración +44. Una de las razones de estas excepciones es permitir la presentación del número telefónico de los usuarios del Reino Unido que se encuentran en itinerancia en otros países. Actualmente, se están buscando soluciones técnicas para abordar esta problemática identificando a los usuarios legítimos de itinerancia para reducir y bloquear llamadas internacionales que suplantan números del Reino Unido. Para solucionar esta problemática se están contemplando dos opciones:

1. Que el proveedor encargado de cursar la llamada desde el exterior realice comprobaciones para determinar si un número desde donde se origina la llamada se encuentra en itinerancia.
2. Que el proveedor al que pertenece el nodo por donde entra la llamada internacional identifique las llamadas móviles procedentes del extranjero, modifique los datos asociados a dichas llamadas y las reenvíe a la red móvil local del llamante, donde pueden realizarse validaciones adicionales para verificar que el número se encuentre en itinerancia.

La prestación de este servicio les permite a los usuarios el rechazo de llamadas entrantes que no permitan la visualización de los datos contenidos en el servicio de Identificación de la Línea Telefónica. Este rechazo puede ser configurado de manera automática, cuando existan las condiciones técnicas que lo permitan, caso en el cual se debe notificar de manera gratuita al usuario llamante explicando que el motivo del rechazo de se debió a una restricción de CLI.

2. Reducción de Mensajes Móviles Fraudulentos

Otra de las herramientas utilizadas por los estafadores para cometer sus crímenes es el envío de mensajes por medio de las redes de servicios móviles. En el Reino Unido se han identificado principalmente tres medios utilizados por estafadores para realizar sus crímenes mediante mensajes: (i) Servicios de Mensajes Cortos de Texto, SMS (ii) Servicios de Comunicación Enriquecidos (*Rich Communications Services* o RCS); y (iii) Otras aplicaciones de mensajería, tales como WhatsApp, Signal, Telegram, entre otras[144].

Teniendo en cuenta que las aplicaciones de mensajería como *WhatsApp*, *Signal*, *Telegram*, aunque necesitan de un número teléfono para registrarse, no enrutan sus mensajes a través de las redes de telecomunicaciones utilizando el número asignado, estos servicios de comunicación en línea (*Online Communication Services* o OCS) quedan por fuera del alcance de las medidas que pueda tomar Ofcom para reducir las estafas que se realizan utilizando estas aplicaciones. Por el contrario, frente al envío de mensajes de SMS y RMS, este ente regulador ha tomado medidas para reducir el usufructo ilegal que realizan de los estafadores al aprovecharse de estos dos (2) servicios.

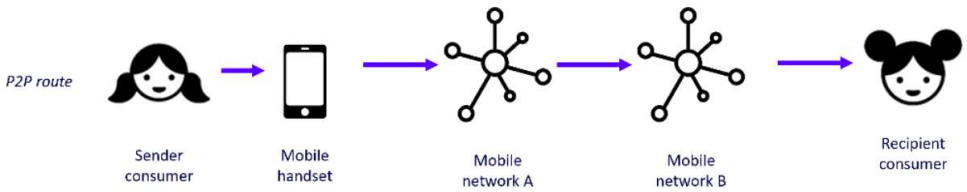
El servicio tradicional de mensajería de texto SMS en redes móviles está disponible para todos los usuarios móviles. Por su parte, el RCS es un servicio más reciente que busca modernizar los servicios prestados por SMS, incluyendo funcionalidades adicionales. Impedir el uso de RCS por parte de estafadores supone algunos desafíos nuevos en comparación con las medidas que se pueden tomar frente a los SMS.

Se han identificado principalmente dos (2) formas en que los estafadores envían información fraudulenta utilizando el servicio de SMS:

- **Mensajes de persona a persona (*Person-to-Person* o P2P):** Corresponden a los mensajes que se envían desde una tarjeta SIM a otra, por medio de redes móviles. Algunos ejemplos de uso típico incluyen el envío de mensajes entre familiares y amigos.

[144] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams

Ilustración 24. Diagrama con la forma en que son enviados los mensajes SMS en el esquema P2P

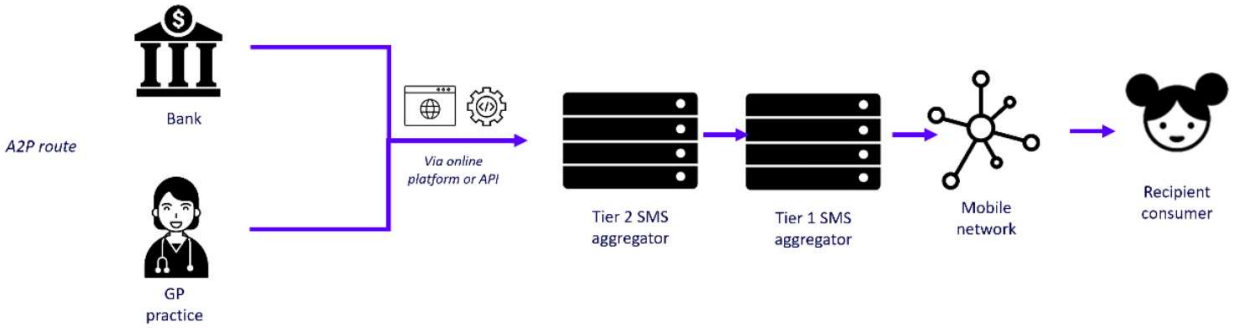


Fuente: Reducing mobile messaging scams[145].

- **Mensajes desde una aplicación a una persona (*Application-to-Person* o A2P):** Son mensajes generados en plataformas en línea o Interfaces de programación de aplicaciones (*Application Programming Interface* o API), que se conectan a las redes de telefonía móvil, permitiendo tanto la creación de mensajes automáticos y como de su envío masivo. Algunos ejemplos de uso típicos incluyen el envío de códigos de acceso de un solo uso para acceder a diversos servicios en línea, recordatorios de citas, mensajes promocionales, así como atención al cliente y encuestas.

  El envió de mensajes A2P incluye agregadores de SMS. Quienes actúan como intermediarios entre los emisores de los mensajes y las redes móviles. Dependiendo de su conexión con los operadores, los agregadores pueden clasificarse como de Nivel 1 (Tier 1), donde tienen una relación contractual directa con un operador de red móvil, o de Nivel 2 (Tier 2) o Nivel 3 (Tier 3), donde la conexión con el operador es indirecta.

Ilustración 25. Diagrama con la forma en que son enviados los mensajes SMS en el esquema A2P



Fuente: Reducing mobile messaging scams[146].

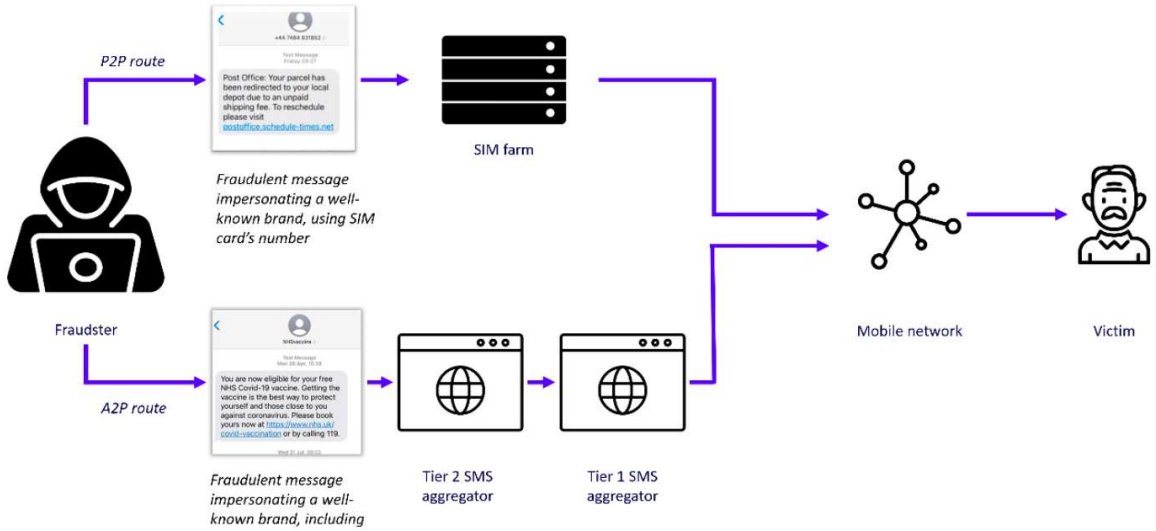
Los estafadores que utilizan la mensajería P2P para cometer sus delitos suelen recurrir a granjas de tarjetas SIM, que corresponden a dispositivos que albergan decenas o cientos de tarjetas SIM y permiten generar mensajes y transmitirlos como SMS por las redes móviles mediante estas tarjetas.

Por otra parte las funcionalidades de los SMS A2P tienen la capacidad de mostrar una Identificación (ID) alfanumérica del remitente, de modo que el mensaje se muestra al receptor con el nombre de una

[145] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams
[146] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams

organización específica, en lugar de un número de teléfono móvil. Generalmente, los estafadores aprovechan las vulnerabilidades en los agregadores para suplantar la Identidad de organizaciones, haciéndolos más creíbles a los destinatarios.

Ilustración 26. Esquema de Cómo los Estafadores Envían Mensajes SMS sobre P2P o A2P



Fuente: Reducing mobile messaging scams[147].

Con el fin de prevenir el uso de mensajes fraudulentos por medio de SMS o RMS el Reino Unido ha implementado las siguientes estrategias:

1. Medidas contra el fraude mediante mensajes P2P:

- Regulaciones sobre Numeración:
  En el Reino Unido, Ofcom ha establecido reglas relacionadas con la asignación, adopción y uso de números de telefonía móvil. Dentro de las medidas adoptadas se encuentran la exigencia de requisito para que los proveedores de comunicaciones se aseguren de usar los números de manera eficaz y eficiente. También requiere que los proveedores de comunicaciones tomen todas las medidas razonablemente practicables para asegurar que sus clientes cumplan con las Condiciones Generales del Plan de Numeración en relación con el uso de números asignados.

  Ofcom también ha publicado una Guía de Buenas Prácticas que establece los pasos que deben realizar los proveedores para prevenir el mal uso de los números de teléfono u las verificaciones que se deben realizar a los clientes para verificar su identidad y sus antecedentes.

  Adicionalmente, los Operadores de Redes Móviles están facultados para suspender el servicio a sus usuarios cuando estos violan los términos y condiciones acordados para la prestación de los servicios.

[147] Extraído del documento disponible en el siguiente vínculo: https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

- Judicialización de las Granjas de Tarjetas SIM:
  En el Reino Unido la normatividad establece que es ilegal suministrar o poseer granjas de tarjetas SIM, si se pretende utilizarlas para cometer fraude, sin embargo su efectividad es limitada, debido a que puede ser difícil para los organismos de seguridad demostrar que esa es la intención.

  Actualmente se está estudiando un proyecto de ley para tipificar el suministro o la posesión de granjas de tarjetas SIM, contemplando las debidas excepciones cuando sean utilizadas para un uso legítimo.

- Limites sobre el Envío Masivo de Mensajes:
  Teniendo en cuenta que los estafadores suelen ofrecer un número ilimitado de mensajes SMS a mediante de granjas de tarjetas SIM, en el Reino Unido los operadores móviles están facultados a aplicar límites de volumen a la cantidad de mensajes SMS que una tarjeta SIM puede enviar en un periodo determinado.

  En el Reino Unido, los operadores móviles tienen establecidos límites sobre la cantidad de mensajes que pueden ser enviados. Generalmente estos umbrales, se establecen por periodos horarios, diarias o mensuales. Los límites suelen establecerse entre 250 y 2500 mensajes al día.

  Estas restricciones deben realizarse de manera que no perjudiquen a los usuarios que los envían para un uso legítimo, y en el Reino Unido se realizan consultas a los usuarios para su definición.

- Registro de Tarjetas SIM:
  Aunque en el Reino Unido, no existe obligación para que los operadores de red recopilen información de registro al emitir tarjetas SIM, se ha identificado como una buena práctica, aplicada por otros países, establecer requisitos para el registro de tarjetas SIM, lo cual facilita la identificación del titular de una tarjeta.

  No obstante, para la venta de servicios móviles postpago, los operadores de redes han establecido políticas para realizar verificaciones de crédito y recopilar información personal para fines de facturación. Estas verificaciones de crédito generalmente incluyen datos de cuentas bancarias e información del historial de direcciones del titular de la tarjeta. Para los contratos de servicios móviles prepago, los operadores no realizan verificaciones de crédito.

  Entre los problemas identificados en el Reino Unido sobre el registro de tarjetas SIM se encuentran:
  - Posibles limitaciones de disponibilidad de tarjetas SIM;
  - Inquietudes sobre la privacidad de los datos y las comunicaciones de las personas; o
  - Incentivos a la creación de mercados negros sobre la comercialización de estas tarjetas.

- Suspensión de IMEI:
  Mediante esta estrategia los operadores móviles pueden bloquear un dispositivo móvil mediante su número IMEI, impidiendo que ese equipo acceda a la red por completo o bloquear específicamente el envío de mensajes SMS.

En Australia, exige a los operadores móviles investigar y tomar las medidas pertinentes para bloquear los mensajes de texto fraudulentos que provienen de los usuarios de sus redes, incluyendo la opción de bloquear el IMEI de los dispositivos móviles utilizados para comunicaciones fraudulentas.

Una de las limitaciones de este método, es que está vinculado a un dispositivo móvil en lugar de a una tarjeta SIM, lo que significa que los estafadores podrían eludir estas medidas utilizando un dispositivo nuevo o alterando el IMEI de los dispositivos que están utilizando para cometer los delitos.

2. Medidas contra el fraude mediante mensajes A2P:

- Debida diligencia en la verificación de los clientes por parte de los Agregadores de Mensajes: Aunque actualmente en el Reino Unido, no existe regulación que se refiera explícitamente a los mensajes SMS enviados mediante agregadores, estas organizaciones deben cumplir con ciertas normas generales tales como hace un uso eficaz, eficiente y debido de la numeración asignada, tomar las medidas razonables para verificar que sus clientes cumplan con las Condiciones Generales exigidas en el Plan de Numeración en relación con el uso de los números.

  Como parte de las de buenas prácticas los agregadores de mensajes A2P realizan verificaciones a sus clientes tales como validaciones a los documentos de identidad, revisión de registros mercantiles y a otros documentos que permitan identificar otros antecedentes. Adicionalmente, con el fin de garantizar que los agregadores que se conectan a las redes de servicios móviles realizan estas de verificaciones, algunos operadores de estos servicios establecen dentro de sus contratos penalizaciones o multas que se aplican se constata que el agregador no realiza las validaciones acordadas o se identifica que desde el agregador se cursaron mensajes fraudulentos. Generalmente este tipo de políticas de verificación se denominan "Conozca a Sus Clientes" (*Know Your Customer* o KYC).

  Otra medida que los operadores de redes móviles, es la implementación un sistema de información conjunto para categorizar a los agregadores que han permitido la generación de mensajes fraudulentos, estableciendo multas y penalidades de acuerdo con su historial y la cantidad de mensajes fraudulentos generados.

  Para evitar la suplantación de identidad de las marcas utilizadas por organizaciones conocidas, los Operadores de Redes Móviles suelen entregar a los agregadores una lista de marcas que deben recibir un trato diferente permitiendo que el tráfico se envíe por medio de conexiones específicas para separarlo del otro tipo tráfico. El agregador debe verificar la autenticidad del remitente y cualquier tráfico que provenga de una conexión diferente a la especificada, se bloquea.

  Por último, un aspecto que potencializa la adopción de estas medidas es promover la compartición de información de datos entre los diferentes actores que participan en la cadena de valor del envío de mensajes A2P. Para promover la compartición de esta información algunos operadores móviles incluyen obligaciones contractuales para exigir a los agregadores que les informen oportunamente sobre los casos de estafas SMS A2P.

- Registro de Identificación (ID) de Remitentes:

En el Reino Unido las organizaciones pueden registrar de manera voluntaria los ID alfanuméricos utilizados por sus marcas para el envío de mensajes para asegurar a sus clientes que los mensajes enviados. Una vez registrado un ID de remitente alfanumérico, otras marcas u organizaciones no deberían poder usarlo al enviar mensajes SMS A2P a consumidores mediante agregadores y operadores móviles.

3. Medidas que aplican contra el fraude mediante mensajes P2P y A2P:

- Herramientas de Monitoreo de Tráfico:
  En el Reino Unido la implementación de herramientas de monitorización del tráfico se realiza de manera voluntaria. Estas herramientas incluyen funcionalidades como Escudos antispam y control de fraude que permiten identificar SMS sospechosos antes de su entrega a los consumidores e incluyen capacidades para encontrar patrones de mensajes fraudulentos en función de factores como su contenido (incluidas frases y URL), los números de teléfono del remitente y del destinatario, y patrones de tráfico, con el fin de bloquear mensajes o enviar etiquetas de advertencia.

9.14. Singapur

Durante los años 2021 a 2023 en Singapur se ha evidenciado el aumento de las víctimas y de las pérdidas causadas por las estafas realizadas utilizando diferentes medios, como se presenta en las cifras contenidas en la Tabla 8.

Tabla 8. Fraudes Totales Realizados en Singapur

Types of scams	Cases reported			Total amount cheated (at least)			Average amount cheated in 1H 2023
	1H 2023	2022	2021	1H 2023	2022	2021	
Phishing scams	2,991	7,097	5,023	SGD 7.40m (US$5.48m)	SGD 16.50m (US$12.23m)	SGD 34.80m (US$25.79m)	SGD 2,474 (US$1,833.66)
Others*	19,348	24,631	18,910	SGD 327.10m (US$242.44m)	SGD 644.20m (US$477.46m)	SGD 597.20m (US$442.63m)	SGD 16,906 (US$12,530)
Total	22,339	31,728	23,933	SGD 334.50m (US$247.92m)	SGD 660.70m (US$489.69m)	SGD 632m (US$468.42m)	SGD 14,974 (US$11,098)

* job, e-commerce, fake friend call, investment, social media impersonation, internet love, loan, government officials impersonation and credit-for-sex scams

Fuente: Singapore proposes shared liability scheme on phishing scams[148].

La Autoridad de Desarrollo de Medios de Infocomunicación (IMDA) de Singapur lanzó el 15 de agosto de 2022 una consulta pública para implementar dos medidas regulatorias para combatir el fraude.

[148] Extraído del documento *Singapore proposes shared liability scheme on phishing scams*; Cullen International; 21 de noviembre de 2023

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

1. Implementar el Registro de ID para los Remitentes de SMS (SMS *Sender ID Registry* o SSIR)

Teniendo en cuenta que los estafadores buscan ganarse la confianza de sus víctimas enviando SMS suplantando la Identidad del remitente de organizaciones legítimas, la IMDA propuso la implementación de un Registro de ID para los Remitentes de SMS[149].

En consecuencia, con la entrada en vigencia de esta normativa, las organizaciones y entidades deberán registrar las Identificaciones (ID) de Remitente que utilizarán para el envío de SMS. En consecuencia, las redes móviles de Singapur bloquearán por defecto todos los ID de Remitentes que no estén registrados. Este requisito aplicaría únicamente a las empresas que utilicen como encabezado para el envío de sus SMS ID alfanuméricos y, por lo tanto, esta norma seria inexequible para los usuarios de teléfonos móviles (incluidas las organizaciones) que envíen SMS utilizando los números de móvil asignados por los proveedores de servicios de telecomunicaciones.

Con respecto a los agregadores de SMS, la norma establece que aquellos de envíen SMS utilizando ID de remitente, deben contar con una licencia de la IMDA para el trámite y obtención del SSIR.

Para tramitar el SSIR las organizaciones deben presentar la documentación que los acredite como una organización legalmente constituida, que para el caso de Singapur corresponde al Número Único de Entidad (*Unique Entity Number* o UEN) que es emitido por las agencias gubernamentales debidamente avaladas y reconocidas.

Como antecedente a la expedición de esta norma, en agosto de 2021 se inició un programa piloto de Registro ID de Remitente de manera voluntaria aspecto que se mantendrá vigente durante el periodo de transición definido por la IMDA, comprendido entre la expedición de la norma, realizado en octubre de 2022, hasta su entrada en vigor, en diciembre de ese mismo año, fecha a partir de la cual sería obligatorio contar con el SSIR para el envío de SMS con ID alfanuméricos en sus encabezados.

2. Implementar de Filtro Antifraude de SMS en las Redes Móviles

El filtro antifraude está diseñado para funcionar como un cortafuegos de seguridad (*Firewall*) que utiliza un escaneo automático para revisar y filtrar los mensajes SMS que contienen en:

- Enlaces maliciosos dirigidos a los consumidores con sitios web que solicitan información confidencial o que provocan la instalación de *malware* y virus; o
- Mensajes con patrones sospechosos que indican que podría tratarse de un mensaje fraudulento, los cuales se podrían identificar a partir del uso de palabras o frases comunes utilizadas en estafas.

La IMDA propone que los operadores de redes móviles de Singapur implementen esta solución, en dos Fases:

[149] Información extraída del documento *Singapore consults on initiatives to reduce scam SMS*; Cullen International; 25 de agosto de 2022

- **Fase 1: Filtrado de mensajes SMS fraudulentos mediante la detección de enlaces maliciosos**
  En esta fase los operadores de redes móviles compararán los enlaces contenidos en los SMS con una base de datos de enlaces maliciosos conocidos (no se especifica quién creará ni gestionará la base de datos). Si se detecta una coincidencia, el mensaje SMS será bloqueado.

- **Fase 2: Filtrado adicional de mensajes SMS fraudulentos que contengan patrones sospechosos:**
  En esta fase el sistema identificará y bloqueará los mensajes SMS basándose en patrones sospechosos, caracterizando, mediante herramientas de inteligencia artificial y *machine learning*, palabras, frases y formatos de mensaje que se utilizan habitualmente en los mensajes SMS fraudulentos.

Adicional a estas medidas, el 20 de diciembre de 2023 la Autoridad Monetaria de Singapur (MAS) y la IMDA realizaron otra consulta pública sobre un nuevo marco regulatorio de responsabilidad compartida (*Shared Responsibility Framework* o SRF) para las estafas realizadas por medio de *phishing* que, de acuerdo con la policía de Singapur, «*generalmente se realizan con correos electrónicos, mensajes de texto, llamadas o anuncios de estafadores que se hacen pasar por funcionarios o entidades de confianza, para que las víctimas revelen detalles como la información de sus tarjetas de crédito o cuentas bancarias, a partir de engaños, para posteriormente realizar transacciones no autorizadas*»[150].

Esta propuesta establece que tanto las Instituciones Financieras (*Financial Institutions* o FI) como los Operadores de Redes Móviles (*Mobile Network Operators* o MNO) podrían ser considerados responsables de las estafas cometidas por medio de *phishing* en aquellos casos donde se compruebe el incumplimiento de las obligaciones adoptada por las entidades gubernamentales para su prevención, dando lugar al pago de indemnizaciones a las víctimas que caigan en este tipo de estafas. El gobierno de Singapur informó que la inclusión de los MNO como posibles entidades responsables sería un aspecto único en el mundo y con esta medida busca frenar el uso de SMS por parte de los estafadores para defraudar a sus víctimas.

De manera paralela, la MAS realizó otra consulta pública para modificar las Directrices de Protección del Usuario de Pagos Electrónicos (EUPG), con el objetivo de mejorar los controles antifraude aplicados en el sector financiero y priorizar la vigilancia y la responsabilidad del consumidor. Tanto la EUPG como la SRF son directrices complementarias y los lineamientos de esta última se basan en los definidos en la EUPG.

La modificación de la EUPG tiene como objetivo asegurar que todas las organizaciones que prestan servicios financieros hagan parte del Centro de Resolución de Disputas de la Industria Financiera *(Financial Industry Disputes Resolution Centre* o FIDReC), para que de esta forma los clientes de las Instituciones Financieras puedan acudir al FIDReC cuando hayan sufrido pérdidas económicas a causa de estafas realizadas mediante phishing.

El SRF está diseñado para cubrir las estafas de phishing, en las que se engaña a un consumidor para que haga clic en un enlace de phishing e introduzca sus credenciales en una plataforma digital falsa y

[150] Información extraída del documento *Singapore proposes shared liability scheme on phishing scams*; Cullen International; 21 de noviembre de 2023.

aplica a entidades financieras locales o extranjeras que tengan sede y presten servicios financieros en Singapur. El SFR excluye los siguientes tipos de estafa:

- Estafas en las que las víctimas autorizan pagos.
- Estafas en las que se engaña a un consumidor para que proporcione sus credenciales enviando SMS.
- Otras variantes de estafas que involucran transacciones no autorizadas que se realizan mediante métodos diferentes al phishing.

La SFR establece las siguientes obligaciones a las FI, los MNO y a los usuarios de los Servicios Financieros:

- **Obligaciones de las Instituciones Financieras**
  - Imponer un periodo de anulación de transacciones por un periodo de 12 horas contados después de la activación del token de seguridad digital, durante el cual el usuario no podrá realizar actividades catalogadas como alto riesgo.
  - Enviar alertas de notificación en tiempo real a sus usuarios para la activación del token de seguridad digital y la realización de actividades catalogadas como alto riesgo.
  - Enviar alertas de notificación a sus usuarios informando retiros de dinero en tiempo real.
  - Ofrecer un canal de denuncias (24/7) y una función de autoservicio denominado "interruptor de seguridad" a sus usuarios, para que estos informen y bloqueen el acceso no autorizado a sus cuentas.

- **Obligaciones de los Operadores de Redes Móviles**
  - Conectar únicamente a agregadores autorizados para el envío de SMS con ID de remitente y asegurar que los SMS son enviados por remitentes autorizados y registrados en el SSIR.
  - Bloquear los SMS con ID de remitente que no provengan de agregadores autorizados.
  - Implementar el Filtro Antifraude de SMS para bloquear los SMS con enlaces de phishing conocidos.

- **Obligaciones de los Usuarios de Servicios Financieros**
  - No compartir sus credenciales personales ni cualquier información que permita el acceso a sus productos financieros.
  - No hacer clic en enlaces proporcionados en SMS o correos electrónicos, a menos que se trate de enlaces informativos de la entidad financiera.

Para establecer al responsable de cubrir las pérdidas económicas por fraudes realizados por *phishing* mediante SMS, se aplica el siguiente procedimiento:

- La Institución Financiera será el primer responsable y asumirá la totalidad de las pérdidas sufridas por el usuario si se evidencia el incumplimiento de alguna de las obligaciones establecidas en la SFR.
- Si la Institución Financiera ha cumplido con todas las obligaciones establecidas en el SRF y se evidencia que la estafa ocurrió como consecuencia de que el MNO incumplió alguna de las obligaciones establecidas en la SFR, el MNO asumirá la totalidad de las pérdidas sufridas por el usuario.
- Si tanto la FI como el MNO han cumplido con las obligaciones establecidas en el SRF, será el titular de la cuenta quien asuma la totalidad de las pérdidas.

La normatividad también estipula las siguientes etapas para dar respuesta a las reclamaciones interpuestas por los usuarios:

- **Etapa de reclamación:** La entidad financiera responsable será el primer punto de contacto con el consumidor y deberá evaluar si la reclamación se encuentra dentro del ámbito de aplicación del SRF e informar al operador de red móvil responsable, si corresponde.
- **Etapa de investigación:** La FI y el MNO responsable, llevarán a cabo la investigación para establecer responsabilidades frente a las reclamaciones presentadas por los usuarios.
- **Etapa de resultado:** La FI responsable informará y explicará al usuario el resultado de la investigación.
- **Etapa de recurso:** Si el usuario no está conforme con la respuesta a la reclamación, podrá interponer otras acciones mediante las vías de recurso ante la FIDReC o la IMDA.

Esta normativa excluye las transacciones realizadas por medio de las tarjetas de crédito, donde la distribución de responsabilidades se especifica en el Código de Prácticas Bancaria.

Por último, es importante señalar que las entidades del gobierno de Singapur consideran que la adopción de medidas para combatir estafas realizadas mediante *malware* sería prematura, en consideración a que estas aún están en etapa de desarrollo y se requieren mayores estudios para su implementación.

ANEXO 2. RECOMENDACIONES Y RESOLUCIONES DE LA UNIÓN INTERNACIONAL DE TELECOMUNICACIONES

En este capítulo se presentan las disposiciones de la Unión Internacional de Telecomunicaciones (UIT) frente a la numeración de redes de telecomunicaciones públicas y transmisión de la identificación de la parte llamante con base en las diferentes resoluciones y recomendaciones que la UIT ha emitido.

La Recomendación UIT-T E.164[151] de la UIT estandariza la estructura y función de los dígitos de los números utilizados para realizar llamadas a través de las redes de telecomunicaciones públicas internacionales para las cinco categorías definidas por este organismo: (i) áreas geográficas; (ii) servicios globales; (iii) redes; (iv) grupos de países (*Group of Countries*); y (v) Recursos de prueba. Las disposiciones contenidas en esta Recomendación también aplican para llamadas que se realicen bajo el Protocolo de Internet (*Internet Protocol* o IP), interconectadas con redes de telecomunicaciones de conmutación de circuitos[152].

Para cada una de estas categorías, la Recomendación UIT-T E.164 detalla la estructura y características de cada uno de los componentes de la numeración de la parte llamante y la parte llamada, y los análisis que deben realizarse para enrutar las llamadas al destinatario de esta. De acuerdo con las estipulaciones establecidas, las autoridades nacionales de cada país administran un Plan Nacional de Numeración (PNN)[153].

[151] Recomendación UIT- T E.164; Unión Internacional de las Telecomunicaciones; noviembre de 2010
[152] Recomendación UIT- T E.370; Unión Internacional de las Telecomunicaciones; febrero de 2001
[153] En Colombia, la función de administrar el PNN le fue asignado a la CRC a través del Decreto 1078 de 2015, ver enlace: https://normograma.mintic.gov.co/mintic/compilacion/docs/decreto_1078_2015.htm

De acuerdo con las Recomendaciones UIT-T E.157[154] y UIT-T E.164, una de las parámetros permitidos para el establecimiento de comunicaciones a través de las redes de telecomunicaciones públicas, es la transmisión del Número de la Parte Llamante (*Calling Party Number* o CPN), que tiene como fin permitir que la parte que recibe la llamada pueda identificar el número de la parte llamante; este servicio suplementario es denominado "Identificador de Línea Llamante" (*Calling Line Identification* o CLI), de acuerdo con definición que se encuentra en la Recomendación UIT-T I.251.3[155].

Este servicio CLI también permite que el usuario de la parte llamante restrinja la presentación del Número de la Parte Llamante (*Calling Party Number* o CPN o Número de Presentación) a la parte llamada, de conformidad con las definiciones y procedimientos contempladas en la Recomendación UIT-T I.251.4[156] y la identificación de llamadas maliciosas donde la parte llamada puede solicitar a la parte llamante que se identifique y se registre a la red, tal como se detalla en la UIT-T I.251.7[157].

La descripción del servicio de CLI y los requisitos para su operación y de codificación, se encuentran en la Recomendación UIT-T Q.731.3[158]. Igualmente, en esta Recomendación y en la Recomendación UIT-T Q.731.5[159] se describen los requisitos de señalización para la central local de origen, la central de tránsito y la central de acceso local o internacional de destino, así como la interacción del CLI con otros servicios suplementarios y con otras redes.

La posibilidad del envío del CLI depende de las funcionalidades y las aplicaciones habilitadas en las redes de telecomunicaciones públicas y de los servicios que se prestan, en el marco de los acuerdos logrados entre los operadores de origen, tránsito y recepción. Igualmente, la información contenida en el CLI puede enviarse en comunicaciones que se realicen entre países, de acuerdo con los acuerdos que se lleguen entre estos.

Este servicio suplementario también permite a la parte llamante restringir la presentación o el envío de su número (Número de Presentación), aspecto que puede estar reglamentado en la legislación y la normatividad adoptada por cada país. El formato del Número de Presentación del CLI debe ser un número que cumpla con las directrices definidas en la Recomendación UIT-T E.164.

Por su parte, la Recomendación UIT-T E.157 establece lineamientos en relación con el envío y la presentación del Número de la Parte Llamante (*Calling Party Number* o CPN o Número de Presentación) los cuales están sujetos a las leyes y normativas adoptados por cada país.

Igualmente, para las llamadas internacionales, esta recomendación establece los siguientes lineamientos:

1. Los operadores desde donde se origina una llamada internacional deben tener la capacidad de identificar el CPN y, en consecuencia, no se deben cursar llamadas internacionales anónimas. Para implementar esta medida en llamadas donde se restringe el envío del Número de Presentación, la recomendación establece que el CPN debe entregarse al operador que presta el servicio al usuario

[154] Recomendación UIT- T E.157; Unión Internacional de las Telecomunicaciones; junio de 2021
[155] Recomendación UIT- T I.251.3; Unión Internacional de las Telecomunicaciones; agosto de 1992
[156] Recomendación UIT- T I.251.4; Unión Internacional de las Telecomunicaciones; agosto de 1992
[157] Recomendación UIT- T I.251.7; Unión Internacional de las Telecomunicaciones; agosto de 1992
[158] Recomendación UIT- T Q.731.3, Unión Internacional de las Telecomunicaciones; marzo de 1993
[159] Recomendación UIT- T Q.731.5, Unión Internacional de las Telecomunicaciones; abril de 2019

de destino, quien es el encargado de restringir su presentación en el dispositivo receptor de la llamada.
2. Cuando la normatividad del país desde donde se realiza la llamada internacional, exige al operador de la red origen que, para cumplir con la restricción de compartir el número de presentación, de acuerdo las solicitudes realizadas por sus abonados, se debe reemplazar el CPN por un Número Especial que le haya sido atribuido, el cual hace parte de un rango de numeración específico definido por el Administrador el Plan Nacional de Numeración (PNN), tanto los administradores de los PNN y los Operadores de Red deben notificar a la UIT estos rangos de numeración. Los Números Especiales, utilizados para reemplazar el Número de la Parte Llamante, deben cumplir con las condiciones establecidas en la recomendación UIT-T E.164.
3. Los operadores de la red de destino tienen derecho a rechazar las llamadas que no cumplan con los lineamientos establecidos en los numerales 1 y 2.

Por su parte la Recomendación UIT-T E.156[160] describe los procedimientos para reportar y tomar medidas en caso de uso indebido de determinados recursos de numeración de la Recomendación UIT-T E.164, incluyendo la forma en que la Oficina de Normalización de Telecomunicaciones de la UIT (*Telecommunication Standardization Bureau* o TSB) abordará y contrarrestará cualquier presunto uso indebido cuando dichos informes le sean presentados.

La Recomendación establece que los proveedores de redes y servicios de comunicaciones únicamente deben utilizar los recursos de numeración que les han sido asignados, y utilizarlos exclusivamente para los fines establecidos. Por su parte los recursos de numeración sin asignar no podrán ser utilizados.

De acuerdo con lo anterior se pueden dar dos tipos de asignaciones en las cuales se pueden encontrar usos indebidos de la numeración:

1. Números de la Recomendación UIT-T E.164 asignados directamente por la TSB de la UIT; y
2. Numeración de la Recomendación UIT-T E.164 asignados por las autoridades encargadas de administrar la numeración en cada país (denominada "Números Asignados Indirectamente por la TSB" en la Recomendación UIT-T E.156).

Cuando se detecten o presenten usos indebidos a recursos de numeración asignados directamente por la TSB, la entidad administradora de los recursos de numeración o el operador de los servicios de telecomunicaciones que haya detectado esta situación, deberá informar su ocurrencia a la TSB quien se encargará de realizar una investigación que involucrará a la administradora de los recursos de numeración desde donde se originó el uso indebido de la numeración y de tomar las medidas correctivas pertinentes, las cuales podrán acarrear incluso el retiro de la asignación de la numeración.

En el caso de detectarse o presentarse usos indebidos de los recursos de numeración asignada indirectamente por la TSB, la entidad administradora de los recursos de numeración o el operador de los servicios de telecomunicaciones que haya detectado esta situación, deberá informar su ocurrencia a la entidad administradora de los recursos de numeración o al operador de los servicios de telecomunicaciones desde donde se originó el uso indebido de la numeración para que investiguen y tomen las medidas respectivas para evitar que se siga haciendo un uso indebido de la numeración.

[160] Recomendación UIT- T E.156; Unión Internacional de las Telecomunicaciones; junio de 2020.

El detalle de los procedimientos y medidas que se pueden tomar por el uso de numeración asignada directa o indirectamente por el TSB, pueden consultarse en la Recomendación UIT-T E.156.

Teniendo en cuenta que los avances tecnológicos han traído nuevos retos a los lineamientos definidos en las Recomendaciones expedidas por la UIT relacionadas con el CLI, la UIT ha expedido las Resoluciones 21[161], 29[162], 61[163] y 65[164] con en el fin de tratar las problemáticas relacionadas con:

- La aparición de Procedimientos Alternativos de Llamada (PALL) que impiden la identificación de la línea llamante (CLI) y/o la identificación de su origen (*Origin Identification* o OI);
- La tendencia de suprimir o modificar en las llamadas internacionales la información de identificación del Número de la Parte Llamante (CPN), la Identificación de la Línea Llamante (CLI) y la identificación del origen (OI), en particular de los campos correspondientes al indicativo del país y del indicativo nacional de destino;
- El aumento en la cantidad de casos notificados a la TSB sobre la apropiación y uso indebido de la numeración de la Recomendación UIT-T E.164, práctica que incluso se ha empleado para realizar estafas.

La Resolución 21 *Measures concerning alternative calling procedures on international telecommunication networks* y la Resolución 29 *Procedimientos alternativos de llamada en las redes internacionales de telecomunicación* definen lineamientos y directrices para hacer frente a los retos que traen consigo, para la Calidad de Servicio (QoS) de las redes y la identificación de la línea llamante (CLI) y/o la identificación de su origen, tanto a los Procedimientos Alternativos de Llamada (PALL) como al impacto que sobre estos procedimientos ha tenido la ubicuidad de las redes IP.

En consecuencia, a través de estas resoluciones la UIT ha decidido continuar ejecutando, entre otras, las siguientes acciones:

1. Identificar y definir todas las modalidades de procedimientos alternativos de llamada.
2. Alentar a las autoridades nacionales y los operadores de telecomunicaciones o concesionarias de la prestación de servicios de telecomunicaciones de los Estados Miembros a adoptar, en la medida de lo posible, todas las disposiciones necesarias para suspender los métodos y las prácticas inherentes a los procedimientos alternativos de llamada que, o bien degraden gravemente la calidad del servicio (QoS) de las redes de telecomunicaciones, o impidan proporcionar la información relativa a la CLI o la identificación del origen de la llamada, OI.
3. Encargar a la Comisión de Estudio 2 de la UIT para que estudie, defina y elabore las Recomendaciones y directrices pertinentes para: (i) Los procedimientos alternativos de llamada, incluyendo los vinculados a la interconexión de las estructuras IP con las redes tradicionales y los casos de obstrucción, ocultación o falsificación de la información relativa a la OI o la CLI; y (ii) la evolución de los procedimientos alternativos de llamada, en particular los relacionados con olas

[161] Resolución 21 "*Measures concerning alternative calling procedures on international telecommunication networks*"; Unión Internacional de las Telecomunicaciones; noviembre de 2018
[162] Resolución 29 "*Procedimientos alternativos de llamada en las redes internacionales de telecomunicación*"; Unión Internacional de las Telecomunicaciones; marzo de 2022
[163] Resolución 61 "*Countering and combating misappropriation and misuse of internationa ltelecommunication numbering resources*"; Unión Internacional de las Telecomunicaciones; marzo de 2022
[164] Resolución 65 "*Comunicación del número de la parte llamante, identificación de la línea llamante e información sobre la identificación del origen*"; Unión Internacional de las Telecomunicaciones; marzo de 2022

utilización de aplicaciones telefónicas en servicios OTT (*Over The Top*) que utilizan números de la UIT-T E.164, lo que puede dar lugar a prácticas fraudulentas.

4. Invitar a las autoridades nacionales y los operadores de telecomunicaciones o concesionarias de la prestación de servicios de telecomunicaciones de los Estados Miembros a adoptar un marco jurídico y reglamentario nacional que: (i) Prohíban la utilización de procedimientos alternativos de llamada que degraden el nivel de QoS y QoE; (ii) Promuevan el envío de la información relativa a la CLI y la OI de llamadas internacionales al operador o prestador de red de destino; y (iii) garanticen una tarificación adecuada, de conformidad con las directrices impartidas por las Recomendaciones UIT-T que sean pertinentes a este asunto.

Adicionalmente, en la Resolución 29 se presenta la siguiente *Propuesta de directrices para las Administraciones y los operadores de telecomunicaciones internacionales o las empresas de explotación autorizadas por los Estados Miembros sobre las consultas relativas a los procedimientos alternativos de llamada*:

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

Tabla 9. Directrices propuestas para realizar consultas relativas a los PALL

País X (el de ubicación del usuario de los PALL)	País Y (el de ubicación del proveedor de los PALL)
En general, conviene adoptar un enfoque razonable y basado en la colaboración	En general, conviene adoptar un enfoque razonable y basado en la colaboración
La administración X, que desea restringir o prohibir los PALL, debe establecer una posición política clara	
La administración X debe hacer saber su posición nacional	La administración Y debe señalar esa información a los operadores de telecomunicaciones internacionales o las empresas de explotación autorizadas por los Estados Miembros y los proveedores de los PALL de su territorio utilizando todos los medios oficiales disponibles
La administración X debe indicar su posición política a las empresas de explotación autorizadas por los Estados Miembros que operan en su territorio y dichas empresas de explotación autorizadas por los Estados Miembros deben adoptar medidas para garantizar que sus acuerdos de explotación nacional se ajusten a dicha posición	Las empresas de explotación autorizadas por los Estados Miembros del país Y deben cooperar considerando toda modificación necesaria de los acuerdos internacionales de explotación
	La administración Y y/o las empresas de explotación autorizadas por los Estados Miembros del país Y deben tratar de asegurarse de que todos los proveedores de PALL que se establezcan en su territorio sean conscientes de que: *a)* este tipo de procedimientos no deben darse a un país en el que estén expresamente prohibidos; y *b)* la configuración de los PALL debe ser de un tipo que no degrade la calidad y las características de la red telefónica pública conmutada internacional.
La administración X adoptará todas las medidas razonables dentro de su jurisdicción y responsabilidad para detener la oferta y/o utilización en su territorio de los PALL que: *a)* estén prohibidos; y/o *b)* sean perjudiciales para la red. Las empresas de explotación autorizadas por los Estados Miembros activas en el país X cooperarán para aplicar dichas medidas.	La administración Y y las empresas de explotación autorizadas por los Estados Miembros activas en el país Y deben adoptar todas las medidas razonables para impedir que los proveedores de PALL de su territorio ofrezcan dichos procedimientos: *a)* en otros países en los que estén prohibidos; y/o *b)* cuando sean perjudiciales para las redes involucradas.

NOTA 1 – Por lo que se refiere a las relaciones entre los países que consideran los PALL como un "servicio internacional de telecomunicaciones", tal como se define en el Reglamento de las Telecomunicaciones Internacionales, las empresas de explotación autorizadas por los Estados Miembros en cuestión deben establecer acuerdos de explotación bilaterales sobre las condiciones de explotación de los PALL.

NOTA 2 – Todas las modalidades de PALL deben ser definidas por la Comisión de Estudio 2 del UIT-T y consignadas en la Recomendación UIT-T pertinente (véanse los métodos basados en la devolución de llamadas, las aplicaciones superpuestas (OTT), la reoriginación de llamadas, etc.).

Fuente: Resolución 29 "Procedimientos alternativos de llamada en las redes internacionales de telecomunicación"[165].

Por su parte la Resolución 61 *Countering and combating misappropriation and misuse of international telecommunication numbering resources* estableció, entre otros, las siguientes directrices y lineamientos

[165] Resolución 29 *Procedimientos alternativos de llamada en las redes internacionales de telecomunicación*; Unión Internacional de las Telecomunicaciones; marzo de 2022

con el fin de hacer frente y disminuir la cantidad de casos notificados a la TSB sobre la apropiación y uso indebido de la numeración de la Recomendación UIT-T E.164:

1. Invitar a los Estados Miembro a asegurar que los recursos de numeración UIT-T E.164 se utilicen únicamente para los fines para los que fueron asignados y que no se utilicen recursos no asignados;
2. Invitar a los Estados Miembro a realizar su mayor esfuerzo para que los proveedores de redes y servicios de telecomunicaciones divulguen la información de enrutamiento a las agencias debidamente autorizadas en casos de fraude o uso o apropiación indebidos de la numeración, de conformidad con la legislación nacional;
3. Invitar a los Estados Miembro para que alienten a los proveedores de redes y servicios de telecomunicaciones a colaborar e intercambiar información sobre actividades fraudulentas relacionadas con la apropiación y el uso indebido de los recursos de numeración y a colaborar para contrarrestar y combatir dichas actividades por parte de las autoridades nacionales;
4. Invitar a los Estados Miembro a alentar a todos los operadores de servicios de telecomunicaciones internacionales para mejorar la eficacia de las directrices dadas por la UTI, aplicando las Recomendaciones expedidas por este organismo, en particular las elaboradas por la Comisión de Estudio 2 del UIT-T, con el fin de contrarrestar, combatir y abordar las actividades fraudulentas derivadas de la apropiación y uso indebido de los recursos de numeración de la Recomendación UIT-T E.164, bloqueando las llamadas internacionales que se aprovechen de esta situación para cometer delitos;
5. Alentar a las administraciones y los organismos autorizados por los Estados Miembro a explotar los recursos de numeración a adoptar, en la medida de lo posible, todas las medidas razonables para proporcionar la información necesaria para abordar los problemas relacionados con la apropiación y el uso indebidos de la numeración de la Recomendación de la UIT-T E.164;
6. Alentar a los Estados Miembro a adoptar un marco jurídico y reglamentario nacional, con el fin de solicitar a los organismos autorizados por los Estados Miembro a explotar los recursos de numeración, a que las llamadas cursadas mediante PALL envíen, por lo menos al operador de destino, la información relativa a la CLI y/o la OI de la parte llamante, siguiendo las Recomendaciones UIT-T que apliquen;
7. Alentar a las administraciones y los organismos autorizados que explotan recursos de numeración pertenecientes a los Estados Miembro a que tomen nota y consideren, en la medida de lo posible, las «Directrices sugeridas para los reguladores, las administraciones y los organismos autorizados por los Estados Miembro a explotar los recursos de numeración, para abordar la apropiación indebida de números», de conformidad con el anexo de la resolución 61;
8. Alentar a los Estados Miembros y los reguladores nacionales a que tomen nota de los casos de actividades relacionadas con la apropiación y el uso indebido de los recursos de numeración UIT-T E.164 notificados por la UIT;
9. Solicitar a la Comisión de Estudio 2 que continúe estudiando todos los aspectos y formas de apropiación y uso indebido de los recursos de numeración, en particular de los códigos internacionales de país, con miras a modificar la Recomendación UIT-T E.156 y sus suplementos y directrices, con el fin de identificar medios que permitan contrarrestar y combatir estas actividades;
10. Solicitar a la Comisión de Estudio 3 del UIT-T que, en colaboración con la Comisión de Estudio 2, elabore definiciones de actividades inapropiadas, incluidas las que causan pérdida de ingresos, relacionadas con la apropiación y el uso indebido de los recursos de numeración internacionales especificados en las Recomendaciones UIT-T pertinentes, y que continúe estudiando estas cuestiones;

COMISIÓN DE REGULACIÓN DE COMUNICACIONES
REPÚBLICA DE COLOMBIA

11. Solicitar a la Comisión de Estudio 3 que continúe estudiando las repercusiones económicas derivadas de la apropiación y el uso indebido de los recursos de numeración, incluido el bloqueo de llamadas; y
12. Encargar a la Comisión de Estudio 3 del UIT-T para que continue estudiando las repercusiones económicas que tiene la no identificación o falsificación de la Identificación de Origen para cometer estafas mediante aplicaciones telefónicas OTT que utilizan PALL, sobre los esfuerzos de los países para desarrollar las redes y servicios de telecomunicaciones locales y elabore las Recomendaciones y directrices pertinentes.

Adicionalmente, esta Resolución presenta dos escenarios con las *Directrices propuestas para los reguladores, las administraciones y los organismos de explotación autorizados por los Estados miembros para hacer frente a la apropiación indebida de números* que se presentan en las siguientes tablas.

Tabla 10. Escenario 1 - Quejas generadas desde el país de destino de la llamada

País X (País desde donde se origina la llamada)	**País Y (País a través del cual la llamada es enrutada)**	**País Z (País al que originalmente estaba destinada la llamada)**
		Al recibir una queja, el Regulador Nacional busca la siguiente información: nombre del operador desde el cual se originó la llamada, hora de la llamada y número llamado. Posteriormente envía esta información al Regulador Nacional del país X.
Cuando se recibe un reclamo, el Regulador Nacional debe solicitar el nombre del operador desde donde se originó la llamada, la hora de la llamada y el número llamado.		
Una vez obtenida esta información, el Regulador Nacional solicita información relevante al operador que originó la llamada, para determinar el siguiente operador a través del cual se enrutó la llamada.		
Una vez obtenida esta información, el Regulador Nacional debe solicitar al regulador nacional del país a través del cual se enrutó la llamada, los detalles de esta (incluido el registro detallado de la llamada (incluido el registro detallado de la llamada (*Call Detail Register* o CDR)) y demás información pertinente.	El regulador nacional solicita a los operadores la información pertinente. Este proceso continúa hasta encontrar la información desde dónde se realizó la llamada inapropiada.	
Cooperar con las autoridades nacionales con el fin de resolver estos incidentes.	Requerir la cooperación de las entidades u organismos involucrados, con el fin de presentar una denuncia penal contra los perpetradores.	Cooperar con las autoridades nacionales, con el fin de resolver estos incidentes.

Fuente: Resolución 61"*Countering and combating misappropriation and misuse of international telecommunication numbering resources*"[166]

Tabla 11. Escenario 2 - Quejas generadas desde el país de origen de la llamada

País X (País desde donde se origina la llamada)		**País Y (País a través del cual la llamada es enrutada)**	**País Z (País al que originalmente estaba destinada la llamada)**
Al recibir una queja, el regulador nacional solicita el nombre del operador desde donde se originó la llamada, la hora de la llamada, el número llamado. También debe solicitar el operador al que se dirigió la llamada, la hora de la llamada y el número llamante. Esta información debe remitirse al regulador nacional del país Z.			
Una vez obtenida esta información, el Regulador Nacional debe solicitar al operador que originó la llamada la información requerida para determinar el siguiente operador a través del cual se enrutó la llamada.			
Cooperar con las autoridades nacionales, con el fin de resolver estos incidentes. Informar a Autoridades Nacionales pertinentes sobre las medidas adoptadas.		Cooperar con las autoridades nacionales, con el fin de resolver estos incidentes.	
Al recibir una queja, el regulador nacional solicita el nombre del operador desde donde se originó la llamada, la hora de la llamada, el número llamado.			

[166] Resolución 61 "*Countering and combating misappropriation and misuse of internationaltelecommunication numbering resources*"; Unión Internacional de las Telecomunicaciones; marzo de 2022

País X (País desde donde se origina la llamada)	País Y (País a través del cual la llamada es enrutada)	País Z (País al que originalmente estaba destinada la llamada)
También debe solicitar el operador al que se dirigió la llamada, la hora de la llamada y el número llamante. Esta información debe remitirse al regulador nacional del país Z.		
Una vez obtenida esta información, el Regulador Nacional debe solicitar al operador que originó la llamada la información requerida para determinar el siguiente operador a través del cual se enrutó la llamada.		
El regulador nacional puede informar al regulador nacional donde opera el prestador de servicio que enruto la llamada los detalles de la llamada (incluido el registro detallado de la llamada (Call Detail Register - CDR)) y, de ser necesario solicitar la demás información que considere pertinente a este regulador.	El regulador nacional podrá solicitar información relevante a otros operadores. Este proceso podrá continuar hasta que se informe a todos los países por los que se enrutó la llamada.	
Cooperar con las autoridades nacionales, con el fin de resolver estos incidentes. Informar a Autoridades Nacionales pertinentes sobre las medidas adoptadas.	Solicitar la cooperación de las entidades u organizaciones involucradas.	Cooperar con las autoridades nacionales, con el fin de resolver estos incidentes.

Fuente: Resolución 61 *Countering and combating misappropriation and misuse of international telecommunication numbering resources*[167].

Por último la Resolución 65 "*Comunicación del número de la parte llamante, identificación de la línea llamante e información sobre la identificación del origen*" estableció, entre otros, las siguientes directrices y lineamientos para combatir las tendencias de suprimir o modificar en las llamadas internacionales la información de identificación del número de la parte llamante (CPN), la identificación de la línea llamante (CLI) y la identificación del origen (OI), para evitar el uso de estas prácticas para cometer estafas:

1. Ratificar que la información relativa al CPN de debe facilitar con la base en las Recomendaciones expedidas por la UIT sobre esta materia.
2. Ratificar que el envío del CLI y la OI en llamadas internacionales se debe facilitar sobre la base de las Recomendaciones pertinentes de la UIT-T, en la medida en que sea técnicamente viable;
3. Ratificar que los CPN enviados deberían incluir, como mínimo, el número de la parte llamante o el número especial asignado del operador/proveedor de servicios responsable de realizar la llamada, de modo que el país de destino pueda identificar al operador/proveedor de servicios de la llamada saliente, o la terminal de
4. de donde procede la llamada, antes de que se curse la llamada en el país de destino;

[167] Resolución 61 *Countering and combating misappropriation and misuse of internationaltelecommunication numbering resources*; Unión Internacional de las Telecomunicaciones; marzo de 2022

5. Ratificar que el OI en un entorno de red heterogéneo será, en la medida en que sea técnicamente posible, un identificador asignado por el proveedor de servicios de origen a un abonado, o un identificador asignado por el proveedor de origen para identificar el origen de la llamada;
6. Ratificar que el CPN, la CLI y la información de OI se deben transmitir de manera transparente por las redes de tránsito;
7. Alentar a los operadores a que establezcan procedimientos que aseguren que la información de la OI, cuando sea procedente, el CPN y la CLI sea fiable y verificable, con objeto de luchar contra la falsificación y otras formas de uso indebido de la numeración;
8. Encargar a la Comisión de Estudio 2, a la Comisión de Estudio 3 y, llegado el caso, a las Comisiones de Estudio 11 y 17 de la UIT-T, a continuar estudiando aspectos relativos al envío del CPN, la CLI y la OI, con particular atención en entornos de red
9. Heterogéneos, contemplando mecanismos de seguridad y técnicas de validación, con el fin de reducir al mínimo el fraude;
10. Ordenar a la TBS a informar los avances logrados por las Comisiones de Estudio sobre los avances en estos aspectos;
11. Ordenar a la TBS a difundir información sobre las experiencias de los países en relación con las medidas adoptadas para requerir y/o solicitar el envío del CPN, CLI y/u OI;
12. Invitar a los Estados Miembro a compartir sus experiencias en relación con las medidas adoptadas para requerir y/o solicitar el envío del CPN, CLI y/u OI; e
13. Invitar a los Estados Miembro a contemplar la elaboración de directrices, lineamientos u otro tipo de instrumentos para requerir y/o solicitar el envío del CPN, CLI y/u OI.