



Bogotá, 4 de agosto de 2025

Doctora
CLAUDIA XIMENA BUSTAMANTE OSORIO
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
Ciudad.

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

Cordial saludo,

En atención a la publicación para comentarios del documento indicado en el Asunto, COMCEL presenta los siguientes comentarios:

1. COMENTARIOS GENERALES:

El documento de la CRC titulado *"Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles"* presenta un diagnóstico sobre el creciente fenómeno de fraude digital a través de llamadas de voz y mensajes SMS en Colombia, e identifica como problema central la **ausencia de herramientas regulatorias eficaces** para prevenir el contacto con fines fraudulentos mediante servicios tradicionales, situación que se ha agravado por el incremento sostenido de delitos informáticos y quejas de usuarios.

Asimismo, la Comisión señala que *"esta problemática desborda su marco competencial"*, y que la solución a esta problemática requiere una "estrategia conjunta, intersectorial e incluso con participación del sector privado, señalando de manera adicional que la comisión de fraude implica elementos que trascienden su capacidad regulatoria, como delitos penales, tratamiento indebido de datos personales o acciones judiciales.

En virtud de lo anterior, la CRC propone una serie de alternativas regulatorias y no regulatorias enfocadas en fortalecer la trazabilidad de las comunicaciones, ajustar el régimen de numeración y promover el uso de tecnologías de detección como la inteligencia artificial. Sin embargo, la CRC desconoce que tiene herramientas para mitigar la mayor parte del fraude que hoy nos vemos enfrentados, en el que la fuente de fraude proviene de los PCA o IT y envían estos mensajes con contenido fraudulento al usuario final, sin ningún tipo de control o mitigación.

Es decir, si se finalizan las relaciones o contratos de acceso entre PCA y/o IT y PRST al constatar reincidencia y la conducta sistemática fraudulenta y la recuperación de códigos cortos por indebido



uso de la numeración al enviar mensajes con contenido fraudulento, de manera ágil y expedita sin demoras innecesarias, los usuarios no recibirían este tipo de mensajes.

Al respecto, es importante indicar que COMCEL se ha tomado la tarea de denunciar este tipo de conductas encontrando algunas demoras por parte de la CRC en la recuperación de códigos cortos, e impidiendo la terminación de contratos de PCA, aun cuando se ha demostrado la reincidencia de parte de IT o de PCA en el envío de mensajes con contenido fraudulento. Esta situación ha permitido que estos PCA, una vez notificados de la recuperación del código corto, utilicen los demás códigos asignados para enviar a través de dicho código los mensajes fraudulentos, y continuar con el fraude.

CASO HÁBLAME:

Caso puntual el que se presenta con el PCA HÁBLAME, es un operador que presuntamente i) no implementa ninguna medida de control con sus clientes, ii) no implementa herramientas tecnológicas para prevenir que se cometan fraudes en el contenido emitido.

De la misma manera, las actuaciones administrativas solicitadas no han tenido ninguna consecuencia. Adicionalmente la CRC le otorgó numeración no geográfica y la modalidad de fraude está migrando a este escenario.

Así las cosas, COMCEL en el documento de respuesta a la consulta pública realizada por la CRC en el mes de junio de este año, hizo un recuento i) de las denuncias penales interpuestas en contra de háblame, ii) de las solicitudes de terminación de la relación de acceso, y iii) de las denuncias para la recuperación de códigos cortos, las cuales, como se ha indicado, no han sido resueltas de manera efectiva.

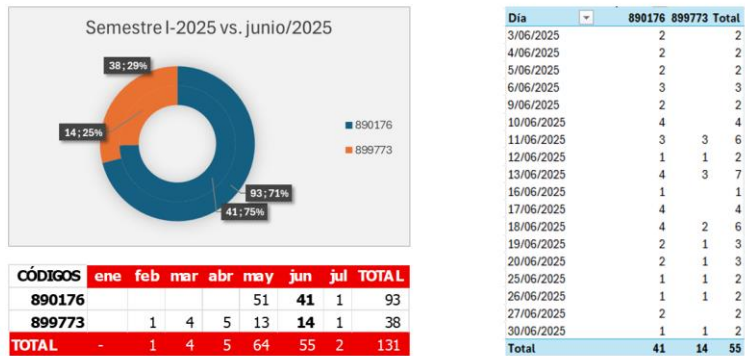
Con el fin de adicionar lo presentado en documento anterior, a título de ejemplo se presentan las estadísticas de los mensajes con contenido presuntamente fraudulento tanto de estafa comercial, bancaria como información presuntamente falsa de supuestos descuentos en la facturación y la suplantación del portal de pagos de CLARO remitida por mediante los códigos 890176 y 199773, teniendo en cuenta la cantidad mensual del primer semestre-2025 y la cantidad diaria de reportes realizados a HÁBLAME en junio-2025, en el cual se evidencia un comportamiento de crecimiento de manera considerable.



CMA HÁBLAME – SMS Orígenes 890176 y 899773



2. Cantidad de notificaciones enviadas al PCA en el Semestre 1-2025 y diarias en el último mes:



CMA HÁBLAME – SMS Orígenes 890176 y 899773



1. SMS recibidos por usuarios Claro:
- Smishing
 - Phishing

Suplantación Portal Pagos Claro:

Fraude Estafa Bancario/Ingeniería social:

Suplantación Portal Pagos Claro:

Fraude Estafa Bancario/Ingeniería social:

Adicionalmente, los mensajes remitidos por HÁBLAME, así hagan uso de códigos cortos que han sido asignados a otros, remite al dominio de HÁBLAME en la URL abreviada que resuelve a Phishing (hab.me) para mayor ilustración el presente ejemplo:



El 13 de julio de 2025, por parte del código corto: 890176, se recibe un correo con contenido presuntamente fraudulento, el cual remite a la página: hab.me



El código corto 890176 es asignado a A2P COLOMBIA SAS

GOV.CO



COMISIÓN
DE REGULACIÓN
DE COMUNICACIONES
REPUBLICA DE COLOMBIA



SISTEMA DE INFORMACIÓN Y GESTIÓN
DE RECURSOS DE IDENTIFICACIÓN
SIGRI

InicioConceptos▼Atribuciones▼Numeración E.164SeñalizaciónCódigos cortosMNCIIN1XYCOLDNRN#ABB

Códigos Cortos SMS

Inicio / Códigos Cortos SMS

Búsqueda

Proveedor

Estado

Modalidad

Código Corto890176

Borrar todos los filtros

Consultar

Exportar consulta

1 registros encontrados20

(1 of 1)

1

	CÓDIGO CORTO	MODALIDAD	ESTADO	EMPRESA
	890176	GRATUITO PARA EL USUARIO	ASIGNADO	A2P COLOMBIA SAS

Y la URL redirecciona al dominio de HABLAME, de la siguiente manera:



Así las cosas, y no obstante las solicitudes de terminación de la relación de acceso entre COMCEL y HABLAME la CRC ha decidido mantener las relaciones de acceso establecidos entre PRSTM y PCA y/o IT, aun cuando el usuario final es el perjudicado y defrauda directamente a COMCEL, en esta relación.

Así las cosas, se hace un llamado a la CRC con la finalidad de adoptar las medidas adecuadas dentro del marco de su competencia de acuerdo a la problemática que tienen los usuarios y los PRSTM.

Finalmente, vale la pena indicar que la numeración se asigna con el fin de cumplir criterios de necesidad del proveedor para poder prestar de manera eficiente y bajo el ámbito de la legalidad, los servicios de telecomunicaciones. Aunado a lo anterior, el operador se encuentra obligado a utilizar estos recursos de manera óptima, adecuada y eficientemente, con el fin de generar competencia y no hacer usos que impliquen distorsiones o usos inadecuados para con los demás PRST que concurren en el sector.

SOBRE SPOOFING:

Sobre el SPOOFING DE ROBOCALLS en tráfico internacional entrante, el cual fue denunciado por COMCEL en la respuesta a la consulta sectorial de junio de 2025, la CRC no presenta una línea de análisis técnico o regulatorio específico que aborde medidas concretas sobre ese tipo de conductas. Así las cosas, no lo desarrolla ni como eje del problema ni como foco de soluciones regulatorias.



Así las cosas, nuevamente se pone de presente que se ha identificado un patrón de suplantación de identidad a través de llamadas de voz, caracterizado por un alto volumen de llamadas internacionales que son terminadas en usuarios nacionales con numeración nacional (enmascaramiento de la numeración), con el objetivo de engañar a los usuarios y lograr que respondan dichas llamadas. A través de esta modalidad se realizan innumerables fraudes a los usuarios con el presunto fin de robar su información personal, falsearla y realizar actos delictivos.

Es necesario que el regulador expida una regulación orientada a controlar este tipo de fraude. Por lo tanto, se solicita que el regulador permita a los PRSTM el bloqueo de las llamadas internacionales que utilicen números locales y utilizar la numeración asignada para las llamadas de LDI.

Así las cosas, y a título de conclusión:

- Aunque se contemplan medidas de trazabilidad, control y monitoreo, el marco actual no disuade suficientemente a los PCA/IT reincidentes en malas prácticas.
- No se impone una consecuencia directa y contundente sobre la relación de acceso entre el infractor y los operadores de red.
- La reincidencia no tiene consecuencias. El regulador propone recuperar códigos cortos por mal uso, pero no vincula directamente esta reincidencia con consecuencias en la relación, aun cuando afecta directamente a uno de los operadores en dicha relación.
- Esto genera incentivos perversos: el costo de reincidir puede ser menor al beneficio económico obtenido por facilitar fraude.
- Mientras persista la posibilidad de seguir operando tras múltiples recuperaciones de numeración, el incentivo al cumplimiento regulatorio es débil.
- La reincidencia sistemática en el uso indebido de códigos cortos demuestra una fallida gestión interna de seguridad por parte del PCA o IT.
- Las prácticas fraudulentas no solo afectan a usuarios, sino que también debilitan la integridad del ecosistema de telecomunicaciones, al erosionar la confianza en los canales tradicionales como el SMS y la voz.
- La repetida intervención del regulador para recuperar numeración demuestra un patrón, no una falla aislada.

En virtud de lo anterior, COMCEL reitera que la solución a esta problemática es la posibilidad de autorizar la terminación la relación de acceso cuando un PCA o IT haya sido objeto de recuperación reiterada de códigos cortos, por causas asociadas al uso indebido con fines fraudulentos. Con esta solución, el medio técnico se cierra, el tráfico del infractor ya no puede circular por la red, y se interrumpe la recurrencia del fraude.



2. COMENTARIOS PARTICULARES:

2.1. 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?

El problema planteado por la CRC no parte del usuario como centro del perjuicio. En virtud de lo anterior, solicitamos reformular el problema con el fin de hacer visible que el fraude es una externalidad del modelo actual de acceso a la red y que al no interrumpirlo, perpetúa la exposición del usuario a un entorno inseguro:

“Persistencia de canales habilitados para la comisión de fraudes a usuarios mediante servicios móviles, debido a la falta de consecuencias efectivas frente a agentes reincidentes.”

b) Frente al problema planteado, ¿por qué considera que las causas presentadas en este documento son las que generan el problema definido?

Las causas mencionadas deben complementarse. Se debe incluir i) la falta de consecuencias estructurales frente a la reincidencia, ii) el vacío regulatorio y la inhabilitación a los PRSTM para implementación de medidas de control, permiten la propagación y crecimiento exponencial de los fraudes de voz y SMS. Iii) imposibilidad de terminar relación de acceso con PCA o IT reincidente en el envío de SMS con contenido fraudulento.

c) Frente al problema planteado, ¿por qué considera que las consecuencias expuestas en el presente documento tienen relación directa con la materialización del problema?

Las consecuencias expuestas en el documento de la CRC tienen una relación directa, clara y verificable con la materialización del problema identificado: la ausencia de herramientas regulatorias para prevenir el contacto a usuarios con fines fraudulentos mediante servicios tradicionales de voz y mensajes de texto.

No obstante lo anterior, se solicita adicionar las siguientes consecuencias: i) Incremento en los costos operativos de mitigación. Las empresas deben invertir en soluciones tecnológicas como firewalls, IA, monitoreo de tráfico, auditorías y personal especializado para suplir la ausencia de consecuencias para el PCA o IT infractor por el envío de mensajes con contenido presuntamente fraudulento. li)Continuidad en la relación de acceso entre PCA y/o IT y PRSTM.



2. Respetto 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?

Se considera que el documento de la CRC identifica a la mayoría de los grupos de valor relevantes. Sin embargo, existen otros actores que deberían ser incluidos en el desarrollo del presente proyecto regulatorio, debido a su rol estratégico en la prevención, detección y mitigación del fraude cibernético:

- Plataformas de mensajería y agregadores internacionales. Muchos fraudes se originan desde plataformas o rutas internacionales (A2P SMS, OTTs, etc.). La regulación debe considerar cómo se integran estos actores en la cadena de valor y cómo se les puede exigir trazabilidad, autenticación de remitentes, responsabilidad y cumplimiento de normas locales.
- Entidades del sector educativo y académico (universidades, centros de investigación) pueden apoyar en el diseño de campañas de sensibilización digital y estudios de impacto del fraude. Su participación puede fortalecer la base técnica y metodológica de las medidas regulatorias.
- Medios de comunicación y plataformas digitales. Son canales clave para la difusión de alertas de fraude, campañas de prevención y educación al usuario. Su inclusión puede potenciar el alcance de las estrategias pedagógicas propuestas por la CRC.

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

a) En relación con el uso indebido de la numeración de códigos cortos:

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?

La implementación de un registro de remitentes de mensajes cortos de texto (SMS) que utilice códigos alfanuméricos para su identificación, así como la identificación de las campañas de comercialización o publicidad asociadas, no garantiza que el envío de SMS con contenido fraudulento deje de presentarse, así mismo, integra desafíos operativos y técnicos que deben ser considerados, si se tiene en cuenta que los PRSTM son los que han realizado cuantiosas inversiones en soluciones tecnológicas como firewalls, IA, monitoreo de tráfico, auditorías y personal especializado para suplir la ausencia de consecuencias para el PCA o IT infractor por el envío de mensajes con contenido presuntamente fraudulento.

A la fecha, y si se revisa el sistema de información y gestión de recursos de identificación SIGRI (<https://www.pnn.gov.co/mapa/>) se evidencia el asignatario de la numeración, en este sentido ya se



conoce el remitente de la información. Esta idea introduciría a un tercero en la ecuación atomizando aun más la responsabilidad en el envío de los mismos. Sumado a lo anterior, la propuesta no da muestras de solucionar la problemática, es decir que no se dejen de remitir mensajes con contenido presuntamente fraudulento.

Adicionalmente, la exigencia de registro y validación previa podría representar una barrera de entrada para actores de menor escala que utilizan los SMS como canal de comunicación legítimo, afectando la equidad en el acceso a estos recursos.

Finalmente, la efectividad del registro depende de la articulación entre operadores móviles, proveedores de contenido, integradores tecnológicos y autoridades como la CRC y la SIC. La falta de estandarización o interoperabilidad podría limitar su eficacia.

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?

Consideramos que la solución propuesta por la CRC no soluciona la problemática planteada, y si genera costos de adecuación tecnológica, necesidad de supervisión y auditoría continua, toda vez que el éxito del registro dependerá de su actualización permanente, la verificación de la información registrada y la imposición de sanciones en caso de incumplimiento.

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?

Antes de proponer esta alternativa, es necesario que la CRC sea consciente de que el problema del envío de mensajes con contenido presuntamente fraudulento NO opera para todos los PCA y/o IT, que son unos pocos los que hacen caso omiso de las obligaciones regulatorias existentes.

Dar aplicación a la propuesta de la CRC impactaría negativamente el ecosistema de mensajería empresarial (A2P), que actualmente utiliza enlaces como mecanismo esencial para:

- Confirmación de transacciones (OTP).
- Redirección a portales de autoservicio o atención al cliente.
- Promociones comerciales y campañas de marketing digital.
- Activación de servicios o descarga de aplicaciones.

En virtud de lo anterior, solicitamos a la CRC descartar de plano esta alternativa.



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?

Respecto de si la cantidad disponible de numeración de códigos cortos es suficiente, bajo la propuesta de la CRC, es este organismo quien debe proceder con la respuesta. No obstante, la asignación exclusiva por entidad y modalidad (sector – entidad / comercio – notificación / campaña) podría generar una presión significativa sobre la disponibilidad de códigos cortos, especialmente en sectores con alta demanda como el financiero, el comercio electrónico y los servicios públicos. Si bien el documento técnico no reporta una escasez inmediata, esta medida podría acelerar el agotamiento de rangos disponibles.

Consideramos innecesaria la propuesta de prohibir la intermediación o reventa del uso de numeración de códigos cortos por parte de los asignatarios, y establecer su uso exclusivo por remitente y modalidad, toda vez que a la fecha y de acuerdo a la experiencia de COMCEL, el envío de mensajes con contenido fraudulento, a la fecha solo se presenta con unos pocos PCA o IT, los cuales, en la mayoría de los casos, una vez advertidos del posible envío de mensajes con contenido presuntamente fraudulento restringen el envío de lo mismos. Situación diferente pasa con HABLAME, quien posiblemente no ha implementado las medidas necesarias en seguridad de la información.

Así mismo, esta propuesta afectaría a muchos proveedores de contenido y aplicaciones (PCA) que operan bajo esquemas de intermediación, en los que un mismo código corto es utilizado por múltiples entidades o comercios y que si hacen la tarea de implementar medidas tecnológicas que impidan el envío de SMS con contenido fraudulento.

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?

La implementación de numeración E.164 para servicios A2P requeriría ajustes en las plataformas de mensajería, sistemas de enrutamiento, bases de datos de asignación y mecanismos de validación de remitentes, tanto por parte de los operadores como de los proveedores de contenido y aplicaciones.



Adicionalmente, se generaría un impacto negativo a los usuarios, toda vez que los códigos cortos son fácilmente reconocibles y recordables por los usuarios. La migración a numeración E.164 podría generar confusión inicial o menor recordación.

Por otro lado, al eliminar la posibilidad de compartición del recurso, se verán impactados los modelos de intermediación actualmente utilizados por integradores tecnológicos y PCA, lo que podría generar barreras de entrada para actores de menor escala.

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.

Desde la perspectiva de prevención del fraude en los servicios móviles, además de las medidas ya contempladas en el documento de formulación del problema, se considera pertinente proponer las siguientes alternativas regulatorias complementarias, orientadas a fortalecer el control, la trazabilidad y la seguridad en el uso de la numeración de códigos cortos para el envío de mensajes cortos de texto (SMS):

1. La posibilidad de terminar, suspender o desconectar los acuerdos de acceso con PCA o IT reincidentes en recuperación de numeración ya sea un código corto o 940.
2. Establecimiento de sanciones proporcionales y progresivas por uso indebido del recurso. Revisar y fortalecer el régimen sancionatorio aplicable a los asignatarios de códigos cortos que incurran en uso indebido, incluyendo la terminación de las relaciones de acceso, la suspensión temporal del recurso.

Un régimen sancionatorio más estricto y visible generaría un efecto disuasivo y promovería el cumplimiento de las obligaciones regulatorias

3. Campañas obligatorias de educación digital y prevención del fraude en cabeza de los PCA e IT.
Establecer la obligación para los operadores móviles, PCA e IT de realizar campañas periódicas de educación a los usuarios sobre cómo identificar mensajes fraudulentos, reportarlos y proteger su información personal.

b) Respecto del uso inadecuado de la numeración E.164:

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?



La implementación de un sistema de identificación alfanumérica y de registro de campañas requeriría ajustes en las plataformas de gestión de llamadas, bases de datos de numeración, sistemas de enrutamiento y herramientas de monitoreo, por parte de los operadores como de los originadores, aumentando los costos en los cuales los operadores han tenido que incurrir para controlar el envío de mensajes con contenido fraudulento. El hecho del registro no garantiza que los mensajes con contenido fraudulento no se envíe.

Como se ha indicado a lo largo de este documento, y de acuerdo a las denuncias y solicitudes de recuperación de códigos cortos, en la práctica procede de unos pocos PCA o IT. En este sentido lo recomendable es NO cargar más a los que si cumplen las directrices de la regulación, y en cambio de ello, se permita terminar la relación de acceso para los reincidentes en recuperación de códigos cortos. Como se indicó anteriormente, si la regulación es clara con las sanciones que se deben aplicar, y la sanción es efectiva, se termina con la conducta.

Asimismo, la exigencia de rangos exclusivos y el registro de campañas podría representar una carga operativa y económica para pequeñas y medianas empresas que utilizan llamadas comerciales como canal de contacto legítimo. Se recomienda que la CRC contemple esquemas diferenciados o progresivos para estos actores.

Finalmente, no es claro como la exigencia de registrar una campaña, evita que el mensaje con contenido fraudulento se envíe.

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?

La efectividad de esta propuesta depende en gran medida de que estas técnicas sean complementadas con acciones regulatorias específicas que fortalezcan el control sobre el uso de los recursos de identificación.

El filtrado inteligente de tráfico, basado en análisis de patrones, inteligencia artificial y aprendizaje automático, permite detectar comportamientos anómalos en tiempo real, como volúmenes inusuales de llamadas, intentos de suplantación de numeración (spoofing). El screening permite bloquear llamadas o mensajes antes de que lleguen al usuario, lo que reduce significativamente la exposición a fraudes como el vishing o el smishing. Esta capacidad de respuesta inmediata es especialmente valiosa en contextos donde los usuarios no cuentan con conocimientos técnicos suficientes para identificar amenazas.

No obstante lo anterior, su implementación aislada no es suficiente. Se requiere un marco regulatorio que:



a. Establezca obligaciones claras sobre el uso de numeración E.164

Es necesario definir reglas específicas sobre la asignación, uso exclusivo, trazabilidad y recuperación de numeración E.164, especialmente en el NDC 940, para evitar su uso compartido o no autorizado.

“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”.

Desde la perspectiva de prevención del fraude en los servicios móviles, se debe fortalecer el régimen sancionatorio por uso indebido de numeración.

Un régimen sancionatorio más estricto y visible generaría un efecto disuasivo y promovería el cumplimiento de las obligaciones regulatorias. Este régimen debe comprender, la no asignación de mas numeración, y la terminación de las relaciones de acceso.

Este régimen sancionatorio debe tener alcance a los carriers internacionales que solicitan acceso a los PRSTM por uso de la numeración móvil y fija Colombiana en las llamadas internacionales entrantes.

“c) En relación con el desconocimiento de los usuarios sobre privacidad de la información técnicas de ingeniería social:”

“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?”

Desde la perspectiva de prevención del fraude en los servicios móviles, se considera altamente pertinente y necesaria la adopción de una medida regulatoria que imponga obligaciones de divulgación pedagógica y de prevención en cabeza de los Proveedores de Contenidos y Aplicaciones (PCA) e Integradores Tecnológicos (IT).

- La divulgación pedagógica permite que los usuarios reconozcan señales de alerta, comprendan sus derechos y adopten medidas preventivas frente a fraudes como el smishing, vishing o spoofing.
- Una ciudadanía informada es menos susceptible a caer en engaños. La educación digital es una herramienta clave para reducir la efectividad de campañas fraudulentas.
- Al imponer obligaciones a PCA e IT, se reconoce que la seguridad del ecosistema no depende únicamente del usuario, sino de todos los actores que intervienen en el flujo



de la comunicación; de hecho, la responsabilidad debe recaer sobre los originadores de estas prácticas fraudulentas, no sobre los usuarios.

“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?”

Desde la perspectiva de prevención del fraude en los servicios móviles, la creación de un portal público administrado por la Comisión de Regulación de Comunicaciones (CRC), que consolide una “lista negra” de recursos de identificación (numeración E.164 y códigos cortos) más denunciados por los usuarios o identificados de oficio por la autoridad, no soluciona la problemática que día a día sufren los usuarios de telecomunicaciones. El desconocimiento de estas medidas por parte del usuario común hace que la misma no genere aspectos positivos. Adicionalmente, es pertinente resaltar que este tipo de iniciativas de listas negras, están proscritas en el ordenamiento jurídico y su creación debe ser del orden legal, haciendo una revisión de constitucionalidad de su origen.

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

La creación de un sistema intersectorial centralizado administrado por la CRC presenta riesgos y desventajas significativas que cuestionan su viabilidad y conveniencia.

1. Extensión del Rol de la CRC:

La CRC, como ente regulador, tiene funciones claras de regulación y vigilancia, pero no está diseñada operativamente para asumir funciones ejecutivas o administrativas directas sobre la gestión diaria de las PQRD a nivel intersectorial. Centralizar en la CRC la administración de este sistema puede desdibujar sus roles regulatorios y generar duplicidad de funciones con otras entidades ya encargadas de tramitar las PQRD.

2. Pérdida de eficiencia y riesgo de burocratización

Centralizar la trazabilidad y las PQRD en un único sistema gestionado por la CRC podría generar cuellos de botella y procesos más lentos. Cada sector (telecomunicaciones, postal, TI, etc.) tiene particularidades técnicas y operativas distintas, y la homogeneización excesiva podría perjudicar la agilidad y pertinencia de la atención al usuario.

3. Riesgos de seguridad y protección de datos

Un sistema centralizado de trazabilidad de recursos de identificación y de PQRD implicaría la consolidación de grandes volúmenes de datos personales sensibles en una sola plataforma. Esto



aumenta el riesgo en términos de ciberseguridad y posibles vulneraciones a la protección de datos, especialmente si se considera que múltiples sectores con distintos niveles de madurez digital estarían integrados en una única solución.

4. Desalineación con el principio de subsidiariedad y descentralización

En lugar de fortalecer las capacidades sectoriales para gestionar sus propias trazabilidades y responder a los usuarios, esta propuesta puede generar una excesiva dependencia de un solo ente regulador, lo cual va en contra de los principios de descentralización y autonomía operativa de cada sector involucrado.

5. Costo de implementación y sostenibilidad

El desarrollo, implementación, mantenimiento y actualización de un sistema intersectorial de este tipo representa una inversión significativa de recursos técnicos, financieros y humanos, cuya sostenibilidad en el tiempo no está garantizada. Además, no queda claro si este costo será asumido por la CRC, trasladado a los operadores o financiado con recursos públicos, lo que podría generar resistencias y conflictos entre los actores involucrados.

En conclusión, aunque el objetivo de mejorar la trazabilidad y la experiencia del usuario es legítimo, la creación de un sistema centralizado intersectorial administrado por la CRC podría generar más problemas que soluciones, tanto a nivel institucional, operativo, de seguridad y sostenibilidad. Una alternativa más viable sería fortalecer las capacidades sectoriales existentes y promover la interoperabilidad entre sistemas ya desarrollados, en lugar de concentrar todo en una única plataforma.

“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”.

Desde la perspectiva de prevención del fraude en los servicios móviles, se considera que el empoderamiento del usuario es un pilar fundamental en la estrategia de mitigación del fraude cibernético. El usuario se empodera si tiene conocimiento de este flagelo.

“d) Sobre la revisión integral del Régimen de Recursos de Identificación

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

Desde la perspectiva de prevención del fraude en los servicios móviles, se considera que la revisión integral del Régimen de Recursos de Identificación debe orientarse no solo a asegurar el uso eficiente de estos recursos, sino también a fortalecer su trazabilidad, seguridad y control frente a usos indebidos, especialmente en el contexto del fraude cibernético mediante servicios móviles.



En ese sentido, se presentan las siguientes propuestas para optimizar los procedimientos de asignación y recuperación de los recursos de identificación, en particular la numeración E.164 y los códigos cortos:

1. Implementación de un sistema de evaluación de riesgo previo a la asignación

Incorporar un componente de análisis de riesgo en el proceso de asignación, que considere antecedentes del solicitante, historial de uso de recursos, cumplimiento normativo y posibles impactos sobre la seguridad del ecosistema.

2. Fortalecimiento del procedimiento de recuperación por uso indebido

Agilizar los tiempos del procedimiento de recuperación, establecer causales adicionales específicas relacionadas con fraude o suplantación, e incorporar mecanismos de suspensión preventiva del recurso mientras se resuelve el proceso. Dicho proceso debe terminar con la posibilidad de finalizar los contratos de acceso entre PRSTM y PCA e IT.

A título de conclusión, observamos que la CRC con sus propuestas busca gravar más, e imponer obligaciones a los PRST, los cuales han implementado herramientas para identificar el envío de mensajes con contenido fraudulento, desconociendo que el problema se soluciona fácilmente si permite la suspensión provisional o la terminación definitiva de la relación de acceso por indebido uso de la numeración. Así las cosas, si el PCA o IT no puede enviar mensajes con contenido fraudulento, se da fin a la controversia.

En virtud de lo anterior, el problema se soluciona de raíz, propiciando un escenario de simplificación regulatoria, si simplemente se autoriza la terminación de las relaciones de acceso entre PRSTM PCA o IT o por el envío de mensajes, o la realización de llamadas con contenido fraudulento.

Cordialmente,

Firmado por:

Santiago Pardo Fajardo

C8E4C986876A45F...

Inicial
MTG

SANTIAGO PARDO FAJARDO
DIRECTOR CORPORATIVO JURIDICO Y DE SOSTENIBILIDAD