Doctora
CLAUDIA XIMENA BUSTAMANTE
Directora Ejecutiva
COMISIÓN DE REGULACIÓN DE COMUNICACIONES -CRC
medidasantifraude@crcom.gov.co;
atencioncliente@crcom.gov.co;
Calle 59A Bis Nº 5-53 Edificio Link Siete Sesenta Ciudad

Referencia: Identificación de medidas para mitigar fraude cibernético por medio de servicios móviles.

Introducción

En el marco del proyecto regulatorio orientado a la mitigación del fraude, resulta indispensable que el análisis del problema y la evaluación de alternativas regulatorias consideren el funcionamiento real y actual del ecosistema de comunicaciones, así como los impactos económicos, operativos y sociales que pueden derivarse de la adopción de medidas generales sobre el tráfico de voz.

Una proporción significativa del tráfico de llamadas que actualmente ingresa al país a través de rutas de larga distancia internacional (LDI) corresponde a **comunicaciones empresariales legítimas**, particularmente aquellas asociadas a **procesos de gestión y cobro de cartera del sector financiero**. Este tipo de llamadas se realiza en el marco de **relaciones contractuales preexistentes entre las entidades financieras y los usuarios**, y cuenta con **autorizaciones expresas otorgadas por estos últimos para la recepción de dichas comunicaciones**, en cumplimiento de la normativa vigente sobre protección de datos y contacto con clientes.

En la práctica, gran parte de estas comunicaciones se origina en **plataformas tecnológicas especializadas en gestión de contact center, cobranzas y comunicaciones empresariales**, cuya infraestructura se encuentra mayoritariamente ubicada fuera del territorio nacional y que utilizan carriers internacionales para cursar las llamadas hacia las redes colombianas mediante rutas LDI. Entre este tipo de soluciones se encuentran plataformas como **Genesys Cloud**, **Amazon Connect**, **Microsoft Teams Phone**, **Twilio** y **Google Cloud Voice**, entre otras plataformas IP de alcance global.

Como resultado de este esquema operativo, es técnicamente posible y plenamente legítimo que las llamadas presenten **numeración nacional (CLI colombiano)** aun cuando su origen técnico se encuentre en infraestructura internacional, sin que ello implique, por sí mismo, prácticas de suplantación o fraude. Este modelo responde a la evolución natural de los servicios de voz hacia

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

arquitecturas basadas en IP y en la nube, y no puede ser evaluado únicamente desde la perspectiva de la ruta internacional o del identificador de la línea llamante.

En este contexto, la adopción de medidas regulatorias que no distingan adecuadamente entre tráfico fraudulento y tráfico empresarial autorizado puede generar **impactos negativos relevantes sobre el sector financiero**, al afectar la efectividad de los procesos de recuperación de cartera, incrementar los niveles de mora, deteriorar los indicadores de riesgo crediticio y trasladar mayores costos al sistema financiero y, en última instancia, a los usuarios finales. Adicionalmente, enfoques basados exclusivamente en la nacionalidad del CLI o en la ruta internacional del tráfico no abordan el problema estructural del fraude, asociado principalmente a la **limitada trazabilidad del origen técnico real en escenarios de tráfico internacional en cadena**.

Por lo anterior, resulta fundamental que las alternativas regulatorias que se evalúen reconozcan explícitamente la existencia de este tipo de tráfico legítimo, diferencien los perfiles de riesgo y privilegien enfoques proporcionales, basados en trazabilidad, monitoreo de comportamiento, cooperación entre los actores del ecosistema y esquemas de etiquetado informativo, de manera que se proteja al usuario final sin afectar de forma desproporcionada servicios esenciales para el funcionamiento del sistema financiero y de la economía en general.

A continuación, se presentan las respuestas a las preguntas formuladas por la Comisión de Regulación de Comunicaciones (CRC), desarrolladas con base en criterios técnicos, operativos y de proporcionalidad regulatoria, con el propósito de aportar insumos objetivos para la toma de decisiones regulatorias.

En el servicio de llamadas de voz, los operadores pueden gestionar tanto tráfico originado por acuerdos directos con clientes nacionales (por ejemplo, bancos, comercios, entidades de salud, aerolíneas), como tráfico internacional que llega a través de cadenas de intermediarios, donde el originador de la llamada no siempre es certificado o plenamente identificable. ¿Qué diferencias, riesgos y oportunidades observa entre estos dos tipos de tráfico en relación con la prevención y mitigación del fraude? ¿Qué criterios, mecanismos o medidas considera relevantes para gestionar de manera diferenciada el tráfico directo y el tráfico en cadena, especialmente en lo relacionado con la trazabilidad, autenticación, control de llamadas sospechosas y judicialización?

Respuesta

En el servicio de llamadas de voz, **desde la experiencia operativa de SSC**, no se identifican únicamente dos tipos de tráfico, sino **tres fuentes funcionales de origen claramente diferenciadas**, cada una con **perfiles de riesgo, capacidades de control y oportunidades de**

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

mitigación distintas frente al fraude. Reconocer esta diferenciación resulta **esencial** para el diseño de **medidas regulatorias efectivas, proporcionales y técnicamente viables**.

1. **Tráfico directo nacional**

Descripción

En el tráfico directo nacional, el elemento determinante **no es el PRST al que se le asignó originalmente la numeración**, sino el PRST que presta efectivamente el servicio y controla el origen técnico de la llamada.

En este esquema, el PRST provee el acceso a la red al cliente y gestiona el establecimiento, enrutamiento y terminación de la llamada dentro de su propia infraestructura. El recurso de numeración utilizado (CLI nacional) puede haber sido asignado al mismo PRST que provee el acceso o a otro PRST que fue el asignatario original del número, sin que ello afecte la legitimidad del servicio.

En escenarios plenamente legítimos como la portabilidad numérica, se **produce una separación entre el PRST asignatario original** del número y el **PRST que presta efectivamente el servicio**. En estos casos, es el operador receptor quien cursa técnicamente la llamada y mantiene el control y la trazabilidad del tráfico, de conformidad con los mecanismos vigentes de gestión y administración de la numeración.

En este esquema:

- El **PRST que presta el servicio** (por ejemplo, Claro, Movistar, Tigo, entre otros):
    - pone a disposición del cliente **numeración fija y/o móvil**, ya sea asignada directamente o heredada mediante portabilidad(móvil),
    - provee el **acceso a la red** (por ejemplo, mediante una troncal SIP o TDM),
    - y **controla el establecimiento, enrutamiento y terminación de la llamada**.

- Existe coincidencia entre:
    - el **titular legítimo del CLI nacional**,
    - el **origen técnico de la llamada**, y
    - el **operador que gestiona efectivamente el tráfico**,

independientemente de cuál PRST haya sido el asignatario original del recurso de numeración.

Riesgo.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

Bajo y controlable.

El operador cuenta con visibilidad completa del tráfico, capacidad de auditoría, suspensión inmediata ante comportamientos irregulares y soporte efectivo para procesos de investigación y judicialización. Adicionalmente, existe una base de datos centralizada de numeración, que permite identificar de manera precisa el PRST que presta efectivamente el servicio asociado a cada CLI nacional, reforzando la trazabilidad del origen y la asignación de responsabilidades en este tipo de tráfico.

Oportunidades de mitigación

- Controles contractuales y técnicos.
- Trazabilidad completa del origen.
- Evidencia técnica sólida para acciones correctivas y judiciales.

2. Trafico desde Plataformas OTT / CPaaS.

Descripción

Se trata de **llamadas plenamente legítimas originadas en plataformas tecnológicas globales**, que no cuentan con red propia en todos los países y que, por tanto, **utilizan carriers internacionales como medio de transporte** para cursar sus comunicaciones.

En estos esquemas, la **plataforma no es titular de la numeración**, sino que **presenta numeración asignada por PRST locales a sus clientes empresariales**, quienes contratan dichos números para realizar comunicaciones salientes. Este modelo genera una **separación entre la asignación del recurso de numeración y el origen técnico de la llamada**, análoga a lo que ocurre en la **portabilidad numérica**, con la diferencia de que dicha separación **no se materializa en otro operador de red**, sino en **infraestructura de plataforma basada en la nube**.

Como resultado, las llamadas pueden **presentar un CLI nacional**, aun cuando su **origen técnico se encuentre en infraestructura internacional de la plataforma**, como ocurre, a modo de ejemplo, con:

- **Google** (servicios de voz integrados a Google Cloud y soluciones empresariales),
- **Amazon** (servicios de voz prestados a través de Amazon Connect),
- **Microsoft** (servicios empresariales sobre Teams Phone),
- **Twilio** (servicios CPaaS y contact center en la nube),
- **Genesys Cloud**,

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- y otras **plataformas IP similares** que dependen de carriers internacionales para cursar llamadas hacia las redes nacionales.

Este tipo de tráfico representa actualmente un porcentaje mayoritario del tráfico de larga distancia internacional (LDI), **estimado en alrededor del 80 %**, y corresponde principalmente a **comunicaciones empresariales, transaccionales , de atención al cliente y cobranzas (NO PUBLICITARIAS o de VENTAS)**.

En cuanto el tráfico de cobranzas los se enmarcan en relaciones contractuales preexistentes y cuentan con autorización previa del usuario, por lo que no deben equipararse a llamadas comerciales o publicitarias.

Riesgos

El tráfico originado en plataformas OTT / CPaaS presenta un **riesgo intermedio**, superior al del tráfico directo nacional, pero **inferior al del tráfico internacional en cadena no identificado**, debido a que se trata mayoritariamente de **servicios empresariales legítimos**, aunque con **limitaciones estructurales de trazabilidad**.

Este riesgo se explica principalmente por:

- **Disociación entre numeración y origen técnico de la llamada.** La llamada se origina en infraestructura de plataforma basada en la nube, mientras que el **CLI nacional corresponde a numeración asignada a un cliente empresarial**, lo que introduce un reto de trazabilidad similar al observado en la portabilidad, pero sin una base centralizada equivalente que identifique al originador técnico del servicio.

- **Dependencia de carriers internacionales para el transporte.** Al no contar con red propia en todos los países, las plataformas dependen de **carriers internacionales**, lo que limita la visibilidad directa del PRST colombiano sobre el origen final del tráfico y puede retrasar la aplicación de medidas correctivas.

- **Posible aprovechamiento del modelo por actores maliciosos.** Aunque el modelo OTT / CPaaS es predominantemente legítimo, **puede ser utilizado de forma indebida** por terceros para ocultar su origen técnico y presentar CLI nacional válido, cuando no existen mecanismos adecuados de identificación y trazabilidad aguas arriba.

No obstante, este riesgo **no se deriva del uso de CLI nacional ni de la naturaleza de la plataforma**, sino de la **ausencia de mecanismos estandarizados de trazabilidad y asignación clara de responsabilidades** a lo largo de la cadena de prestación del servicio.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

Oportunidades de Mitigación.

Desde la perspectiva operativa de SSC, el tráfico originado en plataformas OTT / CPaaS presenta un **riesgo medio y gestionable**, por lo cual las medidas de mitigación deben ser **proporcionales, técnicas y focalizadas**, en concordancia con las alternativas regulatorias analizadas por la CRC, evitando enfoques de bloqueo generalizado que afecten tráfico empresarial legítimo.

En este contexto, se identifican las siguientes oportunidades de mitigación:

- **Fortalecimiento de la trazabilidad técnica del tráfico.** Resulta viable promover que las plataformas OTT / CPaaS, o en su defecto los carriers internacionales que transportan el tráfico, incorporen **información técnica mínima de trazabilidad**, que permita identificar el **origen técnico del servicio**, el **tipo de cliente** y el **esquema de control aplicado aguas arriba**. Este enfoque facilita la identificación de reincidencias, la aplicación de **medidas focalizadas** y la **asignación de responsabilidades**, sin requerir el bloqueo o alteración automática del **CLI nacional**, y es compatible con los esquemas de autenticación evaluados por la CRC (por ejemplo, STIR/SHAKEN/RCD), reconociendo sus limitaciones en entornos internacionales y de plataformas IP.

- **Etiquetado informativo y señalización al usuario final.** Cuando no sea posible verificar plenamente el origen del tráfico, resulta razonable priorizar **esquemas de etiquetado o señalización informativa**, en concordancia con las alternativas analizadas por la CRC, como mecanismo proporcional de protección al usuario y mitigación del riesgo, evitando medidas restrictivas generalizadas.

  En este contexto, SSC considera conveniente que los esquemas de etiquetado contemplen **etiquetas diferenciadas por niveles de confianza**, incluyendo:

  Etiquetas positivas (alto nivel de confianza):
  - *Empresa verificada*
  - *Origen empresarial identificado*
  - *Llamada autenticada*

  Etiquetas neutrales o informativas (confianza intermedia):
  - *Llamada no verificada*
  - *Origen internacional*
  - *Origen no autenticado*

  Etiquetas de advertencia (uso restringido y focalizado):
  - *Posible fraude*
  - *Riesgo elevado*

  Este enfoque incrementa la **transparencia para el usuario**, contribuye a la **prevención de la suplantación**, genera **incentivos para buenas prácticas** por parte de los actores del

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

ecosistema y permite mitigar el riesgo **sin afectar de manera desproporcionada la prestación de servicios legítimos**.

3. **Trafico Internacional , Cadena de Intermediarios.**

Descripción.

El tráfico internacional en cadena corresponde a llamadas que ingresan al país a través de uno o varios operadores internacionales de larga distancia (carriers), en las cuales el **PRST colombiano mantiene relación contractual y técnica únicamente con el operador inmediato anterior**, sin vínculo directo con el originador real de la llamada; durante su tránsito, estas llamadas atraviesan múltiples redes, agregadores y plataformas, lo que reduce la trazabilidad sobre el origen técnico y el cliente final, y permite que un mismo carrier transporte simultáneamente llamadas personales desde el exterior, tráfico de roaming internacional, comunicaciones empresariales legítimas, tráfico originado en plataformas OTT / CPaaS y, en menor proporción, tráfico abusivo, en un contexto en el que la adopción masiva de aplicaciones OTT ha desplazado las llamadas conversacionales tradicionales y ha hecho que el tráfico LDI actual esté compuesto mayoritariamente por comunicaciones empresariales legítimas cursadas a través de plataformas IP y carriers internacionales.

Ejemplos de este tipo de tráfico incluyen:

- Llamadas originadas por personas ubicadas en el exterior que contactan a usuarios en Colombia a través de redes internacionales.
- Llamadas asociadas a **roaming internacional**, en las que el usuario conserva su numeración nacional mientras la llamada se origina en una red extranjera.
- Comunicaciones empresariales legítimas cursadas a través de **carriers internacionales de larga distancia**, incluyendo servicios de atención al cliente, notificaciones y contacto transaccional.
- Tráfico originado en **plataformas OTT / CPaaS** que utilizan carriers internacionales como medio de transporte para cursar llamadas hacia redes nacionales, presentando numeración nacional (CLI nacional), aun cuando el origen técnico de la llamada se encuentra en infraestructura internacional.
- Tráfico que atraviesa múltiples redes y hubs internacionales antes de ingresar al país, con información limitada sobre el origen técnico real.

Riesgo: Alto.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

El tráfico internacional en cadena presenta un riesgo elevado debido a la **limitada trazabilidad del originador real de la llamada**, como resultado de la multiplicidad de intermediarios (carriers, agregadores y plataformas) involucrados en su transporte. Esta situación genera una **disociación entre el CLI presentado y el origen técnico efectivo**, aun en escenarios de tráfico legítimo, lo que reduce la capacidad del PRST colombiano para **identificar responsabilidades, aplicar controles directos y reaccionar oportunamente ante eventos de fraude**. En este contexto, el riesgo no se encuentra en la numeración ni en la ruta internacional en sí mismas, sino en la **opacidad del origen específico del tráfico**.

Oportunidades de Mitigación.

Con base en su experiencia operativa en la gestión de tráfico de voz, SSC considera que la mitigación efectiva del fraude debe fundamentarse en **medidas proporcionales, técnicas y focalizadas**, alineadas con la complejidad del ecosistema actual. En este sentido, SSC prioriza las siguientes alternativas:

- **Monitoreo y gestión de riesgo basada en comportamiento.** SSC recomienda fortalecer modelos de monitoreo del tráfico de voz que permitan identificar desviaciones significativas en patrones de uso, habilitando acciones preventivas y correctivas proporcionales. Este enfoque reduce falsos positivos y evita medidas generalizadas que afecten tráfico legítimo.

- **Etiquetado informativo y señalización al usuario final**. SSC recomienda priorizar esquemas de etiquetado informativo, tanto **positivos** (por ejemplo, "empresa verificada", "origen empresarial identificado") como **neutrales** (por ejemplo, "llamada no verificada", "origen internacional"), como alternativa eficaz a la prohibición o bloqueo de llamadas, en línea con los principios de transparencia y protección al usuario.

- **Cooperación interoperatorial e intercambio de alertas**. SSC recomienda la adopción de mecanismos de cooperación técnica y el intercambio oportuno de alertas entre PRST y otros actores del ecosistema, siempre bajo criterios técnicos verificables, gobernanza clara y protección de datos, como herramienta clave para la contención temprana del fraude.

¿Qué mecanismos, herramientas o procedimientos tiene actualmente implementados su organización para detectar, prevenir y controlar el spoofing en llamadas de voz? ¿Qué nivel de efectividad han observado en estas medidas y qué retos técnicos y operativos han enfrentado en su aplicación?

SSC cuenta con **mecanismos operativos de monitoreo continuo del tráfico de voz**, basados en el análisis de comportamiento (volúmenes, patrones horarios, destinos y rutas), que permiten identificar desviaciones asociadas a posibles eventos de suplantación. Adicionalmente, mantiene una

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

coordinación permanente con operadores de destino, de manera que, ante la notificación de tráfico originado en el exterior con comportamientos anómalos, **SSC aplica de forma inmediata bloqueos focalizados** sobre los números o flujos específicos reportados, gestionando la situación en el menor tiempo posible.

Asimismo, SSC mantiene **relaciones estables con clientes empresariales confiables**, lo que facilita la identificación de patrones legítimos y la detección temprana de desviaciones. Estas medidas han mostrado una **efectividad media a alta** en la contención de eventos de spoofing, particularmente cuando existe cooperación interoperatorial, aunque su alcance se ve limitado por la **trazabilidad disponible en tráfico internacional en cadena**, lo que representa el principal reto técnico y operativo.

¿Qué efectos positivos y negativos prevé en la prohibición de llamadas internacionales con identidad de línea llamante CLI nacional? ¿Qué excepciones o consideraciones deberían contemplarse para no afectar la prestación de servicios legítimos?

Desde la perspectiva de SSC, en línea con la posición del sector, la prohibición de llamadas internacionales con **CLI nacional** puede generar **beneficios limitados** frente a esquemas básicos de suplantación, pero **no garantiza una reducción efectiva del fraude** y conlleva **impactos negativos relevantes** sobre la prestación de servicios legítimos, por lo que **no resulta adecuada como medida generalizada**.

El **spoofing** consiste en la manipulación del identificador de la línea llamante para ocultar el origen real de la llamada, y **puede realizarse tanto con CLI nacional como internacional**. En consecuencia, centrar la mitigación en la nacionalidad del CLI **no aborda el problema estructural**, que es la falta de trazabilidad y autenticación del origen.

Ejemplo ilustrativo: un banco colombiano realiza llamadas de verificación de transacciones a sus clientes utilizando una plataforma en la nube que presenta **CLI nacional legítimo**, aunque el origen técnico de la llamada se encuentra en infraestructura internacional. Bajo una prohibición general, estas llamadas no serían cursadas, afectando un servicio válido. En contraste, un actor fraudulento podría continuar realizando llamadas con **CLI internacional**, eludiendo la medida y manteniendo el riesgo de suplantación.

Por lo anterior, SSC considera más efectivo priorizar **enfoques proporcionales**, basados en **trazabilidad, monitoreo de comportamiento, cooperación interoperatorial y esquemas de etiquetado informativo**, contemplando **excepciones para tráfico empresarial legítimo**, en lugar de prohibiciones generales basadas únicamente en la presentación del CLI.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema que permita el enmascaramiento de la identidad de la línea llamante CLI en llamadas internacionales, siempre que estas sean etiquetadas en el dispositivo del usuario como "No verificada" o "Probable fraude"? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la prevención del fraude, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

Desde la perspectiva de SSC, la implementación de un esquema que permita el **enmascaramiento del CLI en llamadas internacionales**, acompañado de **etiquetado informativo en el dispositivo del usuario**, representa una **oportunidad relevante y moderna** para fortalecer la protección del usuario y la prevención del fraude, siempre que se diseñe bajo criterios de proporcionalidad, trazabilidad y experiencia de usuario.

Ventajas e impactos positivos

- **Empoderamiento del usuario final.** El etiquetado permite que el usuario tome decisiones informadas sobre si atender o no una llamada, sin recurrir a bloqueos automáticos. Este enfoque es consistente con el uso extendido de soluciones de identificación de llamadas como **Truecaller**, **Google Call Screen / Verified Calls (Android)**, **Apple Call Identification & Silence Unknown Callers (iOS)** y **Hiya** (integrada en dispositivos Samsung y operadores en varios países), las cuales ya clasifican llamadas como spam, no verificadas o verificadas, y han demostrado ser efectivas para reducir la exposición al fraude.

- **Gestión de confianza, no solo de riesgo.** El esquema no debe limitarse a etiquetas negativas ("No verificada" o "Probable fraude"), sino que puede incorporar **etiquetas positivas**, tales como "Empresa verificada", "Llamada empresarial" o "Servicio de atención al cliente", que **incrementan la confianza del usuario** y preservan la contactabilidad de servicios legítimos.

- **Mitigación proporcional del fraude.** A diferencia de la prohibición o el bloqueo generalizado, el etiquetado reduce el impacto sobre tráfico legítimo y evita el desplazamiento del fraude hacia otros esquemas, contribuyendo a una mitigación más sostenible.

- **Alineación con tendencias internacionales.** Este enfoque es coherente con prácticas ya implementadas en ecosistemas móviles avanzados y con las alternativas analizadas por la CRC.

Retos y desafíos a considerar

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- **Definición clara y estandarizada de etiquetas.** Es fundamental establecer criterios técnicos y regulatorios homogéneos para la asignación de etiquetas, evitando interpretaciones inconsistentes entre operadores, plataformas y fabricantes de dispositivos.

- **Gobernanza y responsabilidad sobre la clasificación.** Debe definirse quién asigna, valida y actualiza las etiquetas (PRST, plataformas, terceros), así como los mecanismos de reclamación y corrección para evitar errores o afectaciones reputacionales.

- **Interoperabilidad técnica.** La efectividad del esquema depende de su integración con sistemas operativos, fabricantes de dispositivos y redes, así como de la compatibilidad entre tecnologías y mercados.

- **Experiencia de usuario.** Un exceso de etiquetas negativas puede generar fatiga o desconfianza generalizada; por ello, el esquema debe equilibrar advertencias con señales positivas de confianza.

Contribución a la protección del usuario y prevención del fraude

SSC considera que el **etiquetado informativo, combinado con enmascaramiento del CLI cuando no exista verificación suficiente**, constituye una **herramienta eficaz de protección al usuario**, al tiempo que preserva la prestación de servicios legítimos. Este enfoque permite reducir el impacto del fraude sin depender exclusivamente de bloqueos, y traslada la mitigación hacia un modelo de **gestión de confianza**, acorde con el ecosistema digital actual.

Listado sugerido de etiquetas (no exhaustivo)

- **Empresa verificada**
- **Llamada empresarial**
- **Servicio de atención al cliente**
- **Origen internacional**
- **Número no verificado**
- **Posible fraude**
- **Spam reportado por usuarios**

El etiquetado informativo no debe concebirse únicamente como una advertencia, sino como un mecanismo de gestión de confianza, ya adoptado por plataformas y sistemas operativos líderes, que permite proteger al usuario, preservar la contactabilidad y mitigar el fraude de manera proporcional y sostenible.

¿Qué oportunidades y retos identifica en la adopción de protocolos de autenticación comoSTIR/SHAKEN/RCD? ¿Qué condiciones técnicas y regulatorias serían necesarias para su implementación efectiva? ¿Considera que, con la implementación de este protocolo de autenticación, no resulta necesaria la implementación de medidas de filtrado de tráfico o listas de no originación (DNO)?

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

SSC considera que protocolos de autenticación como **STIR/SHAKEN/RCD** son útiles para verificar el identificador de llamadas cuando existe control sobre el origen de la llamada, pero **no son una solución completa**, especialmente en llamadas internacionales en cadena o provenientes de plataformas OTT / CPaaS, donde la autenticación no siempre es posible. Por esta razón, aun con la implementación de estos protocolos, **siguen siendo necesarias** otras medidas como el **monitoreo del tráfico basado en comportamiento**, el **intercambio de alertas entre operadores** y el uso **limitado y estandarizado** de listas de no originación (DNO). En consecuencia, SSC considera que la mitigación del fraude debe abordarse mediante un **enfoque combinado**, que use la autenticación como una herramienta más, y no como un sustituto de todas las demás medidas.

¿Qué parámetros y tecnologías considera más adecuados para estandarizar los modelos de monitoreo y filtrado de tráfico de voz? ¿Cómo garantizar que no se generen falsos positivos (que terminen afectando el tráfico legítimo), así como la protección de la privacidad de las comunicaciones y la proporcionalidad de las medidas?

SSC considera especialmente efectivo el **intercambio operativo de alertas entre PRST**, mediante el cual los operadores de destino notifican oportunamente la existencia de **quejas de usuarios o comportamientos anómalos asociados a numeraciones específicas**. Con base en estas alertas, SSC aplica **medidas de mitigación focalizadas**, tales como el bloqueo de los números reportados, evitando acciones generalizadas sobre rutas o rangos completos. Este mecanismo permite una **respuesta rápida, basada en evidencia**, reduce significativamente los **falsos positivos** y protege la prestación de servicios legítimos, constituyéndose en una práctica alineada con los principios de proporcionalidad y cooperación interoperatorial promovidos por la CRC.

¿Qué actores deberían participar en una plataforma nacional de intercambio de alertas sobre fraudes en llamadas? ¿Qué mecanismos de gobernanza y protección de datos serían necesarios?
¿Cuáles considera que serían los retos técnicos y económicos de construir y operar la plataforma de alertas bajo un modelo centralizado vs un modelo distribuido? ¿Qué mecanismos considera deben ser adoptados y estandarizados para validar la veracidad de una alerta antes de su distribución mediante la plataforma de intercambio?

Plataforma nacional de intercambio de alertas sobre fraude en llamadas de voz

Actores participantes

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

Desde la perspectiva de SSC, una plataforma nacional de intercambio de alertas sobre fraude en llamadas de voz debería contar, como mínimo, con la participación de los siguientes actores del ecosistema:

- **Proveedores de Redes y Servicios de Telecomunicaciones (PRST)** que gestionan tráfico de voz, incluidos operadores fijos, móviles y de larga distancia internacional, en su calidad de responsables de la gestión técnica del tráfico y de la aplicación de medidas de mitigación.
- **Operadores de destino**, en tanto son quienes reciben de manera directa los reportes y quejas de los usuarios finales y pueden identificar tempranamente eventos de fraude.
- **Proveedores de plataformas tecnológicas de comunicaciones**, tales como plataformas OTT, CPaaS o contact center en la nube, en la medida en que originan o gestionan volúmenes relevantes de tráfico de voz.
- **La Comisión de Regulación de Comunicaciones (CRC)**, en su rol de definición de lineamientos regulatorios, supervisión y seguimiento del funcionamiento del esquema, sin que ello implique necesariamente la operación técnica de la plataforma.
- **Autoridades competentes**, únicamente para efectos de investigación y judicialización, cuando exista fundamento legal y solicitud expresa.

SSC considera indispensable que la plataforma se rija por un esquema de gobernanza claro, que contemple, al menos, los siguientes elementos:

- **Finalidad específica y limitada**, orientada exclusivamente a la prevención y mitigación del fraude en llamadas de voz.
- **Intercambio de información mínima necesaria**, circunscrita a metadatos técnicos y operativos (por ejemplo, numeración involucrada, tipo de evento, ventana temporal y operador reportante), excluyendo el contenido de las comunicaciones.
- **Trazabilidad y responsabilidad sobre las alertas**, identificando el origen de la alerta, la fecha de reporte y los criterios técnicos utilizados.
- **Controles de acceso, auditoría y seguridad de la información**, que prevengan usos indebidos o no autorizados.
- **Cumplimiento de los principios de protección de datos personales**, en particular minimización, finalidad, proporcionalidad y retención limitada.

Modelo centralizado versus modelo distribuido

En relación con la arquitectura de la plataforma, SSC identifica las siguientes consideraciones:

- Un **modelo centralizado** puede facilitar una visión agregada del ecosistema y la aplicación uniforme de criterios, pero presenta retos asociados a mayores costos de implementación y operación, riesgos de concentración de información sensible y posibles cuellos de botella operativos.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- Un **modelo distribuido**, basado en estándares mínimos comunes de intercambio, permite una implementación más gradual, reduce costos, favorece la agilidad operativa y limita la concentración de datos sensibles, aunque requiere un mayor esfuerzo de coordinación y estandarización entre los actores.

Desde la perspectiva de SSC, un **modelo distribuido con lineamientos técnicos comunes definidos por la CRC** resulta más viable en términos técnicos y económicos, al menos en una fase inicial de implementación.

Validación de la veracidad de las alertas

Para garantizar la confiabilidad del esquema y evitar la generación de falsos positivos o abusos, SSC considera necesario estandarizar, previo a la distribución de una alerta, los siguientes mecanismos:

- **Definición objetiva de los criterios que constituyen una alerta válida**, tales como la existencia de múltiples quejas de usuarios, patrones de tráfico anómalos consistentes o reincidencia.

- **Aporte de evidencia técnica mínima**, suficiente para sustentar la alerta, sin incluir información sensible o contenido de las comunicaciones.

- **Clasificación del nivel de severidad de la alerta**, diferenciando alertas informativas de alertas críticas.

- **Mecanismos de revisión, actualización y corrección**, que permitan aclarar o retirar alertas cuando se identifiquen errores.

- **Asignación de responsabilidad al emisor de la alerta**, evitando reportes anónimos o sin sustento técnico.

SSC considera que una plataforma nacional de intercambio de alertas debe diseñarse bajo principios de **cooperación interoperatorial, proporcionalidad, trazabilidad y protección de datos**, de manera que permita una mitigación eficaz y oportuna del fraude en llamadas de voz, sin generar cargas desproporcionadas ni afectar la prestación de servicios legítimos.

¿Qué ventajas y desafíos observa en la creación de rangos exclusivos de numeración para llamadas comerciales y publicitarias? ¿Considera que esta medida podría ser efectiva para facilitar la identificación y denuncia de fraudes por parte de los usuarios?

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

Desde la perspectiva de SSC, la creación de **rangos exclusivos de numeración para llamadas comerciales y publicitarias** presenta **algunas ventajas potenciales** en términos de identificación del tipo de llamada por parte del usuario final, pero también **desafíos técnicos, operativos y de efectividad**, que deben ser cuidadosamente considerados antes de su adopción.

Ventajas potenciales

- **Facilitación de la identificación por parte del usuario.** El uso de rangos exclusivos podría permitir que los usuarios reconozcan de manera más sencilla que una llamada tiene fines comerciales o publicitarios, lo que podría contribuir a una toma de decisiones más informada al momento de atender la llamada.

- **Apoyo a la denuncia y gestión de reclamos.** Al existir rangos claramente identificables, los usuarios podrían **asociar con mayor facilidad una llamada sospechosa a un tipo de tráfico específico**, lo que podría facilitar la denuncia de usos indebidos y la gestión posterior por parte de los operadores.

- **Claridad regulatoria sobre el uso de la numeración.** La medida podría aportar mayor claridad respecto a los usos permitidos de ciertos rangos, facilitando la supervisión y el control regulatorio.

Desafíos y limitaciones

- **Riesgo de pérdida de efectividad por saturación o bloqueo generalizado.** En la práctica, los usuarios tienden a **bloquear de forma sistemática rangos identificados como comerciales**, lo que puede afectar comunicaciones legítimas y reducir significativamente la contactabilidad de servicios válidos.

- **Incentivo a la evasión.** La creación de rangos exclusivos puede incentivar a actores fraudulentos a **migrar hacia otros rangos de numeración** o a utilizar esquemas de suplantación, sin una reducción real del fraude.

- **Impacto operativo y de adopción.**La migración de servicios existentes hacia nuevos rangos implica **costos técnicos y operativos**, tanto para PRST como para clientes empresariales, y requiere tiempos de adaptación.

- **Limitada efectividad frente a fraude sofisticado.** La medida resulta más efectiva para clasificar el tipo de llamada que para **prevenir activamente el fraude**, dado que no resuelve el problema de fondo relacionado con la trazabilidad del originador real.

Efectividad para la identificación y denuncia de fraudes

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

SSC considera que la creación de rangos exclusivos **puede contribuir de manera parcial** a la identificación del tipo de llamada por parte del usuario, pero **no constituye una solución suficiente ni determinante** para la prevención del fraude. Su efectividad depende de que se complemente con **otros mecanismos**, tales como etiquetado informativo, monitoreo de comportamiento, cooperación interoperatorial y trazabilidad técnica.

En conclusión, SSC considera que los rangos exclusivos de numeración para llamadas comerciales y publicitarias pueden aportar **claridad y apoyo informativo al usuario**, pero presentan **limitaciones estructurales** y riesgos de evasión, por lo que su adopción debería evaluarse como **una medida complementaria**, y no sustitutiva, dentro de un enfoque integral de mitigación del fraude en llamadas de voz.

¿Qué ventajas, retos y posibles impactos identifica en la implementación de un esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual? ¿De qué manera considera que esta medida podría contribuir a la protección del usuario y a la transparencia en las comunicaciones, y qué desafíos técnicos, operativos o de experiencia de usuario deberían ser tenidos en cuenta para su adopción efectiva en Colombia?

Esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios

Desde la perspectiva de SSC, la implementación de un **esquema de etiquetado obligatorio en el identificador de llamadas para contactos comerciales y publicitarios, manteniendo la numeración actual**, presenta **ventajas relevantes** en términos de protección del usuario y transparencia, siempre que se diseñe bajo criterios técnicos claros, gobernanza adecuada y proporcionalidad.

Ventajas y posibles impactos positivos

- **Mayor transparencia para el usuario final.** El etiquetado permite que el usuario identifique de manera inmediata la naturaleza de la llamada (por ejemplo, comercial, publicitaria o empresarial), sin necesidad de modificar la numeración ni de recurrir a bloqueos automáticos. Esto mejora la comprensión del contexto de la llamada y fortalece la confianza en las comunicaciones legítimas.

- **Empoderamiento del usuario y prevención del fraude.** Al brindar información clara y visible en el identificador de llamadas, el esquema facilita que el usuario tome decisiones informadas sobre si atender o no una llamada, reduciendo la efectividad de esquemas de suplantación que se basan en generar ambigüedad o confianza indebida.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- **Preservación de la numeración y continuidad del servicio.** A diferencia de la creación de rangos exclusivos, el etiquetado permite mantener la numeración actual, evitando impactos operativos, costos de migración y afectaciones a la contactabilidad de servicios empresariales legítimos.

- **Alineación con prácticas ya adoptadas por el ecosistema digital.** El esquema es coherente con soluciones ampliamente utilizadas por los usuarios, como aplicaciones y funcionalidades de identificación de llamadas que ya incorporan etiquetas informativas y de verificación, lo que facilita su aceptación y comprensión.

Retos y desafíos a considerar

- **Definición y estandarización de las etiquetas.** Resulta necesario establecer de forma clara y homogénea las categorías de etiquetado (por ejemplo, "llamada comercial", "empresa verificada", "no verificada"), así como los criterios objetivos para su asignación, evitando interpretaciones dispares entre operadores.

- **Gobernanza y responsabilidad en la asignación de etiquetas.** Debe definirse qué actor es responsable de asignar, validar, actualizar o retirar una etiqueta, así como los mecanismos de reclamación y corrección, para prevenir errores o afectaciones reputacionales a prestadores legítimos.
- **Interoperabilidad técnica y experiencia de usuario.** La efectividad del esquema depende de su correcta implementación en distintos dispositivos, sistemas operativos y redes, garantizando una experiencia de usuario consistente y comprensible.

- **Riesgo de saturación informativa.** Un uso excesivo o indiscriminado de etiquetas negativas podría generar desconfianza generalizada o fatiga en el usuario, por lo que el esquema debe equilibrar advertencias con etiquetas positivas y neutrales.

Contribución a la protección del usuario y a la transparencia

SSC considera que el etiquetado obligatorio, cuando se aplica de manera proporcional y estandarizada, **contribuye de forma significativa a la protección del usuario y a la transparencia en las comunicaciones**, al reducir la asimetría de información y permitir una gestión de confianza más efectiva, sin recurrir a medidas restrictivas que afecten de manera desproporcionada el tráfico legítimo.

En conclusión, SSC considera que un esquema de etiquetado obligatorio para llamadas comerciales y publicitarias, manteniendo la numeración actual, constituye una **herramienta adecuada y moderna** para mejorar la transparencia y la protección del usuario, siempre que se

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

complemente con criterios claros de gobernanza, interoperabilidad técnica y mecanismos de control que eviten abusos o efectos no deseados.

¿Qué beneficios y riesgos identifica en la creación de un registro nacional único de números DNO? ¿Qué criterios deberían regir su actualización y acceso?

Desde la perspectiva de SSC, la creación de un **registro nacional único de números de no originación (DNO)** puede aportar **beneficios relevantes** para la mitigación del fraude en llamadas de voz, pero también conlleva **riesgos técnicos y operativos** que deben ser cuidadosamente gestionados mediante criterios claros de actualización, acceso y gobernanza.

Beneficios potenciales

- **Reducción de usos indebidos de numeración.** Un registro nacional de DNO puede contribuir a evitar el uso fraudulento de numeración que **no debería originar llamadas** bajo ningún escenario legítimo, como rangos no asignados, numeración reservada o números identificados de manera consistente en eventos de fraude confirmado.
- **Homogeneidad en la aplicación de controles básicos.** La existencia de un registro único permitiría aplicar un **criterio común y estandarizado** entre los PRST, reduciendo asimetrías regulatorias y técnicas en la gestión de numeración claramente irregular.
- **Apoyo a la trazabilidad y a la coordinación interoperatorial.** El DNO puede servir como **referencia compartida**, facilitando la cooperación entre operadores y la respuesta coordinada frente a eventos de fraude reincidentes.

Riesgos y desafíos

- **Riesgo de falsos positivos con impacto sistémico.** Al tratarse de un registro único y centralizado, **errores en la inclusión de un número** pueden generar bloqueos generalizados y afectar de manera desproporcionada tráfico legítimo, con impactos inmediatos en la prestación del servicio.

- **Rigidez operativa y tiempos de reacción.** Si los procesos de actualización no son ágiles, el registro puede volverse **obsoleto o inefectivo**, o impedir una reacción oportuna frente a nuevos esquemas de fraude.
- **Incentivo a la evasión.** Actores fraudulentos pueden adaptarse rápidamente, migrando a numeración distinta o a esquemas de suplantación más complejos, limitando la efectividad del DNO como única medida.

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- **Concentración de responsabilidades y riesgos.** La centralización del registro implica mayores exigencias en materia de **seguridad de la información, gobernanza y responsabilidad** ante errores o usos indebidos.

Criterios para la actualización del registro

SSC considera indispensable que la actualización del registro DNO se rija por criterios estrictos y objetivos, tales como:

- **Inclusión limitada a numeración que objetivamente no debe originar llamadas**, evitando incorporar números utilizados en servicios legítimos.
- **Sustento técnico verificable** para la inclusión de un número, basado en evidencia clara de uso indebido o fraude confirmado.
- **Mecanismos de revisión periódica y expiración automática**, que eviten inclusiones permanentes sin reevaluación.
- **Procedimientos de corrección y exclusión ágiles**, cuando se identifiquen errores o cambios en la condición del número.

Criterios de acceso y uso

En cuanto al acceso al registro, SSC considera que deben establecerse las siguientes salvaguardas:

- **Acceso restringido a PRST y actores autorizados**, exclusivamente para fines de prevención y mitigación del fraude.
-
- **Registro y auditoría de consultas y actualizaciones**, garantizando trazabilidad y responsabilidad.
- **Prohibición expresa de usos comerciales o competitivos** de la información.
- **Cumplimiento de los principios de protección de datos**, incluyendo minimización, seguridad y retención limitada.

SSC considera que un registro nacional único de DNO puede ser una **herramienta útil como medida complementaria**, siempre que su alcance sea **estrictamente acotado**, su actualización sea ágil y verificable, y su uso se enmarque en principios de proporcionalidad y protección del tráfico legítimo. En ningún caso debería entenderse como una solución única o sustitutiva de otros

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

mecanismos como el monitoreo de comportamiento, la trazabilidad técnica y la cooperación interoperatorial.

¿Qué ventajas, retos y posibles impactos identifica en la adopción de un esquema en el que cada PRST mantenga su propia lista de no originación (DNO), bajo un estándar mínimo obligatorio definido por la CRC? ¿De qué manera considera que esta medida podría contribuir a la protección contra el fraude y la suplantación en llamadas de voz, y qué desafíos técnicos, operativos o de coordinación deberían ser tenidos en cuenta para asegurar su efectividad y coherencia en Colombia?

Esquema de listas de no originación (DNO) administradas por cada PRST bajo un estándar mínimo obligatorio

Desde la perspectiva de SSC, la adopción de un esquema en el que **cada PRST administre su propia lista de no originación (DNO)**, bajo un **estándar mínimo obligatorio definido por la CRC**, presenta **ventajas relevantes** frente a un registro único centralizado, al tiempo que plantea **retos técnicos, operativos y de coordinación** que deben ser gestionados mediante lineamientos regulatorios claros.

Entre las principales **ventajas**, se destaca que la administración descentralizada de las listas DNO permite a cada PRST **actuar de manera ágil y focalizada** frente a eventos de fraude detectados en su propia red, reduciendo los tiempos de reacción y evitando la propagación automática de bloqueos a todo el ecosistema. Asimismo, este enfoque reduce el **riesgo sistémico de falsos positivos**, al limitar el impacto de eventuales errores de inclusión a la red del PRST que adopta la medida. Adicionalmente, facilita una mejor **alineación con la realidad operativa de cada red**, permitiendo integrar la DNO con otros mecanismos como el monitoreo de comportamiento, la trazabilidad técnica y la cooperación interoperatorial.

No obstante, la existencia de múltiples listas DNO también introduce **retos relevantes**. En particular, resulta necesario asegurar un **nivel mínimo de coherencia interoperatorial**, de manera que no se presenten tratamientos divergentes injustificados sobre la misma numeración. Asimismo, se requiere una adecuada gestión operativa y de gobernanza, que contemple procesos claros de inclusión, revisión, corrección y atención de reclamaciones, así como recursos técnicos suficientes para la administración continua de las listas.

Adicionalmente, SSC considera necesario advertir que este esquema puede verse afectado por **asimetrías de mercado**, especialmente en el caso de PRST con **alta participación de mercado o posición dominante**. En ausencia de salvaguardas regulatorias adecuadas, existe el riesgo de que las listas DNO sean utilizadas de forma **excesiva o desproporcionada**, generando bloqueos amplios que afecten tráfico legítimo o introduzcan distorsiones competitivas. Por ello, resulta

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

indispensable que el estándar mínimo definido por la CRC establezca **criterios objetivos y restrictivos de inclusión**, prohíba expresamente inclusiones masivas sin sustento técnico, y contemple **obligaciones de trazabilidad, justificación y auditoría**, así como **mecanismos ágiles de revisión y corrección**, con una supervisión regulatoria reforzada cuando se trate de PRST con alta participación de mercado.

En términos de **contribución a la protección contra el fraude y la suplantación**, SSC considera que las listas DNO por PRST pueden ser efectivas en la medida en que se utilicen de forma **acotada y objetiva**, enfocadas exclusivamente en numeración que **no debe originar llamadas bajo ningún escenario legítimo**, y se integren dentro de un enfoque de mitigación **multicapa**, complementario a otros mecanismos técnicos y operativos.

Para asegurar la **efectividad y coherencia** del esquema a nivel nacional, SSC considera necesario que la CRC defina, como mínimo: (i) un estándar obligatorio de criterios de inclusión y exclusión, evidencia técnica mínima y plazos de revisión; (ii) lineamientos de intercambio de alertas entre PRST sin imposición de replicación automática de listas; (iii) principios de proporcionalidad, reversibilidad y protección del tráfico legítimo; y (iv) reglas claras de protección de datos y auditoría.

SSC considera que un esquema de listas de no originación administradas por cada PRST, bajo un estándar mínimo definido por la CRC y acompañado de salvaguardas frente a asimetrías de mercado, constituye una **alternativa más flexible, proporcional y operativamente viable** que un registro nacional único, siempre que se diseñe con mecanismos efectivos de coordinación, control y supervisión.

RESUMEN EJECUTIVO

Aportes de SSC al proyecto regulatorio sobre mitigación del fraude en llamadas de voz

1. Contexto general

En el marco del proyecto regulatorio orientado a la mitigación del fraude mediante llamadas de voz, SSC presenta a la Comisión de Regulación de Comunicaciones (CRC) sus aportes técnicos y regulatorios, con base en su experiencia operativa en la gestión de tráfico nacional, internacional, LDI y comunicaciones cursadas a través de plataformas IP y en la nube.

El propósito de estos aportes es contribuir al diseño de un marco regulatorio **efectivo, proporcional y técnicamente viable**, que proteja a los usuarios finales sin generar impactos negativos sobre la competencia, la innovación ni la prestación de servicios legítimos.

2. Diagnóstico del problema

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

Desde la evidencia operativa, SSC considera que el fraude en llamadas de voz **no se origina en la numeración ni en la simple presentación del identificador de la línea llamante (CLI)**, sino en la **dificultad para identificar y rastrear el origen técnico real de las llamadas**, especialmente cuando estas atraviesan múltiples redes, plataformas y operadores.

Adicionalmente, el ecosistema de llamadas de voz presenta **asimetrías significativas en las capacidades de control** entre los distintos actores, lo que implica que **no todos cuentan con el mismo nivel de visibilidad, control ni capacidad de intervención** sobre el tráfico.

En particular:

- los PRST que controlan la red de acceso y la terminación de las llamadas cuentan con visibilidad completa del tráfico y capacidad de bloqueo inmediato;
- los operadores LDI y carriers internacionales tienen control parcial y visibilidad limitada sobre la cadena completa de origen;
- las plataformas OTT o CPaaS controlan la aplicación o el cliente empresarial, pero no la red de acceso;
- y los usuarios finales no tienen capacidad técnica de control.

Estas diferencias son determinantes y deben ser consideradas en el diseño de las medidas regulatorias.

3. Riesgos de enfoques regulatorios no diferenciados

Las medidas que tratan a todos los actores como si tuvieran **las mismas capacidades técnicas de control** pueden generar efectos no deseados, tales como:

- la asignación de responsabilidades a agentes que no cuentan con los medios técnicos para cumplirlas;
- la exigencia de pruebas técnicas a quienes no tienen acceso a los registros necesarios;
- y la concentración de decisiones de bloqueo en pocos actores con alta participación de mercado.

En este contexto, las prohibiciones generales, los bloqueos amplios o las restricciones basadas únicamente en la nacionalidad del CLI **no resultan eficaces para mitigar el fraude** y pueden afectar de manera desproporcionada la prestación de servicios legítimos.

4. Enfoque regulatorio recomendado

SSC propone que la mitigación del fraude se aborde mediante un **enfoque integral, multicapa y proporcional**, que reconozca las distintas capacidades de control y combine de forma complementaria:

- la trazabilidad y validación del origen técnico de las llamadas;

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

- el monitoreo del tráfico basado en comportamiento;
- esquemas de etiquetado informativo en el identificador de llamadas;
- la cooperación interoperatorial y el intercambio de alertas;
- y el uso acotado y estandarizado de listas de no originación (DNO).

Este enfoque permite gestionar el riesgo de manera más precisa, reducir falsos positivos y preservar la continuidad de servicios empresariales, transaccionales y de atención al cliente.

5. Principios regulatorios clave

SSC considera conveniente que el marco regulatorio incorpore expresamente los siguientes principios:

a) Asignación proporcional de responsabilidades:
Las obligaciones regulatorias deben corresponder a la capacidad real de control e intervención de cada actor sobre el tráfico de llamadas, evitando imponer cargas desproporcionadas a quienes no controlan la red de acceso ni la terminación.

b) Principio de carga probatoria:
Las medidas de bloqueo, restricción o inclusión en listas de no originación deben estar sustentadas en evidencia técnica objetiva y verificable, aportada por el PRST que tenga control efectivo sobre la red y los registros técnicos del tráfico.

c) Salvaguardas frente a asimetrías de mercado:
Las medidas antifraude deben incorporar mecanismos de motivación técnica, trazabilidad, auditoría y revisión, especialmente cuando sean aplicadas por PRST con alta participación de mercado, a fin de prevenir efectos desproporcionados o distorsiones competitivas.

6. Protección del usuario y transparencia

SSC considera que los esquemas de **etiquetado informativo en el identificador de llamadas**, manteniendo la numeración vigente, constituyen una herramienta eficaz para fortalecer la protección del usuario y la transparencia en las comunicaciones, al permitir decisiones informadas sin recurrir a bloqueos generalizados.

Estos esquemas deben basarse en criterios técnicos claros, niveles diferenciados de verificación del origen y mecanismos de corrección, interoperabilidad y gobernanza definidos.

7. Conclusión

SSC considera que la adopción de un marco regulatorio que reconozca las diferencias reales de control entre los actores, se base en trazabilidad, evidencia técnica y cooperación interoperatorial,

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001

permitirá a la CRC avanzar de manera efectiva en la mitigación del fraude en llamadas de voz, **protegiendo al usuario final sin afectar de forma desproporcionada la competencia ni los modelos legítimos de prestación de servicios**.

Este enfoque se encuentra alineado con los principios de neutralidad tecnológica, eficiencia regulatoria, promoción de la competencia y sostenibilidad del sector que orientan la actuación de la CRC.

Cordialmente,

CARLOS ANDRÉS VARGAS
Representante Legal
Sistemas Satelitales de Colombia SA ESP

Kr 7 # 155C - 20 Oficina 4105, Bogotá, Colombia
601 7944444 - 601 7940001