

Bogotá D.C., 23 de junio de 2026

Señores

COMISIÓN DE REGULACIÓN DE COMUNICACIONES - CRC

Ciudad

Asunto:

Comentarios al Proyecto de Resolución “*Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones*”, en lo relativo a las medidas sobre servicios tradicionales de voz. Solicitud de exclusión expresa de las gestiones de cobranza y de adopción de un esquema de verificación de origen para tráfico de voz legítimo

Respetados señores:

En nombre de **BYTECOL TECHNOLOGY SYSTEMS SAS**, en nuestra calidad de proveedor de soluciones de telefonía IP, comunicaciones empresariales y servicios asociados al ecosistema de voz, presentamos dentro del término establecido nuestros comentarios al proyecto de resolución de la referencia.

BYTECOL comparte plenamente el propósito de la CRC de mitigar el fraude cibernético, proteger a los usuarios y reducir las modalidades de suplantación telefónica. Sin embargo, consideramos que algunas de las medidas propuestas, en especial el bloqueo de llamadas internacionales entrantes que presenten como CLI un número colombiano, pueden generar afectaciones graves y desproporcionadas sobre comunicaciones legítimas, particularmente aquellas realizadas mediante telefonía IP, centros de contacto, plataformas empresariales en la nube y operaciones de cobranza del sector financiero y real.

El objetivo regulatorio no debe ser impedir el contacto legítimo con los usuarios, sino distinguir de manera técnica, verificable y proporcional entre comunicaciones fraudulentas y comunicaciones empresariales lícitas. Esa distinción es indispensable para evitar que una medida antifraude termine bloqueando canales formales de atención, seguridad, autenticación, cobranza y servicio al cliente.

I. Consideración preliminar: la cobranza no debe ser tratada como venta, publicidad ni fraude

El proyecto parte de una preocupación legítima: los usuarios reciben llamadas no deseadas, llamadas comerciales abusivas y llamadas fraudulentas. No obstante, dentro del universo de llamadas empresariales deben distinguirse, como mínimo, tres categorías diferentes:

1. **Llamadas fraudulentas**, en las que un tercero suplanta la identidad de una entidad, manipula el CLI o utiliza infraestructura de comunicaciones para engañar al usuario.
2. **Llamadas comerciales o publicitarias**, orientadas a promocionar bienes, servicios, ofertas, campañas comerciales o actividades de mercadeo.
3. **Gestiones de cobranza, recuperación de cartera, atención contractual, autenticación, seguridad, prevención de fraude y comunicaciones transaccionales o de servicio**, que responden a una relación jurídica, contractual, financiera o comercial preexistente.

Estas categorías no pueden recibir el mismo tratamiento regulatorio. La gestión de cobranza no es, por naturaleza, una llamada publicitaria ni una llamada fraudulenta. Se trata de una actividad lícita, necesaria y regulada, que permite informar al deudor sobre el estado de sus obligaciones, evitar deterioros mayores en la cartera, ofrecer alternativas de normalización y mantener canales formales de comunicación entre acreedores, entidades financieras, casas de cobranza, comercios, usuarios y consumidores.

La Ley 2300 de 2023 ya establece reglas sobre canales, horarios y periodicidad aplicables a las entidades vigiladas por la Superintendencia Financiera y a quienes adelantan gestiones de cobranza directa, por terceros o por cesión de la obligación. Por tanto, la respuesta regulatoria no debe consistir en equiparar la cobranza con publicidad o fraude, sino en preservar su tratamiento diferencial, sin perjuicio del cumplimiento de las obligaciones legales de protección al consumidor, habeas data, información y trato digno.

En consecuencia, solicitamos que la resolución incluya una exclusión expresa conforme a la cual las gestiones de cobranza, recuperación de cartera, atención contractual, autenticación, seguridad, prevención de fraude y comunicaciones transaccionales o de servicio no sean consideradas “llamadas con fines publicitarios” ni sean objeto de bloqueo o etiquetado por esa sola condición.

II. El bloqueo general de CLI colombiano en tráfico internacional afecta comunicaciones legítimas cursadas por telefonía IP

El proyecto propone que los PRST bloqueen las llamadas internacionales entrantes que presenten como identificador de línea llamante un número perteneciente al Plan Nacional de Numeración colombiano, salvo cuando se trate de roaming internacional debidamente identificado.

Esa regla parte de una premisa comprensible, pero incompleta: que una llamada con CLI colombiano que ingresa por una ruta internacional es sospechosa. En el ecosistema actual de comunicaciones empresariales, esa premisa no siempre es cierta.

Hoy múltiples empresas, entidades financieras, compañías de cobranza, aseguradoras, comercios, prestadores de salud, aerolíneas, BPO, contact centers y proveedores de servicios corporativos utilizan soluciones de telefonía IP, SIP Trunks, plataformas en la nube, herramientas CPaaS/UCaaS y centros de contacto distribuidos. En estos casos, puede ocurrir que la llamada sea cursada técnicamente desde infraestructura internacional o mediante

nodos externos, aunque el número presentado sea un número colombiano legítimo, asignado o autorizado por su titular.

El problema no es la existencia de tráfico de voz con CLI colombiano cursado mediante infraestructura IP o rutas internacionales. El problema es la falta de trazabilidad, autenticación y verificación del origen. Por ello, una medida que bloquee en bloque toda llamada con esa apariencia termina castigando por igual al defraudador y al actor legítimo que sí puede acreditar su identidad, su cliente, su numeración y la finalidad lícita de la comunicación.

Para **BYTECOL**, como proveedor de telefonía IP, esta diferencia es esencial. Nuestros clientes pueden requerir que sus comunicaciones salientes presenten numeración legítima, reconocible y estable para el usuario final. En sectores como el financiero y cobranzas, esa identificación no solo es conveniente, sino necesaria: el usuario debe poder reconocer quién lo llama, devolver la llamada, identificar al acreedor, validar el origen del contacto y ejercer sus derechos.

Bloquear de manera indiscriminada la presentación de CLI colombiano en llamadas cursadas por infraestructura internacional o IP puede producir el efecto contrario al buscado: reducir la confianza del usuario, impedir comunicaciones legítimas y empujar el tráfico hacia canales menos regulados o menos trazables.

III. La medida debe superar un análisis de proporcionalidad

El bloqueo general es la medida más intensa posible. No advierte, no clasifica, no verifica, no permite corregir, no distingue. Simplemente impide la comunicación.

Una medida de esa naturaleza debe ser idónea, necesaria y proporcional en sentido estricto. Consideramos que, en los términos propuestos, no satisface ese estándar.

1. La medida no es plenamente idónea

El fraude telefónico no depende exclusivamente de que el defraudador utilice un CLI colombiano. Un actor malicioso puede modificar su patrón de operación, usar numeración extranjera, recurrir a canales OTT, manipular otros identificadores o trasladar la ingeniería social a aplicaciones de mensajería y llamadas por internet.

Por tanto, bloquear llamadas con CLI colombiano provenientes de rutas internacionales ataca una manifestación visible del problema, pero no necesariamente su causa: la ausencia de verificación confiable del originador.

2. La medida no es necesaria

El propio proyecto contempla alternativas menos lesivas, como monitoreo, identificación de patrones, etiquetado de llamadas sospechosas y etiquetado de llamadas publicitarias. Si la CRC ya prevé mecanismos de advertencia y clasificación para otros supuestos de riesgo en voz, no resulta justificado acudir directamente al bloqueo absoluto para el tráfico internacional con CLI colombiano, sin permitir antes una verificación del origen.

La alternativa menos lesiva consiste en exigir a los proveedores de voz, operadores, clientes corporativos y titulares de numeración mecanismos documentales y técnicos para acreditar la legitimidad del CLI presentado.

3. La medida no es proporcional en sentido estricto

El daño potencial del bloqueo es alto: puede impedir llamadas de cobranza, recordatorios de pago, autenticaciones, prevención de fraude financiero, atención de clientes, confirmaciones transaccionales, avisos contractuales, seguimiento de obligaciones y comunicaciones de servicio.

El beneficio, en cambio, es parcial y evadible. El usuario puede quedar incomunicado frente a entidades legítimas, mientras el defraudador migra a otro canal. Así, el bloqueo puede causar más perjuicio que protección.

IV. La gestión de cobranza requiere una exclusión expresa y operativa

Solicitamos que la CRC incorpore una regla expresa que diferencie la gestión de cobranza de las llamadas publicitarias.

La cobranza no busca vender un producto nuevo ni promover una campaña comercial. Su finalidad principal es informar, gestionar o normalizar una obligación existente. También permite prevenir litigios, evitar reportes negativos innecesarios, ofrecer mecanismos de pago y mantener trazabilidad formal de la relación entre acreedor y deudor.

Si una llamada de cobranza es bloqueada o etiquetada como sospechosa por el solo hecho de usar infraestructura de telefonía IP o presentar CLI colombiano en una ruta internacional, se generan varios efectos negativos:

Se afecta al usuario, quien puede dejar de recibir información relevante sobre su obligación.

Se afecta al acreedor, que pierde un canal lícito para gestionar cartera.

Se afecta al proveedor de telefonía IP, que ve restringida una actividad legítima sin que exista prueba de fraude.

Se afecta el sistema financiero y de crédito, porque se encarecen las gestiones formales y se incentiva el uso de canales alternativos menos trazables.

Se afecta la confianza del usuario, porque una comunicación legítima puede aparecer como sospechosa o no llegar nunca.

Por ello, la exclusión no debe ser meramente declarativa. Debe traducirse en una regla operativa aplicable al bloqueo, al etiquetado y al uso de listas asociadas al RNE.

Proponemos que la CRC precise que no se entienden como llamadas publicitarias, para efectos del proyecto, las siguientes:

- a. Gestiones de cobranza, recuperación de cartera, normalización de obligaciones o contacto relacionado con obligaciones vencidas o vigentes.
- b. Comunicaciones transaccionales o de servicio.

- c. Llamadas de autenticación, prevención de fraude, validación de identidad o seguridad.
- d. Comunicaciones necesarias para la ejecución de una relación contractual vigentes.
- e. Comunicaciones exigidas o permitidas por normas sectoriales, financieras, de protección al consumidor o de habeas data.

Lo anterior debe entenderse sin perjuicio de que, cuando una llamada incluya además una finalidad comercial o publicitaria autónoma, esa finalidad sí quede sometida a las reglas aplicables a llamadas comerciales.

V. La solución adecuada es un esquema de origen verificado

BYTECOL solicita que, en lugar de un bloqueo general, la CRC adopte un esquema de verificación de origen para tráfico de voz legítimo.

Este esquema debería permitir que los proveedores de telefonía IP, operadores, centros de contacto, plataformas empresariales y clientes corporativos acrediten, antes del bloqueo, la legitimidad de las llamadas que cursan con CLI colombiano.

El mecanismo podría estructurarse con los siguientes elementos:

1. Registro de origen verificado

Crear un registro o mecanismo de inscripción ante la CRC, o ante los PRST bajo lineamientos uniformes definidos por la CRC, para tráfico empresarial de voz con CLI nacional.

En dicho registro deberían poder inscribirse proveedores de telefonía IP, operadores, contact centers, entidades financieras, casas de cobranza, empresas usuarias de numeración y demás originadores legítimos.

2. Verificación documental del cliente

El proveedor que curse la llamada debería conservar evidencia de:

- Identidad del cliente u originador.
- Relación contractual con el cliente.
- Finalidad general de la comunicación: cobranza, atención, autenticación, servicio, seguridad, transaccional, comercial u otra.
- Canales de contacto para requerimientos de autoridad u operador.

3. Trazabilidad mínima

Los proveedores deberían conservar registros técnicos razonables que permitan reconstruir, ante una solicitud de autoridad competente, el cliente originador, el número presentado, la fecha, hora, destino, ruta y demás datos técnicos disponibles.

4. Etiquetado diferenciado, no bloqueo

Cuando el origen sea verificable, la llamada no debería ser bloqueada. En caso de que la CRC considere necesaria alguna indicación al usuario, debería utilizarse un etiquetado neutro o informativo, no una etiqueta de sospecha.

La etiqueta no debería aplicarse a comunicaciones verificadas o de cobranza por su sola naturaleza.

5. Puerto seguro de responsabilidad

Debe incorporarse un puerto seguro para el proveedor que cumpla con el estándar definido por la CRC. Si el proveedor verifica la identidad del cliente, mantiene trazabilidad y actúa diligentemente, no debería responder por alteraciones o manipulaciones ocurridas en eslabones anteriores o ajenos a su control, salvo que se pruebe su conocimiento, participación o negligencia.

VI. La resolución debe crear un procedimiento de revisión aplicable también al bloqueo

El proyecto contempla mecanismos de etiquetado, pero el bloqueo tiene un efecto más grave: elimina la comunicación. Por tanto, cualquier régimen de bloqueo debe incluir un procedimiento de revisión ágil, técnico y trazable.

Solicitamos que el procedimiento pueda ser activado no solo por el titular de la línea, sino también por:

- El proveedor de telefonía IP afectado.
- El cliente corporativo originador.
- La entidad financiera o empresa de cobranza.
- El operador que curse el tráfico.
- El usuario destinatario que esperaba o necesitaba recibir la llamada.
- El procedimiento debería contemplar tiempos breves de respuesta, levantamiento provisional cuando exista evidencia inicial de legitimidad, trazabilidad de la decisión y la finalidad lícita de la comunicación.

Sin un mecanismo de revisión, el bloqueo se convierte en una sanción técnica sin debido proceso con efectos reales sobre negocios, usuarios y crédito.

VII. El Análisis de Impacto Normativo debe completarse frente al impacto en telefonía IP y cobranzas

Solicitamos que la CRC complemente el Análisis de Impacto Normativo para medir específicamente el impacto de las medidas de voz sobre:

- Proveedores de telefonía IP.
- Centros de contacto.
- Sector de cobranzas.
- Entidades financieras y vigiladas por la Superintendencia Financiera.
- Empresas que cursan llamadas transaccionales, de autenticación, seguridad o servicio.

- Tráfico legítimo con CLI colombiano cursado mediante infraestructura internacional, IP, cloud o plataformas empresariales.

El análisis no debería limitarse a estimar beneficios derivados de la reducción del fraude. También debe medir los costos de falsos positivos, es decir, llamadas lícitas que serían bloqueadas, etiquetadas indebidamente o desplazadas hacia canales alternativos.

En particular, el AIN debería cuantificar:

- Volumen de llamadas empresariales legítimas que presentan CLI colombiano.
- Proporción de ese tráfico asociada a cobranza, atención al cliente, autenticación, seguridad y comunicaciones transaccionales.
- Impacto económico sobre proveedores de voz IP.
- Impacto sobre la gestión de cartera y recuperación de obligaciones.
- Impacto sobre usuarios que dejan de recibir comunicaciones necesarias.
- Riesgo de migración hacia plataformas OTT no reguladas.
- Costos de implementación para proveedores no móviles y actores que no controlan la red de destino.

Sin esta medición, la CRC corre el riesgo de adoptar una medida que parece eficiente en abstracto, pero que en la práctica bloquea comunicaciones legítimas y traslada tráfico formal a canales menos regulados.

VIII. La obligación no debe imponerse de forma indiferenciada a todos los actores

La propuesta debe reconocer que no todos los actores de la cadena tienen la misma información ni la misma capacidad técnica.

Un proveedor de telefonía IP puede verificar a su cliente, conservar autorizaciones, monitorear tráfico y aportar trazabilidad. Pero no necesariamente conoce en tiempo real el estado de roaming del usuario, ni tiene acceso a la totalidad de información de red del operador móvil, ni controla todos los eslabones internacionales de señalización, por tanto, la resolución debe distribuir obligaciones según la capacidad real de cada actor.

IX. La medida puede distorsionar la competencia y favorecer canales no regulados

Si se bloquean o dificultan llamadas legítimas cursadas por voz tradicional o telefonía IP, el tráfico empresarial no desaparece. Las empresas seguirán necesitando contactar a sus usuarios, clientes y deudores. Lo que ocurrirá es una migración hacia canales alternativos, incluyendo aplicaciones OTT y plataformas no sometidas al mismo régimen sectorial.

Esto genera un riesgo de distorsión competitiva. Los proveedores regulados o formalizados soportan cargas de identificación, trazabilidad, cumplimiento, costos de red y obligaciones frente a autoridades. En cambio, otros canales pueden operar con menor supervisión, menor trazabilidad y menor responsabilidad sectorial.

La CRC debe evitar que una medida antifraude termine debilitando al ecosistema formal de voz y fortaleciendo canales que no necesariamente ofrecen mayores garantías al usuario y generan a su vez un retroceso tecnológico.

Por esa razón, solicitamos que el análisis de abogacía de la competencia evalúe expresamente el impacto de la medida sobre proveedores de telefonía IP, contact centers, empresas de cobranza y demás actores formales del mercado de voz empresarial.

X. Propuesta de ajustes normativos

Respetuosamente proponemos que la CRC incorpore ajustes en los siguientes términos:

1. Excepción al bloqueo por origen verificado

Adicionar al artículo correspondiente una excepción al bloqueo, así:

“No procederá el bloqueo cuando se trate de tráfico empresarial de voz con origen verificado, cursado por proveedores de redes y servicios de telecomunicaciones, proveedores de telefonía IP, centros de contacto, plataformas empresariales o agentes debidamente identificados, siempre que exista acreditación documental de la identidad del originador y trazabilidad mínima de la comunicación, conforme al estándar que defina la CRC.”

2. Exclusión de cobranza y comunicaciones de servicio

Adicionar una regla de interpretación, así:

“Para efectos de las obligaciones de etiquetado de llamadas con fines publicitarios y de las medidas asociadas al Registro de Números Excluidos, no se entenderán como llamadas publicitarias las gestiones de cobranza, recuperación de cartera, normalización de obligaciones, atención contractual, comunicaciones transaccionales, autenticación, prevención de fraude, seguridad, servicio al cliente o comunicaciones necesarias para la ejecución de una relación jurídica, contractual o legal preexistente, siempre que no tengan por objeto principal la promoción comercial de bienes o servicios.”

3. Etiquetado diferenciado

Modificar el régimen de etiquetado para que las llamadas verificadas no sean marcadas como sospechosas por su sola ruta técnica:

“El tráfico de voz con origen verificado no será etiquetado como ‘Alerta de llamada sospechosa’ por el solo hecho de presentar CLI nacional o por cursarse mediante infraestructura IP, cloud o internacional. Cuando proceda un etiquetado informativo, este deberá ser neutro, proporcional y coherente con la finalidad declarada de la comunicación.”

4. Procedimiento de revisión

Adicionar:

“Los proveedores de telefonía IP, operadores que cursen tráfico, clientes corporativos, titulares de numeración, originadores de llamadas y usuarios destinatarios podrán solicitar la revisión de bloqueos o etiquetados aplicados a tráfico legítimo. El procedimiento deberá permitir aportar evidencia de identidad, finalidad de la comunicación y trazabilidad técnica, y deberá resolverse en un término breve definido por la CRC.”

5. Puerto seguro

Adicionar:

“El proveedor que cumpla con los requisitos de verificación de origen, conocimiento del cliente y conservación de trazabilidad definidos por la CRC no será responsable por alteraciones del CLI o de la señalización producidas por terceros en eslabones anteriores o ajenos a su control, salvo prueba de conocimiento, participación o negligencia.”

6. Implementación gradual

Adicionar un periodo de transición:

“Las obligaciones relacionadas con verificación de origen, registros de clientes corporativos, mecanismos de etiquetado y reglas de bloqueo solo serán exigibles una vez la CRC haya definido el estándar técnico y operativo correspondiente, y luego de un periodo de implementación gradual que permita pruebas, ajustes y mecanismos de corrección de falsos positivos.”

XI. Peticiones

Con fundamento en lo anterior, solicitamos respetuosamente a la CRC:

1. No adoptar el bloqueo general e indiscriminado de llamadas internacionales entrantes que presenten CLI colombiano, salvo que previamente se habilite una excepción de origen verificado.
2. Incorporar una exclusión expresa para gestiones de cobranza, recuperación de cartera, normalización de obligaciones, comunicaciones transaccionales, atención contractual, autenticación, seguridad y prevención de fraude, de manera que no sean tratadas como llamadas publicitarias ni fraudulentas por su sola naturaleza.
3. Reconocer que la telefonía IP, los centros de contacto y las plataformas empresariales pueden cursar comunicaciones legítimas con CLI colombiano, aun cuando intervenga infraestructura internacional o en la nube.
4. Adoptar un esquema de verificación de origen basado en identificación del cliente, trazabilidad mínima y finalidad declarada de la comunicación.
5. Sustituir el bloqueo por mecanismos de etiquetado proporcional y diferenciado cuando exista tráfico verificable.
6. Crear un procedimiento de revisión aplicable a bloqueos y etiquetados, que pueda ser activado por proveedores de telefonía IP, clientes corporativos, entidades de cobranza, titulares de numeración, operadores y usuarios destinatarios.
7. Incorporar un puerto seguro de responsabilidad para los proveedores que cumplan diligentemente con el estándar de verificación definido por la CRC.



8. Completar el Análisis de Impacto Normativo frente al impacto de la medida sobre telefonía IP, centros de contacto, sector financiero, sector de cobranzas y tráfico empresarial legítimo.
9. Evaluar expresamente, en sede de abogacía de la competencia, el riesgo de desplazamiento de tráfico formal de voz hacia plataformas OTT o canales no sometidos al mismo grado de regulación.
10. Establecer un periodo de implementación gradual y suficiente, condicionado a la definición previa de los estándares técnicos, operativos y documentales aplicables.

Bytecol reitera su disposición para contribuir en la construcción de una solución efectiva contra el fraude, siempre que dicha solución preserve las comunicaciones legítimas, proteja a los usuarios y no afecte de manera desproporcionada a los proveedores formales de telefonía IP ni a sectores que, como el financiero y el de cobranzas, requieren canales confiables de comunicación de voz.

Cordialmente,

ESGUERRA REZK,
JUAN PABLO
(FIRMA)

Firmado digitalmente por
ESGUERRA REZK, JUAN
PABLO (FIRMA)
Fecha: 2026.06.23 18:06:20
-05'00'

JUAN PABLO ESGUERRA REZK
Representante Legal
BYTECOL TECHNOLOGY SYSTEMS SAS
900.771.083-3