Bogotá, 23 de Junio de 2026

Señores
COMISIÓN DE REGULACIÓN DE COMUNICACIONES
L.C.

Referencia: Experiencia en el Mercado Brasilero para Identificación de medidas para mitigar el fraude cibernético por medio de servicios móviles

De nuestra mayor consideración:

Tenemos el agrado de dirigirnos a ustedes, con el propósito de saludarlos cordialmente y, a la vez, presentar nuestros comentarios al proyecto de acuerdo a nuestra experiencia en el mercado brasilero.

Nuestra contribución técnica se basa en las lecciones aprendidas en Brasil por Cleartech S.A. y en las mejores prácticas internacionales para lucha contra las llamadas y mensajes telefónicos con fines ilícitos (fraude, robocalls abusivos, spam).

A continuación, las recomendaciones se organizan en ejes temáticos, con propuestas concretas y fundamentadas.

Eje 1: Autenticación de llamadas y mitigación de la suplantación de identidad (plataforma STIR/SHAKEN)

- **Adopción de una plataforma centralizada STIR/SHAKEN**: Se recomienda implementar una plataforma centralizada de autenticación e identificación de llamadas basada en el protocolo STIR/SHAKEN. STIR (Secure Telephone Identity Revisited), que consiste en la autenticación digital de la llamada en el origen (el operador de origen inserta una firma criptográfica que certifica que el número presentado es legítimo). SHAKEN (Signature-based Handling of Asserted information using toKENs), basado en firmas, permite verificar esta firma en el operador de destino. De este modo, cada llamada entrante puede ser verificada en tiempo real en cuanto a su origen, garantizando que el número mostrado es de hecho el número real del emisor autorizado. Este mecanismo está diseñado para luchar contra la suplantación de identidad y garantizar que la información del identificador de llamada se transmita de forma segura y fiable a través de las redes.

- **Cómo funciona y ventajas:** Con la autenticación STIR en el origen y la verificación SHAKEN en el destino, las llamadas se presentan ahora a los consumidores con el número de la persona que llama y también con la identificación verificada del emisor, incluido el nombre de la empresa, el logotipo, el motivo de la llamada, así como un sello de fiabilidad. Por ejemplo, en los smartphones compatibles, el nombre de la empresa legítima que llama, su logotipo e incluso el motivo de la llamada (como reservar una cita, ofrecer un servicio, etc.) aparecerán en la pantalla, señalando que la llamada es auténtica y no una estafa. Esto aporta transparencia y restablece la confianza en las llamadas telefónicas: el usuario puede reconocer inmediatamente a la persona que llama legítima y decidir si contesta o no con mayor confianza. Entre los beneficios esperados están: una drástica reducción en la suplantación de identidad (números suplantados), el

bloqueo de las llamadas ilegítimas antes de que molesten al usuario, la protección contra las estafas de voz (vishing) y una mayor efectividad en el rastreo del origen de las llamadas.

En EEUU, las investigaciones han demostrado que antes de STIR/SHAKEN alrededor del 70% de los usuarios no contestaba a las llamadas de números desconocidos, pero el 80% estaría dispuesto a contestar si la llamada mostraba una identificación fiable de la persona que llama, lo que demuestra el potencial de la tecnología para restaurar la confianza en la telefonía. Países como EEUU, Canadá y Brasil ya han adoptado STIR/SHAKEN a escala nacional en los últimos años, haciendo obligatoria la autenticación de las llamadas IP, lo que ha generado resultados significativos en la reducción de las llamadas fraudulentas y llamadas automáticas (las robocalls ilegales) y ha posicionado a estos países a la vanguardia de la lucha contra el fraude telefónico.

- **Consulta de la base de datos nacional de numeración:** Como complemento a STIR/SHAKEN, se recomienda implementar una validación activa con respecto a la base de datos nacional de numeración. En otras palabras, los operadores deberían comprobar automáticamente que el número de teléfono que origina la llamada corresponde realmente a un número asignado y autorizado (verificándolo contra una base de datos central de asignación de números telefónicos). Esta verificación, integrada en la plataforma de autenticación, mitiga la suplantación de identidad al impedir que los estafadores utilicen números no asignados o números que no les pertenecen. En Brasil, el sistema "Origen Verificado" realiza esta verificación de origen en tiempo real, lo que dificulta el uso de números falsos (por ejemplo, estafadores que enmascaran llamadas utilizando prefijos 0800 o números de otras empresas). Garantizar la integridad del número que llama reduce significativamente el riesgo de estafas que se basan en identidades telefónicas falsas. Recomendación: Colombia debe mantener una base de numeración nacional actualizada y exigir que, durante la señalización de la llamada, esta base sea consultada para validar el origen, ya sea mediante el protocolo STIR/SHAKEN u otros mecanismos- bloqueando las llamadas cuyo número de origen no coincida con el abonado/operador legítimo. Esto aumentará la fiabilidad de la identificación de llamadas para usuarios y autoridades.

Eje 2: Modelo centralizado y experiencia brasileña

- **Operando por más de un año en Brasil:** En el caso brasileño, se optó por un modelo centralizado, coordinado por la Entidad Administradora de Autenticación e Identificación (ABR Telecom), implantado, gestionado y operado por Cleartech, que se encarga de intermediar la autenticación de las llamadas entre todos los operadores. Este modelo entró en operación inicial en enero de 2024 y, más de un año después, está maduro, autenticando e identificando más de 4 billones de llamadas al mes a través de las redes brasileñas (un número en rápido crecimiento) con un bajo coste de implementación para el sector. Todos los grandes operadores (móviles y fijos) se han adherido, así como varios operadores más pequeños y docenas de empresas que utilizan el servicio de call center. En agosto de 2024, 33 operadores (móviles y fijos) se habían adherido al programa "Origen Verificado" (STIR/SHAKEN), y 42 empresas de diversos sectores contrataron el servicio para sus call center tan pronto como se lanzó comercialmente.

- **Resultados concretos en Brasil:** La experiencia brasileña en la lucha contra las llamadas ilícitas ya ha demostrado impactos positivos mensurables. Entre junio de 2022 y diciembre de 2024, se estima que las medidas regulatorias adoptadas evitaron que se realizaran 184 900 millones de llamadas no deseadas (cortas o robocalls) en las redes, es decir, se bloquearon casi 185 000 millones de intentos de llamadas abusivas antes de molestar a los usuarios. Este impresionante volumen equivale, en promedio, a más de 800 llamadas no deseadas evitadas por habitante durante el período. Hubo una reducción de ~41% en el volumen de llamadas cortas (de pocos segundos, típicas de las robocalls que cuelgan en cuanto el usuario contesta) al comparar mayo/2022 (antes de las medidas) con julio/2023 - una caída significativa de esta práctica abusiva en poco más de un año. ANATEL (el regulador brasileño) supervisó la proporción de llamadas muy cortas como un indicador de marcación automática masiva, y el endurecimiento de las normas llevó a la suspensión de cientos de llamantes infractores. A mediados de 2023, se habían bloqueado 582 empresas por superar los límites definidos en las medidas cautelares; en total, a finales de 2024 este número de infractores bloqueados superaba los 1.000 (usuarios de servicios de telemarketing abusivos). Muchos de estos infractores han intentado regularizar su conducta: 223 empresas presentaron propuestas de Términos de Compromiso a ANATEL, de las cuales 170 ya fueron aceptadas, comprometiéndose formalmente a seguir las normas bajo pena de sanciones más graves. También se implementó en Brasil un código de identificación específico (0303) para el telemarketing (detallado en el Eje 3), al que ya se han adherido voluntaria u obligatoriamente 2.778 números comerciales, lo que facilita al público reconocer este tipo de llamadas. Estos resultados demuestran que un enfoque que combina tecnología (autenticación de llamadas), normas claras y cumplimiento activo puede mitigar drásticamente el abuso de las llamadas ilícitas, sirviendo de referencia para Colombia.

- **Amplia adopción en el mercado:** Es importante destacar que, en Brasil, la efectividad de las medidas se debe en parte al amplio apoyo del ecosistema: los principales operadores se integraron inmediatamente en la plataforma centralizada, y grandes usuarios de centros de llamadas (como bancos y aseguradoras) apoyaron la iniciativa desde el principio, participando incluso en las pruebas piloto. Esta cooperación sectorial voluntaria aceleró la implementación en lugar de esperar a largos procedimientos regulatorios. Colombia podría inspirarse en este modelo de coordinación sectorial: un acuerdo entre operadores, autoridades y las principales empresas originadoras de llamadas, con una entidad neutral operando la plataforma de autenticación, tiende a generar resultados más rápidos y consistentes en la lucha contra el fraude, a un menor costo individual. Se recomienda evaluar asociaciones con organizaciones técnicas capaces de proporcionar la solución central (en el caso brasileño, Cleartech fue el proveedor tecnológico). En resumen, la experiencia brasileña demuestra que la combinación de tecnología de autenticación + normas claras + colaboración multisectorial da lugar a una reducción significativa de las llamadas ilícitas, sin gravar excesivamente a las empresas legítimas o al regulador.

Eje 3: Identificación clara de las llamadas masivas (Prefijo 0303)

- **Prefijo nacional para telemarketing y llamadas automatizadas:** La adopción de un prefijo telefónico para identificar las llamadas masivas (telemarketing,

cobranzas automatizadas, encuestas, etc.) es una medida regulatoria simple y efectiva para brindar transparencia al usuario. En 2022, Brasil implementó el código nacional 0303, obligatorio para todas las operaciones activas de telemarketing (oferta de productos o servicios por teléfono). De esta manera, cualquier llamada iniciada por 0303 en el identificador de llamadas señala al usuario que se trata de una llamada comercial/marketing, permitiéndole decidir no contestar si no desea recibir ofertas. Esta medida frena la práctica de las empresas de llamar desde números aleatorios o enmascarados para "engañar" a los consumidores y hacerles contestar, una queja común antes de la regulación normativa. En poco tiempo, miles de líneas empezaron a llevar correctamente el prefijo: en julio de 2023, 2.778 números comerciales en Brasil ya utilizaban el código 0303, lo que indica una amplia adopción por parte del sector de los centros de llamadas.

- **Expansión del uso del prefijo a otras categorías:** Inicialmente, el código 0303 brasileño sólo se aplicaba a las ofertas de televenta y telemarketing. Sin embargo, los estafadores y otras operaciones abusivas pueden disfrazarse como si no fueran "televentas" para evadir la norma. Por eso, en Brasil se decidió expandir el uso obligatorio del prefijo: ANATEL determinó que, a partir de enero de 2025, todas las empresas o instituciones que realicen más de 10.000 llamadas telefónicas al día (independientemente del motivo -incluidas recaudaciones, solicitudes de donaciones, encuestas automatizadas, etc.-) deberán utilizar el código 0303 en sus llamadas. En otras palabras, el prefijo identificativo se ha convertido en sinónimo de llamadas masivas, no sólo de telemarketing de ventas. Las organizaciones que se ajusten a este criterio podrán realizar un máximo del 10% de sus llamadas diarias utilizando su número ordinario (sin prefijo) - al menos el 90% de sus llamadas deben salir con el prefijo designado. Esta medida garantiza que prácticamente cualquier operación de llamadas a gran escala esté claramente identificada, lo que dificulta la tarea de los estafadores (que solían alternar cientos de números aleatorios para eludir los bloqueos). Se recomienda que Perú establezca un prefijo nacional específico (similar al 0303) para identificar las llamadas a gran escala. Este prefijo debe ser corto y fácilmente reconocible por el público, y su uso debería ser obligatorio para los centros de llamadas, empresas de telemarketing, empresas de cobranza de deudas o cualquier entidad que realice volúmenes significativos de llamadas automatizadas. La implementación puede ser gradual (empezando con las televentas, por ejemplo, y luego expandiéndose después), pero es crucial cubrir todos los fines de las llamadas masivas ilícitas para evitar lagunas legales.

- **Ventajas para los consumidores y el cumplimiento:** Con un código de identificación estandarizado, los consumidores colombianos podrán identificar inmediatamente la naturaleza de la llamada antes de contestarla, lo que aumentará su protección contra el fraude y las molestias. Además, facilita el cumplimiento de la normativa: si una llamada masiva no muestra el prefijo obligatorio, estará en clara violación de la norma, lo que permite sancionar directamente a la empresa u operador responsable. En Brasil, el prefijo 0303, combinado con sistemas de denuncia (como el sitio web Não Me Perturbe y el portal Qual Empresa Me Ligou?), ha empoderado a los consumidores para bloquear proactivamente las llamadas no deseadas y denunciar a los reincidentes, complementando las acciones de bloqueo automático de las robocalls. Se espera

un efecto similar en Colombia, especialmente si se realizan campañas publicitarias que enseñen al público a reconocer el prefijo y sus implicaciones (véase el Eje 7).

Eje 4: Criterios objetivos para la detección y el bloqueo de llamadas automáticas

- **Parámetros técnicos de abuso:** Es fundamental definir criterios objetivos que caractericen el uso abusivo de llamadas automáticas (llamadas masivas automatizadas) para activar el bloqueo y sanciones de forma transparente. La experiencia internacional y brasileña sugiere un parámetro eficaz: controlar el número de llamadas realizadas por un determinado originador y su duración media de estas llamadas. Por ejemplo, ANATEL ha establecido que el telemarketing abusivo se produce cuando un único número realiza 100.000 o más llamadas al día utilizando marcadores automáticos. En estos casos, las llamadas suelen ser extremadamente cortas: el marcador automático llama y, si no detecta una respuesta humana inmediata, cuelga a los pocos segundos (son las llamadas "silenciosas" o llamadas que duran entre 1 a 6 segundos que molestan a los consumidores). Así, un criterio objetivo implementado en Brasil fue el bloqueo preventivo de cualquier número de teléfono que, en un día, origine más de 100.000 llamadas, de las cuales más del 85 % duran menos de 6 segundos. Este perfil de tráfico indica claramente una activación automatizada de llamadas no deseadas. De hecho, ANATEL constató que cuanto mayor es la proporción de llamadas muy cortas, mayores son los indicios de robocalls y de prácticas irregulares. Sobre esta base, en 2022 estableció un límite de 100.000 llamadas cortas por día, por originador, para todas y cada una de las líneas telefónicas del país. A los números que superasen este volumen se les suspendería temporalmente el acceso.

- **Bloqueo y detención de llamadas abusivas:** La aplicación de estos criterios ha permitido detener miles de millones de llamadas automatizadas en su origen. En Brasil, los propios operadores implementaron sistemas en sus centrales de conmutación para identificar cuándo un determinado número de identificación fiscal o número de teléfono superaba el "semáforo rojo" de llamadas al día, y bloquearon estas llamadas antes de que llegaran al destinatario. Además, se determinó que en las llamadas realizadas mediante robocall, si no hay respuesta inmediata del destinatario (es decir, nadie dice "hola"), la llamada debe desconectarse inmediatamente para no molestar al consumidor. Esta norma obliga a las empresas a configurar sus marcadores para no generar llamadas interminables que quedan sin respuesta. Recomendación para Colombia: podría adoptar formalmente criterios similares - por ejemplo, definir un límite diario de llamadas por originador (ajustado al tamaño del mercado colombiano) y un porcentaje máximo de llamadas muy cortas. Una primera sugerencia podría ser: toda línea que realice más de 50.000 llamadas diarias, de las cuales más del 85% sean de menos de 5 o 6 segundos de duración, debería ser investigada y podría ser bloqueada como medida de precaución . El regulador podría ajustar estos valores con el tiempo. Lo importante es enviar un mensaje claro: no se tolerarán volúmenes masivos de llamadas silenciosas a menos que la organización pueda demostrar que son legítimas. Estos límites objetivos crean un estándar técnico para la monitorización automática y estandarizan las acciones de los operadores a la hora de bloquear los abusos.

- **Mecanismo de implementación:** Idealmente, se debería exigir a los operadores que implementen filtros en sus redes que detecten el incumplimiento de estos criterios en tiempo real. Cuando se identifique un número abusivo, sus llamadas deberían dejar de completarse (bloqueo automático de llamadas) y los detalles deben informarse al regulador (véase el Eje 5 sobre monitoreo). Esta interrupción puede ser temporal (por ejemplo, 15 días) hasta que el emisor dé explicaciones y ajuste su comportamiento. En Brasil, en poco más de un año de vigencia de las medidas cautelares vigentes, más de 582 números/empresas fueron bloqueados sumariamente por exceder los límites establecidos, deteniendo inmediatamente millones de llamadas no deseadas. Importante: los criterios deben ser públicos y objetivos, para garantizar la previsibilidad. Las empresas legítimas de centros de llamadas podrán adaptarse (reduciendo el ritmo de llamadas sin respuesta humana, por ejemplo) para evitar bloqueos, mientras que los actores maliciosos inevitablemente serán atrapados por el alto volumen de llamadas cortas.

Eje 5: Plataforma Centralizada de Análisis y Bloqueo de Mensajes SMS Ilícitos

- **Plataforma Centralizada de Detección**: Se recomienda la implementación de una Plataforma Centralizada a nivel país para la detección, análisis y mitigación de mensajes SMS con fines ilícitos, operada bajo supervisión del regulador y con participación obligatoria de todos los operadores móviles. Actualmente, el proyecto de reglamento establece que los operadores deben contar con plataformas tecnológicas para bloquear mensajes que contengan URLs adulteradas, prácticas de suplantación o tráfico originado desde SIM Box. Sin embargo, este enfoque distribuido (por operador) puede generar asimetrías en capacidades, cobertura y efectividad.

- **Esfuerzo coordinado y homogéneo**: En ese sentido, se propone evolucionar hacia un modelo centralizado que permita aplicar criterios homogéneos de detección, consolidar la información de tráfico a nivel nacional y ejecutar acciones coordinadas frente a campañas de fraude. Esta plataforma actuaría como un punto común de análisis donde se procesen los mensajes (particularmente el tráfico A2P y el tráfico internacional), incorporando capacidades avanzadas de análisis en tiempo real. El resultado esperado es una mejora sustancial en la detección temprana de campañas de smishing, una reducción de brechas entre operadores y una mayor trazabilidad del origen del fraude, alineándose con las mejores prácticas internacionales en materia de control de tráfico ilícito.

Eje 6: Integración con esfuerzos internacionales antifraude

- **Integración con esfuerzos internacionales**: Se recomienda incorporar mecanismos como el uso de motores de reputación de URLs en tiempo real, análisis semántico del contenido mediante modelos de inteligencia artificial, identificación de patrones asociados a campañas masivas (mensajes con estructuras similares enviados a gran escala) e integración con bases de datos internacionales de amenazas.

- **Pasar de enfoque Reactivo a Proactivo**: Se deben establecer lineamientos técnicos que fortalezcan la implementación de capacidades avanzadas de análisis de contenido en los mensajes SMS, con especial énfasis en la identificación de

amenazas asociadas a fraude, suplantación de identidad y distribución de contenido malicioso de forma masiva. El sistema de protección debe ser capaz de anticipar la aparición de campañas de fraude antes de que alcancen una escala significativa, fortaleciendo así la protección del ecosistema de mensajería y de los usuarios finales. En particular, resulta fundamental detectar en etapas muy tempranas campañas de mensajes que contengan URL´s con patrones adulterados —como dominios falsificados, acortadores maliciosos o técnicas de *typosquatting*— así como aquellos que presenten características propias de ingeniería social o estén vinculados a campañas de *phishing* o propagación de *malware*.

Eje 7: Establecimiento Común de Patrones vinculados a SIM Boxes

- **Homogenización de Patrones de Detección de SIM Boxes**: Las Cajas SIM Boxes constituyen uno de los principales vectores para la generación de tráfico SMS fraudulento y también para la evasión de controles regulatorios y comerciales en llamadas de larga distancia. Se recomienda como necesario incorporar un enfoque estructurado basado en patrones de comportamiento. Variables como el volumen de mensajes enviados por línea, la distribución temporal del tráfico, la ausencia de tráfico entrante asociado y la movilidad anómala de las SIM. Asimismo, se recomienda promover el intercambio de información entre operadores respecto a orígenes sospechosos, de manera que las acciones de bloqueo no se limiten a una sola red. La implementación de la plataforma centralizada propuesta permitiría además detectar operaciones de SIM Box que actúan de forma distribuida, incrementando significativamente la efectividad del control.

Eje 08: Repositorio Nacional de Inteligencia Compartida y Gestión de Reputación

- **Repositorio Nacional Antifraude en Telecomunicaciones**: Se recomienda la creación de un repositorio nacional que almacene inteligencia compartida y que permita consolidar, procesar y distribuir información relevante sobre tráfico SMS fraudulento entre operadores y el regulador. Este sistema debe constituirse como un repositorio central de indicadores de riesgo, permitiendo alimentar de manera continua los mecanismos de detección implementados en las redes.

  Entre los elementos que deberían formar parte de este sistema, se incluyen:
  - Listas de números origen asociados a fraude o actividades sospechosas
  - Repositorios de URLs maliciosas o con patrones adulterados
  - Identificadores alfanuméricos utilizados en campañas de suplantación

  La disponibilidad de esta información en tiempo real va a permitir a los operadores aplicar controles más efectivos y coordinados, reduciendo significativamente la capacidad de los actores maliciosos de reutilizar infraestructuras o rotar identidades entre redes. Este enfoque rompe con la fragmentación actual y establece un modelo de defensa colaborativa a nivel país.

Eje 9: Monitoreo centralizado e informes periódicos

- **Sistema de monitoreo centralizado:** Se propone crear un sistema centralizado, administrado por el regulador colombiano, para monitorear continuamente el tráfico de llamadas en los distintos operadores, con especial atención a la

identificación de patrones abusivos o indicios de fraude. Este sistema debería recopilar periódicamente datos estadísticos de los operadores -por ejemplo, el volumen de llamadas originadas por número, la distribución de la duración de las llamadas, las horas pico, la aparición de llamadas internacionales sospechosas- y consolidar esta información para generar informes de monitoreo periódicos. En Brasil, ANATEL ha establecido la obligatoriedad de que los proveedores envíen informes mensuales que contengan detalles de las llamadas con signos de suplantación de identidad u otras irregularidades. Según la Orden de Decisión N° 262/2024, antes del día 15 de cada mes los operadores deben reportar datos como: lista de números de origen que realizaron llamadas sospechosas, número de intentos, fechas, horas, número de destino e identificación del proveedor de origen y destino involucrados. Estos informes permiten al regulador detectar rápidamente actividades anómalas, mapear el rendimiento de las llamadas automáticas e interconexiones entre redes. Con base en la información, el regulador puede, por ejemplo, notificar formalmente a los operadores responsables o facilitadores de las llamadas ilícitas, exigiendo su corrección, e incluso suspender las interconexiones en casos graves.

- **Transparencia y publicación de resultados:** Además de la presentación de datos internos, se recomienda que el regulador elabore informes públicos periódicos (trimestrales o semestrales) que revelen los principales indicadores de la lucha contra las llamadas ilícitas, por ejemplo: la evolución del volumen de llamadas cortas en el país, el número de números bloqueados en el período, el ranking de operadores con mayor tráfico no deseado, número de quejas recibidas, etc. Esta transparencia, adoptada por ANATEL, generó una mayor presión social y del mercado para reducir el problema. En agosto de 2023, por ejemplo, ANATEL informó que en un año hubo una reducción del 41% en las llamadas cortas y presentó cifras de bloqueo y adhesión al prefijo 0303; datos que tuvieron eco en los medios de comunicación y reforzaron el compromiso de las empresas con el cumplimiento de las normas. Para Colombia, se sugiere implementar un "*Panel de Monitoreo de Llamadas No Deseadas*", puesto a disposición del público y actualizado periódicamente, que muestre la efectividad de las medidas. Esto aumentará la confianza de los consumidores en las acciones del regulador y servirá como mecanismo de rendición de cuentas de la iniciativa.

- **Rendición de cuentas mediante el monitoreo:** Con un sistema de monitoreo robusto, el regulador podrá tomar medidas proactivas contra los infractores. En Brasil, el análisis de los informes de tráfico ha permitido abrir procedimientos sancionadores contra los infractores reincidentes (véase el Eje 8). En Colombia, el sistema centralizado podría impulsar directamente la aplicación de los criterios del Eje 4: si identifica un número que supera los límites, el propio sistema genera alertas e instrucciones de bloqueo. Además, en el contexto de STIR/SHAKEN, el monitoreo podría registrar el porcentaje de llamadas autenticadas vs. no autenticadas, lo que ayuda a medir la adopción de la tecnología y su efectividad. Según la experiencia internacional, se espera que con el tiempo la mayoría de las llamadas legítimas sean autenticadas y verificadas, mientras que las llamadas no verificadas (sin firma STIR) pasarán a ser minoritarias y potencialmente sospechosas. El monitoreo continuo respaldará futuros ajustes de la regulación normativa (por ejemplo, endurecimiento de los límites o ampliación de las obligaciones) con base en datos concretos de la realidad colombiana.

Eje 10: Canal de denuncia prioritario (Instituciones financieras y otros)

- **Notificación rápida de números sospechosos:** Se sugiere establecer un canal de comunicación prioritario dedicado a las notificaciones de las entidades financieras (bancos, fintechs, cooperativas) sobre números telefónicos usados para cometer fraudes. Los bancos a menudo son el objetivo de estafadores que se hacen pasar por agentes para robar datos de los clientes, por lo que están en condiciones de identificar rápidamente patrones de llamadas fraudulentas realizadas en nombre de sus marcas. En Brasil, ANATEL ordenó recientemente la creación de un canal sectorial específico para recibir quejas de los bancos sobre números utilizados para cometer estafas. A través de este canal directo, los bancos informan a los operadores y al organismo regulador sobre los detalles de las llamadas fraudulentas activas (números de origen, horarios, contenido de la estafa). Recomendación: El regulador colombiano debería establecer un mecanismo similar, por ejemplo: un contacto dedicado (portal en línea y aplicación) donde los bancos y otras instituciones financieras puedan reportar inmediatamente números sospechosos. Estos reportes deberían tratarse como una prioridad, dado el alto potencial de daño a los consumidores en estos casos de fraude financiero.

- **Acción inmediata de operadores y autoridades:** Una vez recibida una queja calificada de una institución financiera, el procedimiento recomendado es que los operadores identifiquen al abonado responsable de ese número y bloqueen su acceso a las redes telefónicas, poniendo fin rápidamente a las actividades ilícitas. Simultáneamente, el operador de origen y el regulador deben contactar a las autoridades policiales competentes y transmitir la información para la investigación penal. Esta reacción casi en tiempo real es crucial, ya que los estafadores suelen operar durante unos días con un número y luego lo abandonan, por lo que la rapidez de la denuncia y el bloqueo marca la diferencia en la contención del daño . ANATEL ha establecido que cuando los proveedores reciban denuncias a través de este canal especial, deben utilizar los datos facilitados para identificar a la persona que llama y al proveedor de origen, bloquear la línea denunciada y remitirla a las autoridades de seguridad pública. Colombia podría formalizar un proceso similar, incluyendo la cooperación con organismos como la policía nacional, las subdivisiones antifraude y las asociaciones bancarias, para que este flujo de información sea ágil y seguro.

- **Expansión a otros sectores críticos:** Aunque la prioridad son las instituciones financieras (debido a las estafas que involucran cuentas bancarias, tarjetas y préstamos), el canal de reporte del sector puede expandirse a otros sectores vulnerables, por ejemplo, las operadoras de telefonía móvil pueden denunciar números utilizados para clonar WhatsApp; las empresas de comercio electrónico pueden reportar llamadas automáticas de falsos servicios de cobro de deudas; las agencias gubernamentales pueden denunciar números usados en el secuestro de datos (ransomware) a través de llamadas, etc. Lo importante es que exista un canal de comunicación rápido entre las grandes organizaciones que son víctimas de suplantación de identidad y los operadores/autoridades, para que los números de teléfono maliciosos sean cortados lo antes posible. Esta medida de colaboración se anticipa a las denuncias individuales de los usuarios, lo que permite bloquear a los estafadores antes de que alcancen a un gran número de víctimas.

Eje 11: Campañas de concientización y educación digital

- **Concientización pública**: Las tecnologías y las medidas regulatorias solo alcanzarán el máximo efecto si van acompañadas de la concientización del usuario. Por ello, se recomienda que el gobierno colombiano y el regulador promuevan campañas públicas de educación digital centradas en: (a) enseñar a los consumidores a reconocer llamadas legítimas (por ejemplo, identificador de llamadas verificado en pantalla, prefijo especial "XYQZ" que indica telemarketing, etc.); (b) advertir sobre estafas telefónicas comunes y técnicas de ingeniería social; (c) orientar sobre cómo reaccionar ante llamadas sospechosas (no facilitar datos personales, colgar y buscar los canales oficiales de la empresa de la que supuestamente procede la llamada, denunciar números fraudulentos a través de los canales adecuados, etc.). En Brasil, ANATEL ha incorporado estas acciones a través del movimiento #FiqueEsperto, que consiste en difundir consejos de seguridad en redes sociales y radio, enfatizando la precaución a la hora de recibir ofertas por teléfono o mensajes SMS. En octubre (Mes de la Ciberseguridad), se han realizado intensas campañas para evitar que las personas caigan en estafas, complementando medidas técnicas como Origen Verificado.

- **Campañas y asociaciones permanentes:** Se sugiere que la CRC lance una campaña nacional (por ejemplo, "No caigas en la estafa: responda con seguridad" o similar), utilizando la radio, la televisión, los medios sociales y folletos digitales, explicando las nuevas normas (STIR/SHAKEN, prefijo obligatorio, etc.) de forma didáctica y fomentando un comportamiento seguro. Esta campaña debe ser permanente o periódica, ya que los estafadores cambian constantemente de táctica y es necesario educar a las nuevas generaciones de usuarios. Para ampliar el alcance de los mensajes, pueden involucrar socios como asociaciones de protección al consumidor, federaciones bancarias (interesadas en reducir el fraude), operadores de telecomunicaciones y gigantes tecnológicos para amplificar el alcance de los mensajes. En Brasil, ANATEL cuenta con el apoyo de empresas tecnológicas en el movimiento #FiqueEsperto, y ha creado portales como "Qual Empresa Me Ligou?" (¿Qué empresa me llamó?), que permite a los usuarios comprobar si un número pertenece a una empresa conocida. Iniciativas similares en Colombia aumentarían la alfabetización digital y convertirían al usuario en el eslabón más fuerte de la cadena, no el en más débil.

- **Enfoque en la prevención de estafas:** Los mensajes de concientización deben destacar las formas más comunes de estafas telefónicas en el contexto local - por ejemplo, llamadas que simulan ser de bancos solicitando tokens o contraseñas, premios falsos por SMS pidiendo que se devuelva la llamada, la estafa del "falso familiar en apuros", entre otras. Los usuarios bien informados tienden a sospechar cuando reciben una llamada no verificada o una llamada de un número extraño que exige una acción urgente. Además, se debe promover el uso de las herramientas de protección disponibles : registrarse en listas de *No Molestar* (si están disponibles), utilizar bloqueadores de llamadas en teléfonos celulares y, especialmente, valorar el nuevo sello/verificación de llamadas autentificadas (en el caso de STIR/SHAKEN, instruir a los usuarios a responder las llamadas que aparezcan como verificadas con mayor confianza). Como se mencionó, ANATEL combina tecnología y educación para combatir el fraude - este equilibrio también será beneficioso en

Colombia, asegurando que las innovaciones (como la autenticación de llamadas) se comprendan y tengan una adopción popular.

Eje 12: Intensificación de sanciones y compromisos de conducta

- **Aplicación clara y progresiva:** Para que todas las medidas anteriores sean efectivas, es fundamental prever sanciones claras, proporcionales y escalonadas para los infractores, así como mecanismos de negociación para ajustar el comportamiento. Se recomienda que el marco normativo colombiano establezca desde sanciones leves (amonestaciones, multas administrativas proporcionales a la facturación) hasta severas (suspensión de licencias, bloqueo de acceso, multas multimillonarias) para quienes violen sistemáticamente las normas anti-spam/fraude. La experiencia brasileña ilustra un modelo de escalada: inicialmente, a las empresas sorprendidas superando los límites de llamadas cortas se les bloquean los números (suspensión inmediata del acceso - gov.br). ANATEL, luego ofreció la posibilidad de firmar Términos de Compromiso - acuerdos formales en los que la empresa se compromete a cesar el comportamiento irregular y a cumplir con los límites establecidos, bajo pena de fuertes multas en caso de reincidencia reincidencia (gov.br). Más de un centenar de empresas de Brasil se han adherido a estos términos de ajuste, lo que les permite volver a conectarse siempre que tengan un buen comportamiento (gov.br). Para las empresas que no se adhirieron a ellas o continuaron infringiendo las normas, la agencia inició procedimientos sancionadores formales: hasta enero de 2025, se habían abierto 24 procedimientos, con un resultado de 32 millones de reales en multas por telemarketing abusivo. Esta cifra ya ha aumentado a 39 millones de reales (a finales de 2024), a medida que se juzgan nuevos casos. En otras palabras, las sanciones se fueron endureciendo gradualmente para quienes no se adaptaron voluntariamente.

- **Multas proporcionales y TACs:** En Colombia, se sugiere que el marco regulatorio incluya multas proporcionales a la gravedad y reincidencia de la infracción (por ejemplo, un tope de “X” UVT´s o un porcentaje de la facturación anual de la empresa infractora, asegurando que la multa tenga un efecto disuasivo y no sea simplemente absorbida como un "costo de hacer negocios"). Las multas iniciales por infracciones leves podrían ser menores, pero deberían escalar rápidamente en caso de reincidencia. Paralelamente, se debería incorporar la figura del Compromiso de Ajuste de Conducta (inspirado en los Términos de Compromiso brasileños): este permite a las empresas que incumplen por primera vez firmar un acuerdo con el regulador, comprometiéndose a implementar medidas correctivas (por ejemplo, invertir en sistemas anti-llamadas automáticas, capacitar a los equipos, reducir el volumen de llamadas) a cambio de la suspensión o atenuación de la sanción. Si se cumple el acuerdo y no hay reincidencia, la empresa queda regularizada; si no cumple, estará sujeta a sanciones predefinidas más elevadas.

- **Sanciones máximas y efectos administrativos:** El marco regulatorio debe dejar claro que los reincidentes o quienes actúen de mala fe estarán sujetos a las sanciones máximas, que pueden incluir: multas elevadas, suspensión temporal del derecho a operar e incluso cancelación de la licencia en casos extremos, por ejemplo, ANATEL ha señalado que los entes/empresas que se coludan con prácticas delictivas (como permitir el uso de miles de tarjetas SIM fraudulentas sin

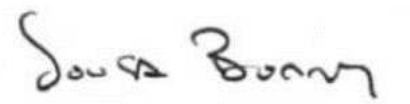
tomar medidas) podrían perder su autorización para operar el servicio. En Colombia, se podría explicitar que *"quien persista en eludir las normas podría perder el derecho a operar el servicio telefónico"* tendrá un fuerte efecto disuasorio en el sector. Asimismo, el regulador debe tener la facultad de suspender rápidamente las interconexiones o los accesos de las empresas infractoras -esto se utilizó en Brasil para cortar el flujo de llamadas de ciertos originadores hasta que cooperaran-. Es importante mencionar que la cooperación entre autoridades también es parte de la sanción: en Brasil, los casos graves de estafas que involucran a instituciones financieras son remitidos por ANATEL a las autoridades policiales para el procesamiento penal de los involucrados. Esta cooperación debería darse en Colombia, de modo que la sanción administrativa (por ejemplo, el bloqueo del número fraudulento) vaya acompañada de una investigación penal contra de los verdaderos estafadores.

En resumen, la combinación de medidas tecnológicas innovadoras (STIR/SHAKEN, Plataforma Centralizada de Protección, etc.) con normas objetivas y un monitoreo riguroso ha demostrado ser la estrategia más efectiva para combatir las llamadas y mensajes ilícitos. El creciente fenómeno del fraude en telecomunicaciones debe ser mitigado mediante el uso de plataformas centralizadas de análisis, inteligencia artificial aplicada al contenido y modelos de reputación compartida. Inspirándose en la exitosa experiencia de Brasil —que en poco más de dos años ha logrado una reducción del 41% de las llamadas cortas y el bloqueo de cientos de llamadas abusivas— y en las prácticas ya adoptadas en países como EE.UU. y Canadá, donde también se han incorporado mecanismos avanzados de control de mensajería fraudulenta, Colombia situará su marco regulatorio a la vanguardia de la lucha contra el fraude en las telecomunicaciones.

Las recomendaciones anteriores tienen como objetivo restaurar la confianza de los usuarios colombianos en el servicio telefónico y en los canales de mensajería, asegurando que las comunicaciones legítimas sean identificadas y confiables, mientras que los abusos y delitos —tanto en voz como en SMS— sean rápidamente detectados, bloqueados y mitigados. Estas buenas prácticas internacionales, probadas en entornos más avanzados, son las que se están proponiendo adaptar al contexto colombiano, con el fin de lograr una reducción significativa del fraude y proteger de manera efectiva a los usuarios. Con la implementación de estos ejes temáticos creemos que Colombia estará fuertemente preparado para enfrentar el desafío de las llamadas y mensajes con fines ilícitos.

Sin otro asunto en particular, nos despedimos.

Atentamente;



MARIO JORGE FERREIRA DE SOUSA BORGES
Gerente General
CLEARTECH PERÚ S.A.C.