OBSERVACIONES 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»

Etapa de participación sectorial — Comisión de Regulación de Comunicaciones (CRC)

Presentado por SAEM COLOMBIA S.A.S. — NIT 900.756.372-4

Respetados Comisionados:

En ejercicio del derecho de participación previsto en el artículo 8 de la Ley 1437 de 2011, en los artículos 2.2.13.3.2 y 2.2.13.3.3 del Decreto 1078 de 2015 y conforme a los principios de intervención del Estado de la Ley 1341 de 2009, SAEM COLOMBIA S.A.S. presenta sus observaciones al proyecto de resolución de la referencia. A diferencia de un pronunciamiento meramente general, este documento se estructura **artículo por artículo**, identifica los efectos concretos de cada medida sobre nuestra actividad, contrasta cada propuesta con experiencias regulatorias internacionales comparables —incluidas aquellas que fracasaron o produjeron efectos no deseados— y propone alternativas que permiten alcanzar el objetivo de mitigación del fraude sin trasladar cargas desproporcionadas a los agentes formales del mercado.

I. Calidad en la que actúa SAEM y alcance de su interés

SAEM COLOMBIA S.A.S. es una empresa colombiana cuya **actividad económica principal es la de Integrador Tecnológico (IT)** de mensajería SMS para Proveedores de Contenidos y Aplicaciones (PCA). En los términos del proyecto, SAEM sería **asignataria del recurso de identificación «código corto A2P»** (artículo 6.4.1.3 propuesto), por cuanto provee la infraestructura de conexión directa con los PRST y cursa, a través de ella, el tráfico de múltiples PCA. SAEM no es —por regla general— asignataria de SENDER ID, salvo respecto del contenido propio que llegara a producir.

Adicionalmente, SAEM presta servicios de **call blasting y telefonía VoIP, envío masivo de correo electrónico**, y opera en varios países de Latinoamérica bajo el dominio saem.tel. Por ello, además de las medidas sobre SMS A2P, le resultan directamente aplicables las disposiciones sobre prevención del fraude en voz (artículo 2.1.10.7.2.2 propuesto: bloqueo de CLI, listas DNO, etiquetado de llamadas y registro de llamadas con fines publicitarios) y la ampliación del RNE al correo electrónico (artículo 2.1.18.1 propuesto).

En su condición de asignataria de código corto A2P, SAEM quedaría además obligada a: (i) financiar al validador centralizado (artículo 6.13.1.2); (ii) adelantar el proceso de KYC sobre cada PCA (artículo 6.13.3.1); (iii) integrar sus plataformas con el validador (artículo 6.13.4.5.2); (iv) participar como miembro obligado del Comité Técnico de Lucha contra el Fraude (artículo 2.1.10.7.3) y del Comité Técnico de Seguimiento (artículo 6.13.5.1); y (v) consolidar sus códigos cortos en uno solo (artículo 19). El interés de SAEM es, por tanto, directo, cierto y cualificado.

II. Consideraciones generales

2.1. Los integradores formales no son el vector del fraude; lo son los actores que operan al margen del régimen

La cadena de valor A2P formal opera bajo contratos con personas jurídicas constituidas, debida diligencia documental, verificación de existencia y representación legal y trazabilidad de extremo a extremo. El fraude por SMS, en cambio, se origina mayoritariamente en factores ajenos a los recursos de identificación asignados legalmente, a saber:

- SMS spoofing (falsificación del remitente alfanumérico o numérico), que no requiere acceso a un código corto asignado.
- Uso de numeración ilegal o no atribuida y de rutas grises de larga distancia internacional.
- Plataformas clandestinas de mensajería y agregadores no establecidos en el país que transaccionan desde el exterior.
- SIM farms, simboxes y estaciones base falsas (IMSI catchers / «SMS blasters»), que inyectan tráfico sin pasar por la red del PRST.
- Suplantación de marcas y entidades mediante herramientas de inteligencia artificial.

Según la Global Anti-Scam Alliance, las pérdidas mundiales por fraude digital superan los USD 442 mil millones anuales, y los reportes de la GSMA atribuyen el crecimiento del fraude a la suplantación y a tecnologías de IA, no a los actores regulados. *La consecuencia regulatoria es clara: una medida que recae sobre quien ya cumple no reduce el fraude que se origina por fuera del perímetro regulado; simplemente desplaza costos y, como muestra la evidencia internacional citada más adelante, el fraude migra al canal menos regulado.*

2.2. Ausencia de cuantificación del impacto y de proporcionalidad (Ley 1341 de 2009, AIN-OCDE)

El artículo 19 de la Ley 1341 de 2009 (modificado por la Ley 1978 de 2019) ordena que la regulación promueva la inversión, la simplificación regulatoria y la protección al usuario, y la metodología de Análisis de Impacto Normativo (AIN) promovida por la OCDE exige soportar las decisiones en un análisis costo-beneficio. El proyecto, sin embargo, no cuantifica: (i) el costo de implementación y operación del validador centralizado que recaerá sobre los IT; (ii) la reducción de ingresos ya causada por la Ley 2300 de 2023; (iii) el costo de las obligaciones de KYC, integración por APIs, reportería, campañas pedagógicas y formación interna; ni (iv) la relación entre ese costo agregado y la reducción efectiva de fraude esperada. Solicitamos que el documento soporte incorpore esa cuantificación antes de adoptar las medidas.

III. Observaciones específicas al articulado

Las siguientes observaciones siguen el orden del articulado del proyecto. Para cada punto se indica: la disposición, el efecto sobre SAEM como IT, la experiencia internacional pertinente y una propuesta concreta de ajuste.

3.1. Validador centralizado: financiado por los IT pero seleccionado por los PRSTM (arts. 14 —Capítulo 13— y 18)

Disposición. El artículo 6.13.1.2 establece que los costos de implementación, gestión, operación y mantenimiento del validador centralizado serán remunerados por «los asignatarios de código corto A2P» —es decir, por los IT—. No obstante, el artículo 18.1 atribuye la selección del

validador exclusivamente a los PRSTM, y el artículo 6.13.5.1 conforma el Comité de Seguimiento únicamente con asignatarios de código corto A2P, sin voto del validador.

Efecto sobre SAEM. Se configura una asimetría estructural: quien paga (el IT) no decide, y quien decide (el PRSTM) no asume el costo. Además, los PRSTM compiten en el mismo mercado en su calidad de IT (el propio artículo 6.4.1.3 los habilita como asignatarios de código corto A2P), de modo que un competidor selecciona y fija las condiciones del proveedor monopólico que el resto de competidores está obligado a contratar y financiar. Esto plantea un riesgo evidente de abuso de posición de dominio y de fijación de tarifas y especificaciones técnicas que favorezcan a unos agentes sobre otros.

Experiencia internacional. La concentración de toda la validación A2P en una única persona jurídica crea un punto único de falla (single point of failure) sobre el 100% del tráfico A2P nacional. La experiencia de la India con el sistema DLT (descrita en 3.2) muestra que la dependencia de un único pipeline de validación —cuando falla— bloquea masivamente tráfico legítimo, incluidos OTP y mensajes transaccionales críticos.

Propuesta. (i) Que el órgano de selección y gobierno del validador esté integrado, con voz y voto, por los IT que financian su operación, y no solo por los PRSTM; (ii) que el financiamiento se distribuya entre toda la cadena de valor (PRSTM, IT y PCA) y no exclusivamente sobre los IT, o que su costo sea remunerado dentro del esquema de remuneración de la Fase II; (iii) que la tarifa del validador se someta a un tope o a revisión de la CRC bajo el principio de orientación a costos, con publicidad de su estructura; y (iv) que el régimen contemple expresamente la posibilidad de más de un validador acreditado e interoperable, para evitar el monopolio y el punto único de falla.

3.2. Régimen de plantillas de contenido A2P: el modelo que fracasó en la India (art. 14 —Sección 4— y 6.13.4)

Disposición. Ningún mensaje A2P podrá enrutarse si no está respaldado por una plantilla aprobada y vigente (art. 6.13.4.1). Las plantillas tienen vigencia mensual con renovación automática (art. 6.13.4.3.3), deben aprobarse en 24–48 horas (art. 6.13.4.3.1) y el PRST debe validarlas en tiempo real, mensaje por mensaje, antes del enrutamiento (art. 6.13.4.7).

Efecto sobre SAEM. El tráfico A2P real es de altísimo volumen y, en gran parte, dinámico (OTP, alertas, notificaciones transaccionales con campos variables). Un régimen de plantillas rígido, con campos variables limitados y vigencia mensual, genera un riesgo permanente de divergencia entre el contenido aprobado y el cursado, lo que —por la vía del artículo 6.13.4.4 y de las causales 6.4.3.2.6 y 6.12.3.2.12— puede derivar en la recuperación del código corto A2P del IT por conductas que no controla.

Experiencia internacional (caso India). India implementó en 2018–2021, mediante la TCCCPR de la TRAI, un sistema de registro obligatorio de entidades, cabeceras (headers) y plantillas de contenido sobre blockchain/DLT, conceptualmente idéntico al aquí propuesto. Cuando entró en operación el «scrubbing» de plantillas (marzo de 2021), se bloquearon masivamente mensajes legítimos —incluidos OTP bancarios y notificaciones transaccionales—, al punto que el regulador

tuvo que suspender temporalmente la verificación. El cronograma se aplazó en repetidas ocasiones durante años, el onboarding de empresas se congestionó y el desajuste entre contenido dinámico y plantillas rígidas resultó estructural. Pese a todo ello, el fraude continuó por rutas no registradas, OTT y spoofing. Es el precedente más directo y debe ser advertencia, no modelo.

Propuesta. (i) Diferenciar por modalidad: exigir preaprobación de plantilla únicamente para contenido comercial/publicitario, y aplicar un régimen liviano (registro categórico, sin aprobación previa mensaje a mensaje) a OTP/autenticación, transaccional e informativo y regulatorio, por su carácter crítico y sensible al tiempo; (ii) admitir plantillas con campos variables amplios y reglas de coincidencia tolerantes; (iii) sustituir la vigencia mensual por una vigencia anual o indefinida sujeta a revisión periódica; (iv) prever, durante una rampa inicial prolongada, que la falta de coincidencia genere etiquetado «sin verificar» y no bloqueo; y (v) fijar un mecanismo expreso de plantillas de emergencia para campañas urgentes de interés público.

3.3. Validación en tiempo real, mensaje a mensaje, por el PRST (art. 6.13.4.7 y 6.13.2.1)

Disposición. El PRST debe consultar al validador, antes de enrutar cada mensaje A2P, la validez del código corto A2P, del SENDER ID y de la plantilla (art. 6.13.4.7.1). El validador debe responder en ≤200 ms (≤500 ms en alta demanda) con disponibilidad del 99,5% mensual (art. 6.13.2.1).

Efecto sobre SAEM. Una disponibilidad del 99,5% admite hasta ~3,6 horas de indisponibilidad mensual; durante esos lapsos, si el PRST opta por bloquear (opción que el art. 6.13.4.7.2 le permite), se interrumpe la entrega de OTP y notificaciones críticas que cursa el IT, con afectación directa a sus clientes y a los usuarios finales. La latencia añadida también degrada throughput en picos.

Propuesta. (i) Elevar la disponibilidad exigida a ≥99,95% y robustecer las exigencias de redundancia geográfica; (ii) que ante indisponibilidad la conducta por defecto sea «fail-open» con etiqueta «sin verificar» —nunca bloqueo de tráfico previamente validado—; (iii) admitir verificación por listas sincronizadas en caché local del PRST (en lugar de consulta sincrónica mensaje a mensaje) para reducir latencia y dependencia del enlace; y (iv) someter los SLA y el plan de contingencia (art. 6.13.2.2) a prueba conjunta con los IT antes de su entrada en vigencia.

3.4. SENDER ID: unicidad por NIT, exigencia de sucursal a extranjeros y registro de marca (arts. 1, 13 —Cap. 12—)

Disposición. Se crea el SENDER ID alfanumérico (3–11 caracteres), uno solo por NIT o cédula (art. 6.12.1.2, parágrafo 2). Los solicitantes extranjeros solo pueden ser asignatarios si establecen sucursal en Colombia. El SENDER ID debe corresponder a razón social, nombre comercial o marca registrada (art. 6.12.1.1).

Efecto sobre SAEM. Como IT, SAEM gestiona el tráfico de numerosos PCA. La regla de «un único SENDER ID por NIT» es razonable para identificar al originador, pero rigideces como la exigencia de marca registrada o las denominaciones reservadas pueden retrasar el onboarding de clientes legítimos y, por esa vía, empujar a algunos hacia canales no regulados. La exigencia de sucursal a extranjeros, sin un régimen claro de representación, puede excluir a anunciantes legítimos del exterior y trasladar su tráfico a agregadores grises.

Experiencia internacional (caso Singapur). Singapur hizo obligatorio en enero de 2023 su SMS Sender ID Registry (SSIR): los remitentes no registrados se marcan «Likely-SCAM». Aunque inicialmente cayó el smishing con cabeceras suplantadas, los reportes públicos posteriores muestran que el fraude se desplazó hacia plataformas OTT, llamadas de voz y nuevas formas de spoofing, de modo que las pérdidas totales por estafas siguieron al alza. Lección: un registro de remitente reduce un vector específico, pero no el fraude agregado si no se actúa simultáneamente sobre el origen ilícito; conviene calibrar la exigencia para no expulsar al actor legítimo.

Propuesta. (i) Aceptar como soporte del identificador no solo la marca registrada sino también el nombre comercial, la enseña o el uso notorio acreditado; (ii) prever un procedimiento expedito y un canal de representación para anunciantes extranjeros que no implique necesariamente sucursal (p. ej., representante o responsable local solidario), evitando empujar ese tráfico a rutas grises; (iii) publicar con suficiente antelación la lista de palabras reservadas y un mecanismo de objeción.

3.5. Código corto A2P único y consolidación forzosa de los códigos cortos existentes (arts. 12 y 19)

Disposición. Cada agente tendrá un único código corto A2P (art. 6.4.1.4). Los IT con múltiples códigos cortos deben consolidarlos en uno solo durante un período de transición de seis (6) meses (art. 19), eligiendo cuál conservar y migrando el resto, con notificación a usuarios y reglas de consentimiento (art. 19.1.5).

Efecto sobre SAEM. La consolidación implica perder códigos cortos que los clientes y los usuarios ya reconocen, reconfigurar enrutamientos y migrar consentimientos. Técnicamente la identificación recae ahora en el SENDER ID, pero la pérdida de los códigos históricos tiene costo comercial y operativo real. Seis meses, además condicionados a la previa publicación de la remuneración de la Fase II, es un plazo insuficiente frente a la magnitud del cambio (selección de validador, KYC de todos los PCA, asignación de recursos, registro y aprobación de plantillas, integración por APIs y consolidación), todo en cadena.

Propuesta. (i) Ampliar el período de transición a 12–18 meses, dado que las fases del artículo 19 son secuenciales y dependen unas de otras; (ii) permitir que un mismo IT conserve más de un código corto A2P cuando acredite necesidad técnica u operativa objetiva (segmentación de tráfico, continuidad de servicios críticos); (iii) reconocer plenamente la continuidad del consentimiento previo migrado y simplificar la notificación a usuarios; (iv) condicionar el inicio

de la transición a que el ecosistema —no solo la remuneración de la Fase II— esté efectivamente listo (validador operativo y APIs publicadas).

3.6. Obligaciones de KYC a cargo del IT y duplicidad con registros existentes (art. 6.13.3)

Disposición. El IT (asignatario de código corto A2P) debe adelantar el KYC de cada PCA: identificación del agente y del beneficiario final, verificación de objeto social, perfil de riesgo, formalización contractual y conservación de información por cinco (5) años, con debida diligencia continua (arts. 6.13.3.1 y 6.13.3.2).

Efecto sobre SAEM. Aunque SAEM ya realiza debida diligencia, el proyecto eleva el estándar al nivel del régimen de prevención de lavado de activos (beneficiario final), con carga documental y de actualización significativa, en buena medida duplicando información que ya reposa en el RPCAI, el RUES y el RUT. La superposición de KYC del IT y verificación del validador puede generar doble control sobre el mismo agente.

Propuesta. (i) Permitir el aprovechamiento e interoperación con RPCAI, RUES y RUT para no duplicar verificaciones; (ii) delimitar el alcance del «beneficiario final» a umbrales razonables y a fuentes oficiales disponibles; (iii) precisar que el IT cumple su deber con la diligencia documental definida, sin convertirse en garante del comportamiento futuro del PCA; (iv) escalonar la entrada en vigencia de la debida diligencia continua.

3.7. Atribución de responsabilidad por mal uso de plantillas: necesidad de un puerto seguro para el mero transporte (art. 6.13.4.4)

Disposición. El artículo 6.13.4.4 atribuye consecuencias regulatorias —incluida la recuperación del recurso— al IT cuando el mal uso le sea «imputable» por haber permitido o facilitado tráfico no autorizado, y prevé recuperación concurrente cuando el mal uso sea imputable a ambos asignatarios.

Efecto sobre SAEM. El IT provee conectividad y trazabilidad, pero no genera ni controla el contenido, que es responsabilidad del PCA asignatario del SENDER ID. Una atribución amplia o basada en estándares difusos de «facilitación» expone al IT a perder su recurso esencial por conductas de terceros, pese a haber cumplido KYC, integración y reporte.

Experiencia internacional. El derecho comparado reconoce un régimen de responsabilidad limitada para el intermediario que se limita a transmitir («mere conduit»): el artículo 12 de la Directiva 2000/31/CE de la Unión Europea y, hoy, el artículo 4 del Reglamento de Servicios Digitales (DSA, 2022/2065) eximen de responsabilidad por el contenido transmitido a quien no origina la transmisión, no selecciona al destinatario ni modifica la información. Es el estándar que debería guiar la atribución al IT.

Propuesta. (i) Incorporar un puerto seguro expreso: el IT no responderá por el contenido cuando acredite haber cumplido el KYC, la integración con el validador, el bloqueo/suspensión oportuna ante orden o indicio, y el reporte dentro de los plazos; (ii) exigir, para imputar

responsabilidad al IT, un estándar de conocimiento efectivo o negligencia grave, no la mera «facilitación»; (iii) graduar la consecuencia (requerimiento, plan de corrección, suspensión parcial) antes de la recuperación del recurso esencial.

3.8. Suspensión unilateral por el PRST y nuevas causales de oposición al acceso (arts. 5 y 8 —parágrafo 4—)

Disposición. Tras la segunda recuperación de un código corto por ciertas causales, el PRST puede suspender unilateralmente por un mes la relación de acceso; tras la tercera, puede solicitar la desconexión definitiva (art. 8, parágrafo 4). El artículo 5 crea dos causales de oposición al acceso frente a agentes a quienes se autorizó previamente la desconexión.

Efecto sobre SAEM. La suspensión unilateral del acceso por el PRST —que puede ser, a la vez, competidor del IT— sin control previo de la CRC, y las causales de oposición, otorgan al PRST una herramienta con potencial anticompetitivo y afectan la estabilidad del insumo esencial del IT (la interconexión).

Propuesta. (i) Que toda suspensión o desconexión del acceso esté precedida de control de la CRC y del debido proceso, con oportunidad de descargos del IT/PCA; (ii) que la suspensión unilateral solo proceda ante riesgo grave e inminente debidamente acreditado y por el tiempo estrictamente necesario; (iii) que las causales de oposición se interpreten de forma restrictiva y temporal, con carga probatoria a cargo del PRST que se opone.

3.9. Medidas sobre servicios de voz: relevantes para el call blasting y la VoIP de SAEM (art. 3 —2.1.10.7.2.2—)

Disposición. Se prohíbe el enmascaramiento del CLI y se ordena bloquear llamadas internacionales entrantes con CLI nacional (2.1.10.7.2.2.1); se exige monitoreo en tiempo real con etiquetado «Alerta de llamada sospechosa» (2.1.10.7.2.2.2); se crea el registro de «Llamada con fines publicitarios», con bloqueo cuando el destinatario esté en el RNE (2.1.10.7.2.2.2.1); y se impone la lista DNO (2.1.10.7.2.2.3).

Efecto sobre SAEM. Las campañas legítimas de voz (notificación, encuestas, cobranza autorizada) suelen usar un número único de retorno, que un monitoreo mal calibrado puede confundir con robocall y etiquetar o bloquear, afectando la contactabilidad legítima. La prohibición de enmascaramiento es razonable frente al fraude, pero requiere precisar que el uso legítimo de un CLI de retorno corporativo no constituye enmascaramiento.

Experiencia internacional (STIR/SHAKEN). El marco STIR/SHAKEN de autenticación de identificador de llamada en Estados Unidos y Canadá —que el propio proyecto evaluó como alternativa— redujo parte del spoofing, pero las llamadas fraudulentas persistieron, especialmente desde gateways internacionales y redes no IP, confirmando que el origen ilícito y los puntos de entrada no autenticados son el verdadero foco. Ello respalda concentrar el esfuerzo en el bloqueo del tráfico internacional con CLI nacional falsificado, más que en cargar al originador formal.

Propuesta. (i) Precisar que el uso de un CLI de retorno corporativo legítimo, asignado y verificable, no constituye enmascaramiento; (ii) calibrar los umbrales de detección de robocall (ACD/ASR) en el marco del CTLFSM, con participación de los originadores corporativos, para evitar falsos positivos; (iii) priorizar y dotar de recursos el bloqueo del tráfico internacional entrante con CLI nacional falsificado, foco principal del fraude.

3.10. Cargas administrativas recurrentes: campañas, formación y reportería (arts. 6.14.1.3, 6.14.1.5 y 17)

Disposición. Se imponen a los asignatarios del ecosistema A2P al menos cuatro campañas pedagógicas anuales (6.14.1.3), cuatro sesiones anuales de formación interna con reporte trimestral (6.14.1.5) y obligaciones de reporte de información (Formato T.5.9 a cargo del validador, art. 17).

Efecto sobre SAEM. Para un IT mediano, la sumatoria de obligaciones trimestrales de difusión, capacitación y reporte representa una carga administrativa fija desproporcionada respecto del aporte marginal a la prevención del fraude, frente a un agente que no tiene relación directa con el usuario final.

Propuesta. (i) Proporcionalidad por tamaño y por relación con el usuario final: que las campañas masivas recaigan principalmente sobre PRST y PCA con relación directa con el usuario, y que el IT pueda cumplir mediante difusión del micrositio de la CRC; (ii) periodicidad anual o semestral en lugar de trimestral para la formación y los reportes; (iii) formatos de reporte unificados y consultables, evitando duplicidades entre validador, IT y PRST.

3.11. Condicionamiento a la Fase II (remuneración del SMS A2P)

Disposición. La entrada en vigencia de las medidas técnicas de A2P se condiciona a la publicación del acto que defina la nueva remuneración del ecosistema A2P (Fase II), y todo el período de transición se cuenta desde ese hito.

Efecto sobre SAEM. La viabilidad económica del IT depende directamente de la remuneración. Adoptar las cargas técnicas y operativas sin conocer la remuneración impide a SAEM evaluar la sostenibilidad del modelo y planear su inversión. La separación en fases no debe traducirse en incertidumbre sobre los costos que la propia resolución traslada al IT.

Propuesta. (i) Que la Fase II resuelva también, de manera explícita, cómo se remunera o se reconoce el costo del validador y del cumplimiento del nuevo régimen en la cadena de valor; (ii) que el AIN integre el análisis económico de ambas fases, de modo que las cargas técnicas y su financiación se evalúen conjuntamente con la remuneración.

IV. Principios constitucionales y regulatorios comprometidos

Libertad económica e iniciativa privada (art. 333 C.P.). Las restricciones deben respetar el ejercicio legítimo de la actividad empresarial dentro de los límites del bien común; trasladar cargas excesivas a quienes ya cumplen no satisface ese estándar.

Confianza legítima. Los agentes formales han hecho inversiones bajo el régimen vigente de códigos cortos; un cambio abrupto sin transición suficiente afecta expectativas legítimas amparadas por la jurisprudencia constitucional.

Proporcionalidad y necesidad. Toda medida debe ser idónea, necesaria y proporcional al fin. Las medidas que recaen sobre el actor formal, sin atacar el origen ilícito del fraude, no superan el juicio de idoneidad ni de necesidad.

Libre competencia y prohibición de abuso de posición de dominio (Ley 1340 de 2009; abogacía de la competencia, art. 9 ibíd.). El diseño del validador (selección por PRSTM, financiación por IT, monopolio de hecho) y las facultades de suspensión unilateral del PRST deben ser examinados específicamente por la Superintendencia de Industria y Comercio en sede de abogacía de la competencia.

V. Solicitudes

Con fundamento en lo anterior, SAEM COLOMBIA S.A.S. solicita respetuosamente a la Comisión:

1. Realizar y publicar, antes de adoptar las medidas, un Análisis de Impacto Normativo que cuantifique los costos del nuevo régimen (validador, KYC, integración por APIs, reportería, campañas y formación) sobre los IT y la relación de esos costos con la reducción efectiva de fraude.
2. Rediseñar el gobierno y la financiación del validador centralizado: participación de los IT en su selección y gobierno; distribución del costo en toda la cadena de valor (o su reconocimiento en la remuneración de la Fase II); tope o revisión de tarifa orientada a costos; y posibilidad de validadores múltiples e interoperables para evitar el monopolio y el punto único de falla.
3. Diferenciar el régimen de plantillas por modalidad —régimen liviano para OTP, transaccional, informativo y regulatorio; preaprobación solo para comercial—, con campos variables amplios, vigencia anual o indefinida y etiquetado «sin verificar» (no bloqueo) durante una rampa inicial prolongada.
4. Adoptar como conducta por defecto el «fail-open» con etiqueta «sin verificar» ante indisponibilidad del validador, elevar la disponibilidad exigida a ≥99,95% y admitir validación por caché sincronizada para reducir latencia y dependencia.
5. Incorporar un puerto seguro (mere conduit) para el IT, condicionando su responsabilidad al conocimiento efectivo o negligencia grave, y graduando las consecuencias antes de la recuperación del recurso esencial.
6. Ampliar el período de transición a 12–18 meses; permitir más de un código corto A2P por IT ante necesidad técnica acreditada; y reconocer plenamente la continuidad del consentimiento migrado.

7. Interoperar el KYC con RPCAI, RUES y RUT para evitar duplicidades, y delimitar el alcance del beneficiario final y de la debida diligencia continua.
8. Someter a control previo de la CRC y al debido proceso toda suspensión o desconexión del acceso por parte del PRST, e interpretar de forma restrictiva las causales de oposición.
9. Precisar que el uso de un CLI de retorno corporativo legítimo no constituye enmascaramiento, y concentrar el esfuerzo en el bloqueo del tráfico internacional entrante con CLI nacional falsificado.
10. Aplicar proporcionalidad por tamaño y por relación con el usuario final en las obligaciones de campañas, formación y reportería, con periodicidad anual o semestral y formatos unificados.
11. Concentrar la estrategia en las verdaderas fuentes del fraude —SMS spoofing, numeración ilegal, plataformas clandestinas y agregadores no establecidos en el país, SIM farms y SMS blasters, y suplantación basada en IA—, mediante auditoría a plataformas que transaccionan desde el exterior y cooperación con operadores, autoridades y organismos como la GSMA.

Las empresas integradoras tecnológicas hemos desarrollado durante años mecanismos de control, trazabilidad y validación contractual que garantizan la legitimidad de los servicios prestados. Una regulación eficaz debe perseguir a quienes operan al margen de la ley y no imponer mayores cargas a quienes ya cumplen y contribuyen al desarrollo del ecosistema digital colombiano. Quedamos atentos a participar en las mesas de trabajo y comités que la Comisión disponga.

Atentamente,

_____

Juan Camilo Guzman Yara
CEO
SAEM COLOMBIA S.A.S. — NIT 900.756.372-4

Nota: Las referencias a experiencias internacionales (India — TRAI/TCCCPR-DLT; Singapur — SSIR; Estados Unidos/Canadá — STIR/SHAKEN; Unión Europea — Directiva 2000/31/CE y DSA 2022/2065) se incluyen como soporte argumentativo y deben verificarse con fuentes actualizadas antes de la radicación final. Este documento no sustituye el concepto de los asesores jurídicos y regulatorios de la empresa.