Outlook

Observaciones a propuesta regulatoria – Proyecto 2000-41-7-1 – Interacción 3 – ScamZero

Desde Miguel Palma Arcia <miguelandrespalma@hotmail.com>
Fecha Lun 22/06/2026 20:10
Para [2025] [DR] Medidas para mitigar el fraude cibernético <medidasantifraude@crcom.gov.co>

Bogotá, D.C., 22 de junio de 2026

Señores
Comisión de Regulación de Comunicaciones – CRC
Dirección de Diseño Regulatorio
medidasantifraude@crcom.gov.co

REF: Observaciones ciudadanas a la propuesta «Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles» – Proyecto 2000-41-7-1 – Interacción 3

Respetado señor Comisionado:

En atención a la invitación de la CRC y en seguimiento a la respuesta emitida al radicado 2026812737, presento observaciones en calidad de **Miguel Andrés Palma Arcia, Fundador de ScamZero** (info@scamzero.app), aplicación antifraude con inteligencia artificial disponible en Colombia para Android e iOS. He revisado el proyecto de resolución y el documento soporte publicados el 5 de junio de 2026.

I. Valoración general

ScamZero respalda la propuesta regulatoria y reconoce el diagnóstico del documento soporte: el fraude por smishing creció nueve veces entre 2022 y 2023, alcanzando reclamaciones totales de $92.235 millones de pesos en 2024 solo en el sistema financiero —cifra que el propio documento advierte es una subestimación, dado que 15 bancos, 10 compañías de financiamiento y 2 cooperativas no pudieron desagregar sus datos por modalidad. Las medidas propuestas en el artículo 3 de la resolución —monitoreo P2P, bloqueo CLI, listas DNO, etiquetado de llamadas y el Comité Técnico— son necesarias y urgentes.

Sin embargo, el documento soporte identifica con precisión una limitación estructural de la propuesta: los mecanismos de control actúan **en la red y en los operadores**, y el propio documento reconoce que los mecanismos existentes son «reactivos, no predictivos» y que «a nivel sectorial no necesariamente existe un estándar homogéneo respecto a las variables monitoreadas». Esto genera una brecha inevitable: los mensajes y llamadas fraudulentas que superan los filtros de red llegan al usuario final sin ninguna capa de protección adicional.

II. Observación 1: brecha en la capa de protección del usuario final

El artículo 3 de la resolución (numeral 2.1.10.7.2.1) establece que los PRST deben detectar patrones atípicos en SMS P2P —volumen inusual, alta dispersión de destinatarios, homogeneidad de contenido— y aplicar un esquema escalonado de cinco etapas que puede tomar hasta varios días hábiles en completarse. Este mecanismo es correcto para casos de tráfico masivo, pero **no protege al usuario en tiempo real frente al mensaje o llamada individual** que ya llegó a su dispositivo.

El documento soporte identifica explícitamente que el fraude ocurre también **fuera de las redes tradicionales**: el canal OTT (WhatsApp, Telegram, aplicaciones de mensajería) queda fuera del alcance de esta resolución por decisión de alcance, y los estafadores migran activamente hacia esos canales. Un usuario que recibe un enlace de phishing por WhatsApp no está protegido por ninguna de las medidas propuestas en este proyecto regulatorio.

Observación: Se sugiere que el eje de medidas educativas (eje temático c del proyecto) incluya explícitamente una disposición que reconozca y promueva el uso de herramientas de verificación ciudadana en tiempo real —como soluciones de análisis de mensajes, enlaces y números accesibles al usuario desde su dispositivo— como complemento de las medidas de red. Esto no implica señalar una solución específica (respetando la neutralidad tecnológica), sino reconocer la capa de usuario como parte integral de la arquitectura antifraude.

III. Observación 2: composición del Comité Técnico (artículo 3, numeral 2.1.10.7.3)

El numeral 2.1.10.7.3.1 establece que el CTLFSM estará conformado por representantes de los PRST y la CRC, con participación como invitados de COLCERT, la Fiscalía, la Policía, la SIC y la Superintendencia Financiera. Esta conformación cubre la visión de los operadores y las autoridades, pero no incluye representantes de la sociedad civil ni del ecosistema de herramientas ciudadanas.

El documento soporte cita la experiencia de Singapur, donde las instituciones financieras y los operadores son responsables por las pérdidas de los usuarios cuando no cumplen las directrices antifraude. Este modelo implica que el usuario es el beneficiario final de las medidas. Sin embargo, el usuario no tiene voz en el Comité que define esas medidas.

Los comentarios recibidos en la interacción 2 de ASOBANCARIA —citados en el documento soporte— señalan que «la ausencia de medidas suficientemente disuasivas genera un alto retorno económico del fraude y traslada los riesgos y pérdidas al consumidor financiero». Incluir representantes de organizaciones de usuarios y de soluciones de protección ciudadana en el CTLFSM aportaría la perspectiva del usuario como insumo sistemático en las decisiones técnicas del Comité.

Observación: Se propone que el numeral 2.1.10.7.3.1 incluya, además de los miembros actuales, la posibilidad de que la CRC invite de forma permanente —no solo ocasional— a representantes de organizaciones de protección al consumidor digital y desarrolladores de soluciones ciudadanas de mitigación del fraude, cuando los temas de la agenda así lo ameriten.

IV. Observación 3: el eje educativo debe aterrizar en acciones concretas para el usuario

El documento soporte identifica como una de las causas del problema el «desconocimiento de los usuarios respecto de la privacidad de la información, de las modalidades de ataque y de sus posibles acciones de prevención y mitigación». El eje temático (c) propone medidas pedagógicas a cargo de los PRST, PCA, IT y la CRC.

Desde la experiencia de ScamZero, el mayor obstáculo no es que el usuario no quiera protegerse, sino que **no sabe qué hacer cuando recibe un mensaje que le genera duda**. Las campañas educativas de "no hagas clic en links sospechosos" son insuficientes si el usuario no tiene una herramienta concreta para determinar si un link es sospechoso antes de decidir. La estadística del propio documento lo confirma: el smishing multiplicó por nueve sus reclamaciones en un año, lo que indica que las estrategias educativas existentes no están siendo efectivas.

Observación: Las medidas pedagógicas del eje (c) deberían incluir expresamente la divulgación de herramientas de verificación disponibles en el mercado (links, mensajes, números) como parte del mensaje de prevención que los PRST y la CRC comunican a los usuarios. Esto es coherente con la

neutralidad tecnológica: no se promueve una solución específica, sino la existencia de una categoría de herramientas.

V. Aporte de datos y disposición de colaboración

ScamZero opera con datos reales de intentos de fraude detectados en Colombia. Contamos con patrones de mensajes fraudulentos, dominios de phishing activos y números reportados por usuarios que podrían aportar como insumo al CTLFSM, complementando los datos de los PRST desde la capa del usuario final —precisamente la fuente de datos que la regulación actual no contempla sistematizar.

Ponemos a disposición de la CRC esta información y expresamos disposición para participar en los espacios técnicos que el Comité establezca.

Cordialmente,

Miguel Andrés Palma Arcia
Fundador – ScamZero
info@scamzero.app | scamzero.app
C.C. 1.140.888.131