02-2716

Bogotá D.C, 4 de agosto de 2025

Doctora
Claudia Ximena Bustamante Osorio
Directora Ejecutiva
Comisión de Regulación de Comunicaciones
Ciudad

Asunto: Comentarios al documento de formulación del problema "IDENTIFICACIÓN DE MEDIDAS PARA MITIGAR EL FRAUDE CIBERNÉTICO POR MEDIO DE SERVICIOS MÓVILES"

Respetada Directora,

Inspirados en el bien común, en la democracia participativa, en la modernización del Estado y en la búsqueda del mayor desarrollo, inclusión y beneficio social para los colombianos, desde la Cámara de Industria Digital y Servicios de la ANDI trabajamos por mejorar la competitividad digital del país. Es así como atendiendo el interés de construir un país más productivo y sostenible, en concordancia con las dinámicas globales, nos permitimos manifestar a través de esta comunicación algunos comentarios con relación al documento en mención. Solicitamos respetuosamente nuestros comentarios sean tenidos en cuenta por la entidad.

1. Sobre el problema planteado:

Consideramos respetuosamente que el problema formulado por la CRC es correcto en su núcleo, pero aún resulta incompleto en la identificación de todos los elementos necesarios para comprender la magnitud del fenómeno y los actores involucrados.

a) Sobre si el problema definido en este documento involucra todos los elementos que evidencian las dificultades generadas por la comisión de fraude cibernético mediante la provisión de los servicios tradicionales de llamadas de voz y SMS, se considera importante plantear lo siguiente:

La formulación del problema parte de una lógica que se centra mayoritariamente en los agentes formalmente registrados ante la CRC (específicamente los operadores registrados en el Sistema de Información y Gestión de Recursos de Identificación (SIGRI) o en el Registro

de Proveedores de Contenidos y Aplicaciones, e Integradores (RPCAI)). Sin querer decir que estos agentes no sean los más importantes y respecto de los cuales se podrían tomar medidas concretas de una manera más eficiente, se cree que una de las principales complejidades del fraude cibernético es que en la asignación y monitoreo de los recursos, no se cuenta con fuentes de información que permitan contar con un sistema de conocimiento y acreditación de los Proveedores de contenidos y aplicaciones y/o integradores tecnológicos, en adelante PCA y/o IT, por una parte, y por la otra, que los ataques se originan desde algunos PCA y/o IT que justamente, no cumplen cabalmente las obligaciones regulatorias que corresponden para el uso adecuado de los recursos de identificación correspondiente.

Desde la experiencia de entidades financieras vigiladas por la Superintendencia Financiera de Colombia, el contacto a usuarios mediante llamadas y SMS son de las principales vías utilizadas por los delincuentes para ejecutar fraudes por ingeniería social, especialmente a través de *smishing* y *vishing*. Estas prácticas afectan la confianza del usuario de un sector altamente regulado pero vulnerable por el uso de esas vías, generan impactos reputacionales y operativos, y comprometen la seguridad del ecosistema financiero y de los mismos operadores. Estas prácticas encaminadas a ejecutar fraudes por ingeniería social, generan un impacto directo negativo en los PRSTM, PCA y/o IT, al no dotar con herramientas y responsabilidades a los usuarios de los servicios que les permita constatar la identidad del remitente del mensaje (PCA y/o IT), lo que conlleva a una exposición mayor a posibles fraudes utilizando la red del operador móvil y los riesgos referidos a todos los actores en la cadena de prestación del servicio.

La ausencia de herramientas regulatorias específicas que involucren a todos los actores de la cadena de valor para sancionar el uso indebido de los recursos de identificación, como los códigos cortos y la numeración E.164, ha limitado la capacidad de respuesta del sector financiero y de los operadores de servicios de telecomunicación móviles. Por ello, se considera fundamental que se permita la facultad de la terminación de los acuerdos de acceso entre los PRST y los PCA-IT, cuando se constate la reiteración de un uso indebido de la numeración, por envío de mensajes con contenido presuntamente fraudulento, de acuerdo con el procedimiento establecido en la Ley y regulación.

Y, es que más allá de lo anterior, la problemática no se reduce solo a esto, si no a que los usuarios de los servicios no conocen y no tienen por qué hacerlo, las diferencias de los recursos de identificación, ni la veracidad o legitimidad de éstos. Así, los delincuentes suplantan todo tipo de entidades legítimas utilizando numeración falsa, envío de mensajes SMS con identificadores alterados, y llamadas desde centrales automáticas que imitan el lenguaje institucional, sin que el usuario final tenga cómo saber que la identificación de quien cursa el mensaje es fraudulenta.

Así pues, en la práctica, no existe para los consumidores una forma clara y segura de verificar si una llamada o mensaje recibido proviene efectivamente de su entidad financiera o de un actor fraudulento. Esto, más allá de que las entidades financieras y otros actores implementen campañas de educación financiera y de prevención del fraude.

Por otro lado, se considera muy valioso que el documento reconozca que existe un crecimiento sostenido del fenómeno:

"es importante tener en cuenta que, si bien el tráfico de los servicios de mensajería y voz móvil 3G, así como del servicio de telefonía fija, han mostrado una tendencia decreciente en los últimos años, las afectaciones a los usuarios derivadas de acciones irregulares con fines de fraude presentan un crecimiento sostenido, incluso exponencial en algunos casos."

Este diagnóstico, reafirma la necesidad de una nueva aproximación regulatoria al problema, ágil y fácil de expedir, pero que no subestime las tecnologías por su antigüedad o decrecimiento en volumen de tráfico, sino que reconozca su papel como puntos de entrada al fraude.

Así las cosas, esta problemática enfatiza si se corta de raíz el medio bajo el cual los PCA o IT envían estos mensajes con contenido fraudulento.

Es decir, si la CRC de manera ágil autoriza la finalización de las relaciones o contratos de acceso entre PCA y/o IT y PRST al constatar reincidencia en recuperación de códigos cortos por indebido uso de la numeración al enviar mensajes con contenido fraudulento, y si el proceso de recuperación de numeración se realiza de manera expedita sin demoras innecesarias, los usuarios no recibirían este tipo de mensajes.

b) Sobre si las causas presentadas en este documento son las que generan el problema definido:

Si bien las causas identificadas por la CRC son pertinentes y reflejan aspectos clave del problema, se puede observar lo siguiente:

i. Las medidas técnicas y regulatorias sobre administración de recursos de identificación se han enfocado en el uso eficiente de un recurso escaso

Se coincide con la CRC en que el enfoque de la regulación de los recursos de identificación se ha orientado principalmente hacia su uso eficiente, en tanto se trata de un recurso escaso. No obstante, sin querer desconocer la labor de la Comisión, se considera que las medidas tomadas hasta el momento han permitido que no existan hoy en día mecanismos regulatorios robustos para distinguir entre comunicaciones legítimas y suplantadas, ni obligaciones claras para que los operadores verifiquen o monitoreen el uso adecuado de los números asignados.

Así las cosas, i) el marco actual no disuade suficientemente a los PCA/IT reincidentes en malas prácticas, ii) no se impone una consecuencia directa y contundente sobre la relación de acceso entre el infractor y los operadores de red, iii) la reincidencia no tiene consecuencias claras, iv) No se generan los incentivos adecuados: el costo de reincidir puede ser menor al beneficio económico obtenido por facilitar fraude, v) Mientras persista la posibilidad de seguir operando tras múltiples recuperaciones de numeración, el incentivo al cumplimiento regulatorio es débil, vi) La reincidencia sistemática en el uso indebido de códigos cortos demuestra una fallida gestión interna de seguridad por parte del PCA o IT. vii) Las prácticas fraudulentas no solo afectan a usuarios, sino que también debilitan la integridad del ecosistema de telecomunicaciones y de las instituciones suplantadas al erosionar la confianza en los canales tradicionales como el SMS y la voz. Finalmente, la repetida intervención del regulador para recuperar numeración demuestra un patrón, no una falla aislada.

Un punto clave identificado es la falta de una taxonomía unificada en torno a este tipo de fraudes, lo cual pone en evidencia la falta de coordinación interinstitucional para regular esta materia.

Se debe incluir i) la falta de consecuencias estructurales frente a la reincidencia, ii) el vacío regulatorio y la inhabilitación de los PRSTM para implementación de medidas de control, permiten la propagación y crecimiento exponencial de los fraudes de voz y SMS, iii) imposibilidad de terminar relación de acceso con PCA o IT reincidente en el envío de SMS con contenido fraudulento iv) Participación activa por parte del MinTIC.

ii. Las medidas de gestión y control implementadas por los PRST y asignatarios son insuficientes

Se considera problemático que el documento establezca como una de las causas del problema la supuesta insuficiencia de las medidas adoptadas por los PRST y asignatarios de recursos de identificación, sin considerar de forma suficiente las limitaciones regulatorias, técnicas y operativas a las que se enfrentan los agentes para actuar de forma eficaz y oportuna frente a los eventos de fraude.

En primer lugar, debe decirse que no es posible exigir prevención sin que exista habilitación normativa ni capacidad operativa para esos efectos. Los operadores no cuentan ni con las competencias legales, ni con una instancia de coordinación institucional adecuada para bloquear, filtrar o prevenir proactivamente conductas fraudulentas que se cursan a través de sus redes y que se ejecutan en cuestión de segundos.

Adicionalmente, cuando los efectos del fraude se producen de forma tan rápida (como en los casos de *smishing* o llamadas falsas que inducen a transferencias bancarias) cualquier acción que se adopte una vez iniciado el evento es, naturalmente, tardía. Las medidas

reactivas no son una falla de diseño, sino el único recurso disponible frente a una amenaza ya ejecutada. Este escenario es estructural y no depende solo de la voluntad de los agentes.

Así pues, se considera que lo urgente es reconocer que el marco regulatorio y operativo actual no permite tomar medidas más eficientes y efectivas. De esa forma, la CRC podría tener en cuenta las siguientes recomendaciones de cara a avanzar hacia un ecosistema más preventivo que reactivo:

A) Facultar de forma expresa a los PRST y asignatarios de recursos de numeración para bloquear tráfico o numeración sospechosa de forma preventiva, sin que ello implique riesgos regulatorios por afectación de servicios legítimos.

B) Permitir la suspensión provisional o la terminación definitiva de la relación de acceso por indebido uso de numeración. Así las cosas, ei el PCA o IT no puede enviar mensajes con contenido fraudulento, se da fin a la controversia, y se soluciona de raíz la problemática planteada.

iii. Desconocimiento de los usuarios sobre privacidad de la información que facilita la obtención de datos personales con fines fraudulentos

Se considera que, si bien este factor puede tener incidencia en la problemática planteada, la CRC enfatiza más de lo debido en ella.

Sea lo primero señalar que los ataques de ingeniería social se definen como aquellas prácticas mediante la cual se obtiene información confidencial a través de manipulación de usuarios legítimos[1]. Esa manipulación proviene de los atacantes al explotar características humanas como la confianza básica en los demás, el deseo de brindar asistencia o la propensión a lucirse y se caracteriza precisamente por adaptarse de manera sofisticada a los comportamientos del usuario, incluso cuando estos puedan tener un conocimiento razonable sobre buenas prácticas de seguridad digital.

Actualmente, según la Cartilla metodológica de Atención de Delitos Informáticos de la Fiscalía General de la Nación, hay un aumento en denuncias ciudadanas por la afectación a la información y a los datos, como consecuencia del necesario aumento en el uso de las tecnologías de la información y las comunicaciones en la vida cotidiana. Adicionalmente, la Corporación Excelencia en la Justicia expone un indicador que mide el número de delitos informáticos registrados por el Ministerio de Defensa Nacional, donde destaca un crecimiento significativo de esta tipología de delitos desde 2020[2] a nivel nacional.

[1] Fiscalía General de la Nación. Cartilla Metodológica de Atención de Delitos Informáticos.
[2] Corporación Excelencia en la Justicia. Delitos Informáticos en Colombia. Disponible en: https://cej.org.co/indicadores-de-justicia/criminalidad/delitos-informaticos-colombia/

El énfasis en la responsabilidad individual del usuario en la protección de su información personal omite reconocer un conjunto de variables estructurales que están directamente asociadas al *modus operandi* de los criminales en la ingeniería social.

El crecimiento sostenido de los delitos cibernéticos a partir del año 2020 evidencia que la sola existencia de normas como la Ley 1266 de 2008 y la Ley 1581 de 2012 no ha sido suficiente para contener la evolución del fenómeno delictivo. En otras palabras, el incremento reciente en la comisión de estos delitos demuestra que no se trata de una problemática permanente o estructural asociada únicamente al desconocimiento normativo por parte de los usuarios, sino de una amenaza dinámica, que ha escalado en sofisticación y volumen en un entorno digital cada vez más complejo y vulnerable.

Según la Cámara Colombiana de Informática y Telecomunicaciones, el porcentaje de incremento de ciberdelitos viene creciendo de manera significativa y el comportamiento de estabilidad al alza tuvo un punto de inflexión en 2019, atribuible a un escenario en el que confluyen, entre otros, factores como: (i) la incidencia del factor geopolítico en el contexto global. Los grupos de amenazas como APT C36 han sido más activos en los últimos años en Colombia; (ii) el incremento en el número de servicios de comercio electrónico y servicios de banca digital. El sector Fintech en Latinoamérica indica que las Billeteras Virtuales vienen creciendo un 27% cada año, tendencia que será duplicada para el 2025; todo lo anterior aumenta el nivel de exposición y apetito de los ciber atacantes; y (iii) desactualización de los sistemas y del recurso humano por fuga de talentos de Ciberseguridad. Alta rotación y poca claridad en la designación de responsables en la estructura organizacional[3].

Adicionalmente la rápida digitalización de los diferentes ecosistemas que usan las personas y particularmente del sector financiero ha ampliado de forma significativa la superficie de ataque a la que están expuestas las personas y las entidades financieras. Esto ha permitido que los actores criminales desarrollen y apliquen con mayor frecuencia y sofisticación campañas de *phishing*, ataques a la cadena de suministro, técnicas avanzadas de ingeniería social, *ransomware* y otros mecanismos de acceso ilegítimo a la información[4].

A su vez, aunque la SFC ha emitido lineamientos relevantes en materia de ciberseguridad—como la Circular Externa 007 de 2018 y la Circular Externa 033 de 2020 que establece criterios mínimos para la gestión de riesgos–, el crecimiento sostenido de los delitos cibernéticos evidencia que las medidas no han tenido un impacto significativo ni disuasorio frente a estas amenazas en evolución.

[3] Cámara Colombiana de Informática y Telecomunicaciones 2023. IA para la protección y prevención de amenazas. Informe Anual de Ciberseguridad.
[4] Cámara Colombiana de Informática y Telecomunicaciones 2024. Ciberseguridad en el sistema financiero colombiano: entre la amenaza y la resiliencia.

Así, se considera que el problema definido enfatiza sobre una causa que, aunque es relevante, no evidencia de manera directa que la socialización y concientización de los usuarios sobre los riesgos asociados a fraudes digitales contrarresten los escenarios de ataques cibernéticos, toda vez que, como fue argumentado, la ingeniería social tiene muchas variantes en las que, por más que el usuario conozca sobre derechos y definiciones los riesgos digitales, puede caer, de manera totalmente informada en escenarios de ciberataques.

c) En cuanto a las consecuencias expuestas en el presente documento

Se considera que son coherentes con lo que se ha observado. En el caso del sector financiero, las entidades prestadoras de servicios han tenido que asumir altos costos crecientes en razón a compensaciones, atención a incidentes y campañas educativas. A su vez, los PRST, han hecho lo propio para tratar de identificar los mensajes con contenido presuntamente fraudulento que se dirige por parte de los PCA y/o IT a sus usuarios.

Lo anterior sumado a un régimen de responsabilidad desarticulado y desbalanceado, y a la obligatoriedad que experimentan los PRSTM de mantener vigentes sus relaciones de acceso con PCA e IT, que hacen evidente que remiten mensajes con contenido fraudulento, genera además, la pérdida de confianza de los usuarios ha generado una mayor resistencia al uso de canales digitales, lo que afecta no solo los desarrollos y las experiencias, sino la misma inclusión financiera y la eficiencia operativa. Es claro además que este no es un problema exclusivo de Colombia o incluso de la región, sino que es un desafío global.

2. Respecto de los grupos de valor

a) Se sugiere incluir como grupo de valor no solo a las entidades financieras sino también a las Fintech, dado que son actores altamente expuestos al fraude cibernético mediante servicios móviles. Para éstas, los canales de contacto con clientes (SMS, llamadas, notificaciones, entre otros) son esenciales para la operación, y cualquier afectación en su seguridad impacta directamente la relación con el cliente y la estabilidad del sistema financiero.

Adicionalmente, se sugiere incluir dentro de los grupos de valor identificados a actores clave como lo son el Ministerio de Tecnologías de la información y las Comunicaciones, la Fiscalía General de la Nación, la SFC, la Superintendencia de Economía Solidaria y el Ministerio de Hacienda y Crédito Público, entre otros, a fin de lograr una coordinación interinstitucional alineada y coordinada, que someta a sus vigilados a reglas homogéneas y de aplicación igualitaria a las empresas de telecomunicaciones y, de esa forma abordar de manera integral la problemática.

3. Sobre las posibles alternativas de solución:

Las medidas que se relacionan a continuación deben implementarse en un contexto de trabajo mancomunado entre los distintos actores que hacen parte de la cadena de valor:

a) En relación con el uso indebido de la numeración de códigos cortos

i. Un registro de remitentes con códigos alfanuméricos y campañas identificadas son medidas altamente positivas ya que facilitarían la identificación de emisores legítimos y permitiría a los usuarios reconocer con mayor claridad las comunicaciones oficiales, reduciendo el riesgo de suplantación. Esta medida sería especialmente útil para proteger marcas reconocidas que son blanco frecuente de fraude, como las entidades financieras. No obstante, el principal desafío será la adopción de tecnología avanzada y de fácil implementación, para garantizar la interoperabilidad entre operadores y la gestión del registro en tiempo real, asegurando que los datos estén actualizados y que exista validación efectiva de identidad para cada remitente. Otro desafío es garantizar dentro de la cadena de actores la seguridad y privacidad de la información, teniendo en consideración la información que se está manejando y cómo la misma va a ser protegida, así como la trazabilidad de la responsabilidad de quien la debilita o vulnera.

ii. La creación de un registro unificado que incluya tanto códigos cortos como numeración E.164 no geográfica (como el NDC 940) es una medida viable y deseable. Esta integración permitiría una trazabilidad más robusta de las campañas de mensajería y una gestión más eficiente de los recursos de identificación, facilitando la detección de usos indebidos. El principal reto estaría en que los usuarios comprendan la diferencia entre los tipos de numeración, evitando confusiones que puedan ser aprovechadas por actores maliciosos.

iii. La exclusividad de uso por código corto es una medida efectiva para evitar la suplantación. Sin embargo, podría generar escasez de numeración por lo cual se recomienda evaluar la ampliación del rango disponible o permitir la migración a numeración E.164 no geográfica, con reglas claras de uso exclusivo por entidad. La asignación de códigos debe realizarse acorde con las validaciones previas sobre la legitimidad de la actividad económica de las empresas en los registros oficiales y que se encuentren debidamente acreditadas. La reventa de códigos no debería ser considerada debido a que generaría desconfianza y se podría constituir eventos de fraude.

b) Respecto del uso inadecuado de la numeración E.164:

i. El registro de originadores de llamadas comerciales es altamente recomendable. Esto permitirá a los usuarios identificar llamadas legítimas y facilitará el bloqueo de llamadas fraudulentas. Se ha identificado múltiples casos de suplantación de numeración en llamadas de *vishing* y *spoofing*.

Las técnicas tecnológicas de filtrado (*screening*) para identificar y bloquear llamadas o mensajes sospechosos resultan positivas, pero deben ser complementadas con una regulación sobre el uso de numeración. Permite hacer un filtro de los mensajes y llamadas que posiblemente, estén siendo utilizados para cometer algún tipo de fraude, adoptando herramientas tecnológicas de Inteligencia Artificial o *machine learning*, con el fin de robustecer el sistema y permitir una identificación efectiva, para garantizar la información a los usuarios y generar mayor confianza en las operaciones de telecomunicaciones.

En particular, se sugiere establecer rangos dedicados para llamadas comerciales legítimas, con validación previa del originador. De igual forma garantizar el cumplimiento de los principios rectores de la ley 1581 de 2012.

c) En relación con el desconocimiento de los usuarios sobre la privacidad de la información y las técnicas de ingeniería social:

i. Aunque se reconoce que la socialización tiene un impacto positivo para mitigar en alguna medida los casos de ataques cibernéticos, las medidas de divulgación pedagógica no atacan realmente el problema de raíz. Teniendo en cuenta lo que se ha dicho, la ingeniería social usa métodos de manipulación psicológica, por más que un usuario conozca todo el material teórico sobre los riesgos, al momento práctico, el criminal ejerce una serie de conductas encaminadas a manipular la decisión cognitiva del usuario, en la que, este último podría conocer todas las normas aplicables y aun así caer en un escenario de fraude porque la fuente de información—suplantación de una entidad financiera legítima—supo reconocer sus patrones legítimos de conducta y envío un mensaje que a todas luces, parecía de un remitente legítimo. Entidades del sistema financiero han venido desarrollado campañas educativas multicanal en torno al fraude, pero esto no ha mitigado el problema de su comisión ni los efectos negativos que esto conlleva, sobre todo cuando en el proceso se involucran suplantaciones de terceros que llevan al consumidor a un entorno de confianza (como sucede con la compra del seguro SOAT a través de páginas o SMS fraudulentas, que terminan llevando a la persona a hacer un pago que no corresponde).

ii. La creación de un sistema intersectorial de trazabilidad administrado por la CRC sería una medida positiva y necesaria, en tanto permitiría centralizar la información sobre recursos de identificación utilizados con fines presuntamente fraudulentos y facilitaría la articulación entre sectores. Esto permite una respuesta más rápida y coordinada ante incidentes y facilita la identificación de patrones de fraude. Además, permite tener información con mayor detalle, que puede ser un recurso valioso para que las autoridades competentes, realicen investigaciones objetivas que deriven en penas para quienes cometan hechos delictivos. Debe considerarse, los canales por los cuales se deben escalar dichas peticiones, tiempos de respuesta y los recursos que deben ser usados para atender de forma oportuna.

Sin embargo, su valor radica en su capacidad operativa y preventiva, no únicamente en su complementariedad con campañas educativas, las cuales, si bien importantes, no deben ser el componente principal de la estrategia regulatoria. Finalmente, se reitera que, aunque se reconoce la relevancia de socializar con los usuarios los riesgos de fraude cibernético, se reitera que este no puede ser el eje central en el proyecto regulatorio, toda vez, que como ha sido analizado en las preguntas anteriores, los mecanismos de control son los que no han resultado suficientes para resolver los escenarios de delitos cibernéticos, razón por la cual se manifiesta que el enfoque más allá de instruir sobre la materia, debería enfocarse hacia los medios de control aplicables para evitar los delitos cibernéticos.

Adicionalmente, es importante destacar que la adopción de estas herramientas debe estar alineada con la normatividad vigente en materia de protección de datos personales, tales como la Ley 1581 de 2012 y demás regulaciones complementarias, para garantizar el debido respeto a los derechos de los usuarios sobre su información.

En este contexto, se sugiere que la CRC permita la posibilidad de terminar las relaciones de acceso entre PRSTM y PCA-IT que remitan de manera reiterada SMS con contenidos fraudulentos.

Por último, se sugiere que el gobierno fomente, promueva y, en la medida de lo posible, subsidie iniciativas tanto del sector público como del privado orientadas a la reducción masiva del riesgo cibernético desde la raíz, representada por los prestadores de servicios, quienes constituyen los actores más transversales en la problemática.

d) Sobre la revisión integral del Régimen de Recursos de Identificación:

i. Ausencia de articulación efectiva de la estrategia nacional para prevenir el fraude mediante llamadas y mensajes de texto

Se coincide con la CRC en que la falta de articulación interinstitucional efectiva es una de las causas estructurales del problema y, en efecto, es un componente relevante para avanzar hacia una estrategia coordinada, efectiva y transversal frente al fraude cibernético. Así las cosas, si se implementan medidas que permitan la terminación de relación existentes entre PCA o IT cuando se comprueba reincidencia en el envío de mensajes con contenido presuntamente fraudulento.

Por otra parte, se recomienda:

A) Automatizar los procesos de asignación y recuperación de recursos de identificación mediante plataformas interoperables.

B) Establecer criterios de “uso seguro” de dichos recursos de identificación además del uso eficiente.

C) Incluir cláusulas de revocación inmediata ante evidencia de uso fraudulento.

D) Permitir auditorías cruzadas entre operadores, CRC y entidades afectadas.

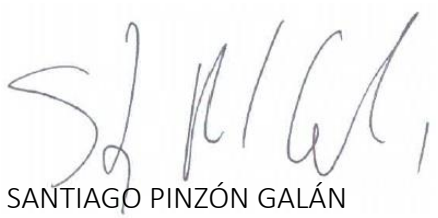
E) Analizar la imposición de medidas regulatorias dirigidos a PCA a IT, con un especial énfasis en aquellos que enrutan tráfico cuyo contenido resulta potencialmente fraudulento.

F) Introducir nuevas herramientas que les permitan a los PRST, ante evidencias de fraude, bloquear el tráfico proveniente de los PCA e IT.

Esperamos contribuir con nuestros comentarios a esta iniciativa.

Agradecemos su atención.

Cordialmente,



SANTIAGO PINZÓN GALÁN
Director Ejecutivo de la Cámara de Industria Digital y Servicios
ANDI