02-3127

Bogotá D.C, 23 de junio de 2026

Doctor
FELIPE AUGUSTO DÍAZ SUAZA
Director Ejecutivo
Comisión de Regulación de Comunicaciones
Ciudad

Asunto: Comentarios al Proyecto de Resolución "Por la cual se establecen medidas para mitigar el fraude cibernético por medio de servicios móviles y se dictan otras disposiciones".

Respetado Director,

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 proyecto de Resolución en mención. Solicitamos respetuosamente nuestros comentarios sean tenidos en cuenta por la entidad.

I. Comentarios Generales

El Proyecto de Resolución tiene como finalidad combatir el fraude cibernético, proteger a los usuarios frente a la suplantación, el phishing y el smishing, y preservar la confianza en el ecosistema digital. Desde esta perspectiva, se coincide con dicho propósito y se reconoce la necesidad de implementar las medidas necesarias e idóneas para salvaguardar la seguridad y el bienestar de los usuarios.

Pese a lo anterior, se considera necesario advertir que el Proyecto de Resolución podría producir efectos contrarios a la finalidad que persigue. En particular, la iniciativa resulta preocupante en la medida en que: (i) impone cargas que podrían resultar desproporcionadas frente a alternativas menos restrictivas e igualmente eficaces, comprometiendo la neutralidad tecnológica, la continuidad de servicios críticos y la seguridad digital de los

usuarios; y (ii) algunas propuestas incluidas en el Proyecto pueden conllevar a tensiones con la libertad de empresa y la libre competencia.

a. Efecto negativo sobre la seguridad digital

El Proyecto establece obligaciones sobre quienes generan mensajes de autenticación (OTP), segundo factor (2FA), verificación de identidad, alertas de seguridad y comunicaciones transaccionales. Estas comunicaciones son, en muchos casos, parte intrínseca de servicios digitales prestados por actores distintos a los proveedores de redes y servicios de telecomunicaciones, e incluso de desde fuera del país.

Frente a lo anterior, resulta pertinente indicar que la autenticación multifactor mediante OTP y 2FA es una de las medidas de seguridad más utilizadas para mitigar la apropiación de cuentas, la suplantación y el fraude en internet. El Proyecto somete estos mensajes al mismo aparato de plantillas obligatorias, aprobación previa, validación anual y eventual bloqueo aplicable a otras modalidades de mensajería A2P. Aunque el Proyecto reconoce que los mensajes de autenticación y seguridad tienen una naturaleza especial y no requieren consentimiento adicional, dicha diferenciación pierde eficacia si, en la práctica, estos mensajes quedan sujetos al mismo esquema de validación previa y bloqueo operativo que las comunicaciones comerciales o publicitarias.

En este sentido, el Proyecto de Resolución desconoce que cada uno de esos pasos introduce latencia, costos y puntos de falla en una cadena que debe ser instantánea y de altísima disponibilidad, especialmente teniendo en cuenta que su finalidad es proteger las cuentas de los usuarios.

Si un OTP no se entrega por falta de plantilla vigente, por una desactivación, por una caída del validador o por un bloqueo del PRST, el usuario no podrá iniciar sesión, recuperar su cuenta ni autenticar el uso de su cuenta. El efecto previsible podría ser no menos fraude, sino más exposición a usuarios bloqueados, migración a factores menos seguros y mayor superficie para el fraude de cuentas. Una medida concebida para mitigar el fraude no debe perjudicar la herramienta que más lo previene y afectar desproporcionadamente medidas de seguridad reconocidas como eficaces internacionalmente.

En ese sentido, es esencial distinguir con precisión entre (i) las comunicaciones legítimas de autenticación y seguridad, solicitadas por el propio usuario o derivadas de un servicio contratado, y (ii) las prácticas fraudulentas de phishing, smishing, suplantación de marca, ingeniería social, malware, SIM swapping, granjas de SIM. El OTP y el 2FA son mecanismos reconocidos de respuesta al fraude, no su causa. Por lo tanto, imponerles barreras podría generar riesgos de seguridad adicionales para el ecosistema digital.

Adicionalmente, se considera necesario que el Proyecto incorpore un tratamiento diferenciado para las comunicaciones críticas asociadas a servicios financieros,

especialmente aquellas utilizadas para autenticación reforzada, códigos OTP, alertas transaccionales, confirmación de identidad, bloqueo preventivo de productos y notificaciones de seguridad. Estas comunicaciones cumplen una función distinta a la mensajería comercial o publicitaria, pues hacen parte de la arquitectura de prevención del fraude y permiten reaccionar oportunamente frente a operaciones sospechosas, apropiación de cuentas o intentos de suplantación.

Por ello, no deberían quedar sometidas, sin distinción, a reglas que puedan introducir latencia, indisponibilidad, bloqueos automáticos o etiquetados negativos que afecten su entrega oportuna.

II. Comentarios específicos

1. Preocupación frente a las medidas impuestas relacionadas con el SENDER ID

El artículo 1 del Proyecto de Resolución define el SENDER ID como un recurso de identificación administrado por la CRC que identifica al responsable del contenido enviado por SMS y USSD. Por su parte, el Capítulo 12 (artículos 6.12.1.1 y siguientes) regula su asignación, condicionando la tenencia de SENDER ID a la posibilidad de cursar tráfico A2P.

Resulta preocupante que la figura del SENDER ID se utilice como mecanismo para imponer un régimen de habilitación previa a los generadores de contenido, condicionando la posibilidad misma de comunicación con usuarios. Aunque la CRC administra legítimamente ciertos recursos de identificación, esa competencia debe ejercerse dentro de los límites propios de la administración técnica, eficiente y segura de tales recursos, sin convertirlos en un instrumento de autorización previa de actividades económicas o de comunicaciones legítimas.

Ahora bien, se reconoce la importancia del SENDER ID como herramienta para identificar con mayor claridad al originador de comunicaciones A2P, reducir la suplantación y mejorar la confianza del usuario. Sin embargo, convertirlo en requisito administrativo previo, con asignación única por entidad, exigencias de validación, causales de recuperación y dependencia del validador centralizado, puede transformarlo en una barrera de acceso y permanencia en el mercado.

Un régimen de asignación previa, con tiempos administrativos y causales de recuperación, resulta incompatible con la velocidad operativa de los servicios digitales y con la incorporación ágil de nuevos remitentes legítimos. La consecuencia práctica es la imposición de barreras de entrada para startups, comercios digitales y desarrolladores, y de demoras para proveedores de mayor escala, con el riesgo de que servicios de seguridad no puedan operar en Colombia.

1.1. Establecimiento de una sucursal en Colombia

De otro lado, el Parágrafo 2 del artículo 6.12.1.2 dispone que "*a cada persona natural o jurídica le será asignado un único SENDER ID*"; solo se asignará "*un SENDER ID por NIT o por cédula*"; y los solicitantes extranjeros podrán ser asignatarios ***"siempre que hayan establecido una sucursal en Colombia"***. La exigencia de sucursal se reitera en el numeral 6.12.2.1.1 del Proyecto de Resolución.

La exigencia de establecer una sucursal en el país como condición para enviar mensajes de autenticación y seguridad a usuarios en Colombia resulta desproporcionada y potencialmente discriminatoria frente a los proveedores extranjeros. Obligar a una presencia local permanente para el ejercicio de una función puramente técnica de identificación no es una medida proporcional y, de hecho, impone una carga estructural gravosa que no guarda relación de necesidad ni con el fin de identificar al remitente.

Adicionalmente, esta obligación puede generar tensiones con los compromisos internacionales asumidos por Colombia en materia de comercio transfronterizo de servicios. En particular, el TLC con Estados Unidos contempla disciplinas orientadas a evitar que la prestación transfronteriza de servicios sea condicionada a la obligación de establecer presencia local en el territorio de la otra parte. Por ello, una medida que exige a proveedores extranjeros constituir una sucursal en Colombia como condición para acceder al SENDER ID y cursar mensajes A2P podría ser incompatible con dichos compromisos.

Finalmente, la exigencia de una sucursal obligatoria puede desincentivar la prestación de servicios de seguridad desde el exterior y podría impedir o desincentivar que ciertos proveedores globales mantengan el SMS como canal de autenticación en Colombia, llevando a los usuarios a alternativas menos seguras o reduciendo la disponibilidad de mecanismos de autenticación robusta en el país. Ello afectaría la seguridad del ecosistema digital, que el propio Proyecto pretende proteger.

1.2. Mensajes de autenticación y seguridad (Artículos 6.12.1.3.1, 6.13.4.1 y 6.13.4.7.2)

El artículo 6.12.1.3.1 establece que los mensajes de autenticación y seguridad (OTP, alertas de inicio de sesión, confirmaciones) se generan a solicitud del usuario y no requieren consentimiento adicional. No obstante, los artículos 6.13.4.1 y 6.13.4.7.2 exigen que todo mensaje A2P (incluida la autenticación) cuente con plantilla aprobada y vigente, y disponen que en su ausencia el PRST podrá bloquear el mensaje o marcarlo como "sin verificar".

Al respecto, se considera que el Proyecto incurre en una contradicción pues en principio reconoce la naturaleza especial de los mensajes de autenticación y luego los somete al mismo control previo de contenido y a la misma posibilidad de bloqueo que la mensajería comercial o publicitaria. Estos mensajes son generados a solicitud activa del propio usuario

en un momento específico, lo que descarta que se trate de comunicaciones imprevistas o no deseadas que por sí solas puedan generar casos de fraude.

Las características técnicas de estos mensajes hacen de difícil cumplimiento algunas de las medidas propuestas por la CRC. Los OTP contienen variables dinámicas, son sensibles al tiempo y se cursan en volúmenes elevados con exigencias de disponibilidad casi absoluta. Aunque el Proyecto no necesariamente exige aprobar el valor exacto de cada OTP, sí somete la plantilla, el contenido estático, el sentido del contenido dinámico y el enrutamiento del mensaje a un esquema de validación previa y consulta operativa que puede generar falsos bloqueos, latencia o indisponibilidad.

La aprobación previa, la vigencia mensual de la plantilla (incluso si es de renovación automática) y la consulta en tiempo real al validador antes de enrutar cada mensaje añaden latencia y barreras para su adecuado funcionamiento. De hecho, cualquier interrupción en la entrega de un OTP impide, por ejemplo, el inicio de sesión o la recuperación de cuenta. Entonces, el costo de un falso bloqueo de un mensaje de seguridad es muy superior al de un mensaje comercial no entregado. El efecto de la propuesta sería desconocer la importancia de la herramienta que mejor protege a los usuarios, en contra del propio objetivo del Proyecto de Resolución.

2. Validador centralizado (Artículos 6.13.1.1 a 6.13.1.6 y 18)

Los artículos 6.13.1.1 a 6.13.1.6 y 18 crean un validador centralizado, entendido como una persona jurídica única seleccionada por los PRST móviles y financiada por los asignatarios de código corto A2P, encargado de la verificación del KYC, de la aprobación de plantillas y de la emisión de certificaciones, sin cuyo aval no es posible acceder a los recursos ni cursar tráfico.

Esta configuración impone una arquitectura compleja que puede entorpecer la operación técnica y generar distorsiones en el mercado, al superponer un intermediario obligatorio en la cadena de valor de la mensajería A2P. Resulta especialmente preocupante que el Proyecto concentre en un actor privado único funciones que condicionan el acceso al mercado, la asignación de recursos y el flujo de comunicaciones.

La delegación en un particular de funciones que condicionan el ejercicio de una actividad económica y el flujo de comunicaciones exige una base legal clara. La ausencia de una habilitación legal expresa sobre el validador central plantea problemas de legalidad y proporcionalidad. Además, aunque el Proyecto prevé supervisión por parte de la CRC o del Administrador de Recursos de Identificación, no establece salvaguardas suficientes de debido proceso, auditoría, responsabilidad, transparencia, no discriminación y mecanismos de revisión frente a decisiones del validador.

Adicionalmente, el proyecto debería precisar con mayor claridad la gobernanza de los registros, bases de datos, listas y mecanismos de clasificación utilizados para validar,

bloquear, etiquetar o restringir comunicaciones. En particular, debería definirse quién administra, actualiza y supervisa dichos registros; cuáles son los criterios técnicos y probatorios para incluir, excluir, suspender o reclasificar un originador, SENDER ID, código corto o plantilla; y cuáles son los plazos máximos para resolver solicitudes de revisión o corrección.

Estas precisiones son indispensables para evitar decisiones arbitrarias, reducir falsos positivos y garantizar que los actores afectados cuenten con mecanismos efectivos de contradicción y debido proceso.

Por otra parte, la creación de un validador único introduce riesgos sistémicos y de eficiencia para el ecosistema. En primer lugar, un validador único constituye un punto de falla que podría afectar masivamente la entrega de mensajes críticos, salvo que se incorporen mecanismos robustos de contingencia, validación diferida o reglas de continuidad para comunicaciones de seguridad. En segundo lugar, al carecer de presión competitiva, este modelo puede desincentivar la innovación tecnológica en soluciones de validación. Por último, el esquema traslada el costo financiero de esta infraestructura a los asignatarios de código corto A2P, obligándolos a financiar un actor privado cuya gobernanza y estructura deben estar sometidas a controles estrictos.

3. Plantillas de contenido obligatorias, aprobación previa y vigencia mensual (Artículos 6.13.4.1 a 6.13.4.3)

Los artículos 6.13.4.1 a 6.13.4.3, junto con la definición de Plantilla de contenido A2P, disponen que ningún mensaje A2P puede cursarse sin una plantilla aprobada y vigente; que el validador revisa el contenido estático y el sentido del contenido dinámico; que las plantillas tienen vigencia mensual renovable; y que la aprobación o el rechazo se resuelven en plazos de 24 a 48 horas.

El Proyecto instaura un mecanismo de aprobación previa de plantillas como condición para cursar comunicaciones A2P. Este esquema debe analizarse con especial cuidado, pues puede operar como un control previo sobre comunicaciones legítimas y generar restricciones desproporcionadas a la libertad de empresa, la libre competencia y la continuidad de servicios digitales.

Aunque la renovación sea automática, mantener una vigencia mensual y causales amplias de desactivación introduce incertidumbre operativa para servicios críticos. En particular, si la plantilla puede ser suspendida, rechazada o desactivada por criterios amplios o poco determinados, como los establece el Proyecto de Resolución, los remitentes legítimos enfrentan un riesgo operativo permanente que puede afectar comunicaciones de seguridad, autenticación, alertas de fraude o mensajes transaccionales necesarios para la prestación de servicios digitales.

Además, los servicios digitales modifican textos, idiomas, variables y enlaces de manera continua y a gran escala. Exigir una plantilla aprobada por mensaje o campaña, con vigencia mensual y revisión del contenido dinámico, es incompatible con flujos automatizados y con la personalización legítima. En el caso de los OTP, el contenido dinámico es, por diseño, impredecible. El esquema introduce latencia, costos y fragilidad operativa, y traslada al validador decisiones que afectan la entrega de mensajes legítimos, con un incentivo estructural a la sobre-restricción para evitar responsabilidad.

4. Bloqueo o etiquetado de mensajes sin plantilla por el PRST (Artículo 6.13.4.7.2)

El artículo 6.13.4.7.2 obliga al PRST a verificar, antes de enrutar cada mensaje A2P, la existencia de código corto A2P, SENDER ID y plantilla vigente en el sistema validador, y dispone que, en ausencia de alguno de estos elementos, el PRST deberá bloquear el mensaje impidiendo su entrega al usuario final o, alternativamente, a su elección, marcarlo con la etiqueta de no verificado.

Al respecto, condicionar el enrutamiento de cada comunicación a una consulta de verificación genera una dependencia operativa y añade una latencia inadmisible a la red. Bajo esta arquitectura, cualquier retraso técnico en la consulta o un falso negativo en el sistema central se traducirá en el bloqueo automático de interacciones críticas que requieren inmediatez, tales como las alertas de fraude o los códigos de autenticación, lo cual perjudicará gravemente a los usuarios y a los remitentes globales.

Además, la alternativa de marcar un mensaje de seguridad legítimo con la etiqueta de “sin verificar” resulta ser una medida equívoca y contraproducente. En lugar de alertar eficazmente, esta señalización induce a error al usuario y mina su confianza en las comunicaciones que son, precisamente, las que buscan proteger su identidad y su patrimonio. El costo económico y reputacional de un falso bloqueo o de una mala catalogación sobre una comunicación crítica es desproporcionadamente elevado y asimétrico frente al beneficio marginal que el Proyecto pretende obtener mediante una exigencia procedimental.

Asimismo, debe considerarse que el etiquetado erróneo de comunicaciones legítimas como “sin verificar” puede generar un efecto adverso sobre la confianza del usuario en los canales oficiales. En particular, si un mensaje de autenticación, una alerta de seguridad o una comunicación transaccional legítima aparece asociada a una advertencia de falta de verificación, el usuario puede ser inducido a desconfiar de los canales formales y a acudir a canales alternativos menos seguros.

Este escenario podría ser aprovechado por defraudadores mediante esquemas de ingeniería social, en los que se explote la confusión generada por inconsistencias en el etiquetado para redirigir al usuario hacia comunicaciones fraudulentas.

5. KYC, identificación del beneficiario final y conservación por cinco años (Artículos 6.13.3.1 y 6.13.3.2)

De acuerdo con el Proyecto de Resolución, los asignatarios de SENDER ID iniciarán ante los asignatarios de código corto A2P el proceso de KYC como clientes, obtendrán la certificación correspondiente y formalizarán los contratos requeridos. Frente a este modelo es importante señalar que el PCA asume la posición de cliente y debe ser examinado y certificado.

Al respecto, el Proyecto de Resolución incluye cargas administrativas desproporcionadas y obligatorias para los PCA que no aportan seguridad al ecosistema y sí generan costos y demoras injustificadas para el PCA. Antes de acceder al SENDER ID, el PCA queda sujeto a un trámite de habilitación ante un particular y a la obtención de una certificación. El resultado es trámites excesivos sobre el mismo sujeto dado que el asignatario del código corto A2P examina al PCA y el validador vuelve a revisar ese examen.

Además, la habilitación previa del PCA implica la imposición de barreras de acceso al mercado, que además depende de la decisión de un tercero particular. Esta subordinación operativa no solo restringe injustificadamente la libre entrada de nuevos competidores, sino que carece de control estatal directo, lo que incrementa el riesgo de conductas discriminatorias. Al condicionar la viabilidad comercial de un PCA a la discrecionalidad de un tercero independiente, se desincentiva la inversión en el sector y se ralentiza la adopción de innovaciones tecnológicas, perjudicando la eficiencia general del mercado de mensajería A2P.

El proyecto define el KYC como un proceso de debida diligencia mediante el cual los asignatarios de código corto A2P deben verificar identidad, legitimidad y perfil de riesgo de los agentes con quienes contratan, con el propósito de prevenir el uso indebido de recursos de identificación para la comisión de fraudes por SMS. Resulta preocupante que el Proyecto exija la identificación del beneficiario final y disponga que el formato correspondiente sea elaborado con base en criterios de prevención del lavado de activos y financiación del terrorismo. La incorporación de estándares LA/FT en una regulación cuyo objeto es mitigar fraude por SMS puede generar ambigüedad jurídica, duplicidad regulatoria y cargas desproporcionadas para empresas que no son sujetos obligados bajo el régimen colombiano de prevención de LA/FT. Esto teniendo en cuenta que la debida diligencia LA/FT corresponde a un régimen legal especializado, con autoridades, sujetos obligados, metodologías y consecuencias propias.

Adicionalmente, es necesario evaluar la proporcionalidad de condicionar la asignación del SENDER ID a una certificación de KYC emitida dentro de un modelo centralizado. El proyecto establece que el KYC es condición necesaria para que el validador centralizado expida la certificación requerida para la asignación del SENDER ID. Este diseño puede convertirse en una barrera para el acceso al mercado, especialmente para pequeñas empresas,

desarrolladores, comercios electrónicos, startups y proveedores globales que operan con múltiples intermediarios o modelos de mensajería transaccional.

Finalmente, la redacción actual del artículo 6.13.3.1.7 resulta excesivamente amplia porque exige conservar la totalidad de la información KYC por cinco años después de la terminación del contrato, sin diferenciar entre tipos de datos, niveles de riesgo, existencia de incidentes, obligaciones legales específicas o necesidad probatoria. Ello puede implicar la retención prolongada de datos personales y empresariales sensibles, incluyendo información de representantes legales, documentos de identidad, beneficiarios finales, antecedentes, perfil de riesgo, información contractual y datos comerciales. Esta retención generalizada incrementa los riesgos de seguridad, acceso no autorizado, usos secundarios, duplicidad de bases de datos y exposición innecesaria de titulares y empresas a riesgos de seguridad.

6. Atribución de responsabilidad por mal uso potencial de plantillas (Artículos 6.13.4.4 y 6.12.3.2.12)

El artículo 6.13.4.4 regula la atribución de responsabilidad por el mal uso de plantillas, y el numeral 6.12.3.2.12 establece como causal de recuperación del SENDER ID el envío de mensajes que potencialmente pueden ser atribuibles al mal uso de las plantillas y que sea imputable al asignatario.

Una causal de recuperación basada en lo potencialmente atribuible al mal uso de las plantillas introduce un estándar indeterminado y cercano a la responsabilidad objetiva, con la consecuencia gravísima de la pérdida del recurso y la desactivación de todas las plantillas del asignatario. Consideramos respetuosamente que la indeterminación afecta la tipicidad, la seguridad jurídica y el debido proceso protegidos en el artículo 29 de la Constitución Política. La responsabilidad debe fundarse en conocimiento efectivo y control real, y no en una simple potencialidad.

7. Enfoque diferencial en campañas educativas

Las campañas pedagógicas previstas en el proyecto deben incorporar enfoques diferenciales para las poblaciones más expuestas o vulnerables frente a estas modalidades de fraude, como adultos mayores, personas con menor alfabetización digital y personas con discapacidad. La prevención del fraude no depende únicamente de controles técnicos, sino que también requiere que los usuarios identifiquen señales de alerta, reconozcan los canales oficiales de comunicación, comprendan los riesgos de entregar información sensible y conozcan los pasos para reportar eventos sospechosos.

Por ello, las campañas deberían diseñarse con lenguaje claro, formatos accesibles y canales adecuados para cada población objetivo, de forma que la información sea comprensible, oportuna y útil para prevenir eventos de fraude.

Desde la perspectiva del usuario final, las medidas propuestas también pueden generar riesgos no intencionados que deben ser mitigados mediante estrategias complementarias. Entre ellos se encuentran la posible pérdida de acceso a servicios financieros por fallas en la recepción de códigos de autenticación, la dificultad para distinguir entre comunicaciones legítimas y fraudulentas en escenarios de etiquetado inconsistente, y la eventual disminución de la confianza en los canales oficiales.

Estos efectos podrían derivar en comportamientos adversos, tales como la búsqueda de canales alternativos no seguros o la entrega de información sensible en contextos de confusión, lo que incrementa la exposición al fraude.

8. Evaluación de riesgos no intencionados

Sin perjuicio de los beneficios esperados, el proyecto puede generar riesgos no intencionados que deben ser evaluados de manera integral. Entre ellos se encuentran la interrupción de controles antifraude críticos, la introducción de nuevos puntos únicos de falla, el incremento de la dependencia de infraestructuras de terceros y la posible generación de incentivos adversos para la adaptación de los esquemas de fraude.

Estos riesgos no necesariamente se derivan de fallas en la implementación, sino del diseño mismos de los mecanismos propuestos, particularmente cuando introducen dependencias centralizadas o restricciones operativas sobre canales que actualmente cumplen funciones esenciales en la prevención del fraude.

En este sentido, se recomienda que la CRC incorpore un enfoque de evaluación ex ante y ex post del riesgo sistémico asociado a las medidas, con el fin de asegurar que los beneficios esperados superen los impactos potenciales sobre la estabilidad, continuidad y seguridad del ecosistema.

Igualmente, desde la perspectiva de la buena regulación, las medidas propuestas deberían estar soportadas en un Análisis de Impacto Normativo (AIN) robusto e integral que permita evaluar no solo los beneficios esperados en la prevención del fraude cibernético, sino también los posibles efectos adversos y riesgos no intencionados que podrían derivarse de su implementación.

Particularmente, dicho análisis debería considerar aspectos como la posible afectación de comunicaciones críticas de autenticación y seguridad, la introducción de puntos únicos de falla asociados a esquemas centralizados de validación, los impactos sobre la continuidad y disponibilidad de servicios digitales, los costos de implementación y cumplimiento para los distintos actores involucrados, así como los eventuales efectos sobre la innovación, la competencia y la experiencia de los usuarios.

Lo anterior permitiría asegurar que las medidas finalmente adoptadas sean necesarias, idóneas y proporcionales, y que los beneficios esperados en materia de prevención del fraude superen los impactos potenciales sobre la estabilidad, continuidad, seguridad y eficiencia del ecosistema digital.

9. Comentario en materia de protección de datos personales

Se considera necesario incorporar un análisis específico desde la perspectiva de protección de datos personales, teniendo en cuenta que varias de las medidas propuestas implican el tratamiento intensivo, sistemático y potencialmente centralizado de información de usuarios, originadores y tráfico de comunicaciones.

En primer lugar, el Proyecto debería establecer de manera expresa que todas las medidas se sujetan a los principios de la Ley 1581 de 2012, particularmente finalidad, necesidad, proporcionalidad, seguridad y confidencialidad. El tratamiento de datos debe limitarse exclusivamente a la prevención del fraude y evitar la recolección excesiva o el uso para finalidades distintas. En relación con el validador centralizado, su diseño implica la creación de una base de datos de alta concentración que procesará información relevante de múltiples actores del ecosistema.

En este sentido, resulta necesario definir de forma expresa su rol en el tratamiento de datos personales (responsable, encargado o corresponsable), así como exigir la realización de una evaluación de impacto en protección de datos personales previa a su implementación. Igualmente, deben establecerse reglas claras de gobernanza de la información, criterios de inclusión y exclusión, así como límites estrictos de conservación y acceso.

Adicionalmente, los mecanismos de validación de plantillas y verificación previa podrían implicar acceso al contenido de comunicaciones, incluyendo mensajes de autenticación, alertas transaccionales o comunicaciones de seguridad. Se recomienda limitar estos procesos a la validación de metadatos o elementos estructurales, evitando el acceso al contenido completo cuando no sea necesario, y prohibir expresamente el almacenamiento de datos sensibles como códigos OTP u otros factores de autenticación. Respecto al intercambio de información entre actores (PRST, integradores, asignatarios, autoridades), se deben definir claramente las finalidades específicas de cada flujo de datos, las bases legales aplicables y las restricciones al uso ulterior de la información. Este intercambio debe regirse por criterios de necesidad y proporcionalidad, evitando escenarios de reutilización o expansión indebida del tratamiento.

Las medidas de trazabilidad y detección de patrones pueden implicar el uso de herramientas automatizadas y generación de perfiles. En este contexto, se deben incorporar garantías de transparencia, mecanismos de revisión frente a decisiones automatizadas, y límites claros para evitar el profiling masivo que exceda la finalidad de prevención del fraude.

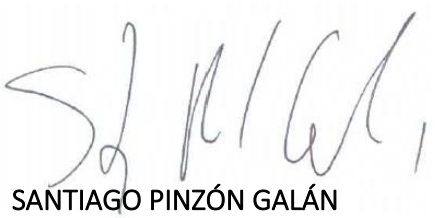
En materia de seguridad de la información, el Proyecto debería establecer requisitos mínimos, tales como cifrado de la información en tránsito y reposo, controles de acceso basados en roles, registros de auditoría y planes de continuidad de negocio, especialmente considerando los riesgos derivados de la centralización de funciones en un único validador.

En conclusión, aunque el Proyecto persigue un objetivo legítimo de prevención del fraude, resulta fundamental asegurar que las medidas adoptadas incorporen salvaguardas robustas en materia de protección de datos personales, garantizando que sean proporcionales, necesarias y compatibles con el marco legal vigente.

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