Superintendencia de Industria y Comercio

DELEGATURA PARA LA PROTECCIÓN DE DATOS PERSONALES
PROYECTO DE CIRCULAR SOBRE TRATAMIENTO DE DATOS PERSONALES EN LA PRESTACCIÓN DE SERVICIOS FINANCIERSOS MEDIANTE EL USO DE TECNOLOGÍAS DIGITALES (FINTECH)

DOCUMENTO DE RESPUESTA A LOS COMENTARIOS

Agradecemos a todas las personas naturales y jurídicas que enviaron sus comentarios al proyecto de circular mencionado, publicado por la Superintendencia de Industria y Comercio el pasado 6 de mayo de 2025.

Consideramos que la participación ciudadana es fundamental para dotar de legitimidad las decisiones públicas, en tanto permite conocer e integrar al ejercicio regulatorio las distintas visiones de diferentes actores sobre las virtudes, los defectos y los posibles impactos de la regulación propuesta.

Este documento recoge las respuestas a los comentarios, sugerencias y observaciones formulados por más de treinta personas, gremios, asociaciones y entidades públicas al proyecto de circular sobre instrucciones en torno al tratamiento de datos personales en la prestación de servicios financieros mediante el uso de tecnologías digitales (fintech).

Las respuestas han sido organizadas conforme al contenido de cada instrucción, precisando, cuando corresponde, los fundamentos jurídicos aplicables, el alcance normativo de las disposiciones, y los ajustes realizados como resultado del análisis técnico y jurídico de los aportes recibidos. En algunos casos, las instrucciones fueron modificadas o reformuladas para mejorar su redacción, reforzar su carácter orientador o evitar duplicidades; en otros, se reiteró su validez en el marco del régimen normativo de protección de datos personales. Excepcionalmente, se eliminaron algunas instrucciones en tanto los aportes recibidos evidenciaron su inconveniencia.

Este ejercicio busca no solo dar respuesta formal a los comentarios, sino también fortalecer el diálogo técnico con los actores del ecosistema, promover la implementación clara y efectiva de la normativa, y reforzar la confianza en la

gestión responsable de los datos personales en entornos digitales altamente automatizados.

A partir de este ejercicio, desde la Delegatura para la Protección de Datos Personales **hemos preparado un segundo borrador de circular** torno al tratamiento de datos personales en la prestación de servicios financieros mediante el uso de tecnologías digitales (fintech), con el fin de continuar con el diálogo propuesto y concretar el ejercicio regulatorio.

Como parte de nuestro compromiso con la transparencia y el valor de la participación ponemos a disposición de la ciudadanía interesada tanto las respuestas a los comentarios recibidos haciendo referencia a cada una de las instrucciones del primer borrador publicado para comentarios, como un segundo borrador de circular en el que integramos dichos comentarios y observaciones recibidos.

Respuestas a los comentarios recibidos

Sobre el ámbito de aplicación personal y material y la competencia de la Superintendencia de Industria y Comercio

Tomamos nota de varios comentarios en relación con tres asuntos de carácter general. Frente a estos comentarios, introdujimos varios ajustes, tanto en los considerandos, como en las instrucciones específicas. En algunos puntos, revisamos la redacción general, en otros introdujimos ajustes puntuales. Todo ello con el propósito de concretar la función básica de la circular: servir de instrumento para el cabal cumplimiento de las obligaciones legales y constitucionales en materia de protección de datos personales, y claro, cuando lo vimos pertinente, con el fin de aligerar la redacción, evitar redundancias y aclarar las posibles confusiones. Veamos estos tres asuntos

El primero, relacionado con el ámbito de aplicación de las instrucciones y un posible traslape con el ámbito de competencias de la Superintendencia Financiera de Colombia. Para aclarar este punto, insistimos en él, desde el cabezote de la circular, al identificar tanto el objeto como los destinatarios de la circular e introdujimos un párrafo en las consideraciones para dejar explícito que esta circular solo está dirigida a los sujetos vigilados por la Superintendencia de Industria y Comercio.

El segundo, relacionado con una supuesta extralimitación de las funciones de la Superintendencia de Industria y Comercio, ya por que algunas de las instrucciones se limitaban a "repetir" o "parafrasear" los textos legales, ya porque algunas incluían deberes no estrictamente previstos en dichos textos. Para esto insistimos en la competencia de la Superintendencia para instruir a los sujetos vigilados y para velar por el cumplimiento de las obligaciones legales y constitucionales en la materia, e introdujimos sendos párrafos en las consideraciones alusivos al espíritu sistematizador de la normatividad vigente que guía este esfuerzo regulatorio en relación con unos sujetos obligados muy específicos: aquellos que adelanten tratamiento de datos personales para la prestación de servicios y productos financieros utilizando tecnologías digitales.

El tercero, relacionado con los destinatarios y con los roles. Para mayor claridad incluimos una definición de fintech a partir de aludir a la "innovación en el sistema financiero mediante el uso de tecnologías digitales para la prestación de servicios y la comercialización de productos financieros", y retomamos los roles que tanto la Ley 1266 de 2008, como la Ley 1581 de 2012 establecen en relación con el tratamiento de datos personales (usuario, fuente, responsable y encargado) y a partir de aquí preciamos quiénes son, en estos contextos, sujetos vigilados por la Superintendencia de Industria y Comercio. Asimismo, a lo largo de la circular utilizamos, cuando fue pertinente, la expresión sujetos vigilados (para incluirlos a todos, a partir de los cuatro roles ya descritos) o cuando era pertinente, utilizamos las expresiones: responsable, encargado, fuente, etc.

Sobre la instrucción 1

La instrucción reafirma un principio esencial del régimen normativo de protección de datos personales: el principio de finalidad, consagrado en el literal b) del artículo 4 de la Ley 1581 de 2012, el cual establece que *"el tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al titular"*. Este principio exige que cualquier actividad de tratamiento esté orientada a un propósito lícito a la luz de la Constitución Política determinado, explícito y previamente informado, lo que excluye tratamientos genéricos, indefinidos o desvinculados de un objetivo constitucionalmente legítimo.

Asimismo, la instrucción recoge lo establecido en el artículo 11 del Decreto 1377 de 2013, según el cual los responsables y encargados solo pueden tratar datos personales *"durante el tiempo que sea razonable y necesario, de acuerdo con*

las finalidades que justificaron el tratamiento". Esta limitación temporal al tratamiento es una salvaguarda frente a tratamientos extensivos o injustificados que puedan afectar derechos fundamentales.

En consecuencia, la instrucción no introduce una obligación nueva, sino que precisa cómo debe aplicarse este límite temporal en el contexto específico de los modelos de negocio Fintech y de quienes adelantan tratamiento de datos personales en este contexto y bajo diferentes roles.

Por otro lado, no se consideró apropiado incluir un listado cerrado de finalidades en la instrucción, ya que estas dependen de la diversidad de modelos de negocio en el ecosistema fintech, la naturaleza del servicio ofrecido y el ciclo de vida de los datos. No obstante, en todos los casos, la finalidad debe ser constitucionalmente legítima, informada al titular y documentada por parte del responsable.

Sobre la instrucción 2

La instrucción incorpora el principio de necesidad o minimización, el cual ha sido reconocido por la Corte Constitucional como uno de los principios rectores del régimen de protección de datos personales. En particular, en las sentencias C-748 de 2011 y T-307 de 1999 se ha sostenido que *"los datos personales registrados deben ser los estrictamente necesarios para el cumplimiento de las finalidades perseguidas con la base de datos de que se trate"*, y que *"la información solicitada debe ser estrictamente necesaria y útil para alcanzar la finalidad constitucional perseguida"*.

En consecuencia, la instrucción no introduce una prohibición absoluta al acceso y tratamiento a ciertos tipos de datos, sino que exige que su tratamiento sea justificado, necesario y alineado con las finalidades constitucionalmente legítimas informadas al titular. El principio de minimización no implica que no se puedan recolectar datos personales**,** sino que solo se recolecten los que resulten pertinentes, adecuados y necesarios para cumplir con la finalidad declarada y autorizada.

Este principio tiene particular relevancia para los modelos de negocio objeto de la presente instrucción**,** caracterizados por el uso de aplicaciones tecnológicas que, en algunos casos, solicitan acceso a funcionalidades del dispositivo móvil (como lista de contactos, geolocalización o galería de imágenes). Estas prácticas deben evaluarse conforme al principio de necesidad: si el dato solicitado no

guarda una relación directa y necesaria para la prestación el servicio ofrecido, su tratamiento se considera excesivo y, por tanto, contrario a la ley.

Sobre la instrucción 3

La instrucción se fundamenta en el deber de informar y de obtener la autorización libre, previa e informada del titular, exigencias que constituyen condiciones habilitantes para cualquier tratamiento de datos personales, conforme a lo dispuesto en los artículos 9 y 12 de la Ley 1581 de 2012**.** En particular, el artículo 12 establece que, al momento de solicitar la autorización, el responsable del tratamiento debe informar al titular, de manera clara y expresa, sobre:

- El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- Los derechos que le asisten como titular;
- La identificación, dirección física o electrónica y teléfono del responsable del tratamiento.

Así mismo, la norma establece la obligación del responsable de conservar prueba del cumplimiento de este deber y de entregar copia de la autorización cuando el titular lo solicite. Por tanto, la instrucción no introduce un requisito nuevo, sino que reitera las obligaciones legales ya vigentes y exigibles a todos los responsables, incluyendo las fintech, sin excepción.

Se ajustó la redacción de la instrucción para reafirmar que su propósito no es imponer restricciones arbitrarias, sino recordar y armonizar las obligaciones ya previstas en la legislación vigente, garantizando su cumplimiento adecuado en entornos digitales, y se ajusta al principio de transparencia**,** según el cual los titulares deben ser informados sobre cada acceso específico a funcionalidades del dispositivo (por ejemplo, cámara, ubicación o contactos) a través de aplicaciones fintech. La transparencia es una condición para la validez del consentimiento, pues permite al titular tomar una decisión informada sobre el uso de sus datos, con base en finalidades específicas, claras y legítimas.

Finalmente, conforme a los comentarios recibidos, se advierte que no es jurídicamente válido interpretar que la Política de Tratamiento de Datos sustituya

o supla la función de la autorización para el tratamiento de datos. La política es un instrumento de divulgación general que cumple el deber de informar al titular y a otras partes interesadas sobre del marco institucional de tratamiento de datos personales, pero no sustituye el deber de obtener consentimiento expreso e individual por parte del titular. Aceptar esa equivalencia implicaría desconocer el régimen normativo vigente y debilitar las garantías sustanciales que le asisten al titular sobre el control de su información personal.

Sobre la instrucción 4

La instrucción reitera una obligación legal fundamental del régimen colombiano de protección de datos personales: la necesidad de obtener y conservar prueba suficiente de la autorización otorgada por el titular para el tratamiento de sus datos personales, conforme a lo previsto en los artículos 9 y 12 de la Ley 1581 de 2012, y en concordancia con los artículos 2.2.2.25.2.1 y siguientes del Decreto 1074 de 2015.

La autorización debe ser libre, previa, expresa e informada. Esto significa que el titular debe manifestar su consentimiento sin coacción, antes de cualquier tratamiento, de manera clara e inequívoca, y con conocimiento suficiente sobre las finalidades del tratamiento, los derechos que le asisten y los datos de identificación del responsable del tratamiento.

La autorización puede obtenerse por cualquier medio que permita su consulta posterior. En este sentido, la instrucción se ajusta y refuerza este estándar legal, especialmente en el contexto del tratamiento de datos por personas que prestan servicios financieros a través de medios tecnológicos, donde las interacciones con los usuarios se realizan de manera remota y automatizada a través de plataformas digitales y aplicaciones móviles. En tales entornos, contar con pruebas claras, trazables y verificables de la autorización no solo constituye una obligación legal, sino también una condición para generar confianza con los usuarios y un elemento clave de protección jurídica ante posibles reclamaciones, verificaciones o investigaciones administrativas.

Sobre la instrucción 5

La instrucción reafirma una obligación legal esencial para el tratamiento de datos personales por parte de los responsables: asegurar que la autorización sea libre, previa, expresa e informada, conforme a los principios de libertad y finalidad

consagrados en el artículo 4 de la Ley 1581 de 2012, y al artículo 9, que establece que el tratamiento solo puede realizarse con autorización del titular y para las finalidades previamente informadas.

En particular, la instrucción fue ajustada para establecer con mayor claridad que, cuando se solicite autorización para el tratamiento de datos personales con finalidades adicionales a aquellas estrictamente necesarias para la prestación del servicio, esta debe otorgarse de manera diferenciada. En consecuencia, los responsables del tratamiento deberán distinguir como mínimo dos grupos de finalidades al momento de solicitar la autorización:

- Finalidades necesarias o esenciales, sin las cuales no es posible prestar el servicio principal.
- Finalidades accesorias o facultativas, como el envío de comunicaciones comerciales, actividades de mercadeo, perfilamiento o cesión de datos a terceros.

Este ajuste tiene como objetivo garantizar un consentimiento válido, evitando prácticas de consentimiento forzado o empaquetado, que son contrarias al principio de libertad y pueden comprometer la validez jurídica de la autorización.

En los modelos de negocio relacionados con fintech, caracterizados por la digitalización, el uso intensivo de datos y la automatización de procesos, esta diferencia es crucial. La autorización para finalidades facultativas no puede ser una condición para el acceso a los servicios financieros básicos, y la negativa del titular a autorizarlas no debe impedir la prestación del servicio principal.

Para facilitar este ejercicio, la nueva redacción de la instrucción permite que las finalidades facultativas puedan ser agrupadas de manera razonable, siempre que se cumplan dos condiciones:

- Que el lenguaje utilizado para presentar la solicitud de autorización sea claro, sencillo y comprensible, de modo que el titular entienda el alcance y consecuencias de su decisión.
- Que el mecanismo de recolección permita al titular aceptar o rechazar las finalidades no necesarias, sin restricciones indebidas.

En conclusión, la instrucción no impone una carga nueva ni restringe la operación de los modelos de negocio fintech, sino que concreta los principios vigentes, orientando su aplicación en entornos digitales de alta complejidad, donde la

transparencia y el respeto por los derechos del titular constituyen pilares fundamentales para la sostenibilidad del ecosistema.

Sobre las instrucciones 6 y 7

Ambas instrucciones fueron unificadas, con el fin de ofrecer una interpretación más clara, coherente y sistemática de las reglas que regulan el tratamiento de datos personales sensibles, especialmente en lo relativo al uso de datos biométricos en entornos digitales.

La instrucción no introduce una regla nueva ni impone una carga adicional, sino que reafirma los límites legales existentes para el tratamiento de datos sensibles, de conformidad con lo dispuesto en el artículo 6 de la Ley 1581 de 2012 y en el artículo 6 del Decreto 1377 de 2013.

En el contexto fintech, donde el uso de datos biométricos es crítico y generalizado para fines de autenticación o prevención del fraude, la instrucción reformulada enfatiza que su tratamiento puede ser legítimo cumpliendo las condiciones previstas en la Ley. En especial, que se cuente con la autorización específica y expresa del titular, a partir de una carga reforzada de precisar las finalidades y los límites del tratamiento de este tipo de datos.

En cuanto a la protección reforzada de los datos sensibles y la prohibición expresa a su tratamiento, la Corte Constitucional en sentencia C-748 de 2011 ha establecido lo siguiente:

> *"Como se indicó en apartes previos, la prohibición de tratamiento de datos sensibles es una garantía del habeas data y del derecho a la intimidad, y además se encuentra estrechamente relacionada con la protección de la dignidad humana. Sin embargo, en ciertas ocasiones el tratamiento de tales datos es indispensable para la adecuada prestación de servicios, como la atención médica y la educación, o para la realización de derechos ligados precisamente a la esfera íntima de las personas como la libertad de asociación y el ejercicio de las libertades religiosas y de opinión. Las excepciones del artículo 6 responden precisamente a la necesidad del tratamiento de datos sensible en dichos escenarios.*
>
> *Ahora bien, como se trata de casos exceptuados y que, por tanto, pueden generar altos riesgos en términos de vulneración del habeas data, la*

> *intimidad e incluso la dignidad de los titulares de los datos,* ***los agentes que realizan en estos casos el tratamiento tienen una responsabilidad reforzada que se traduce en una exigencia mayor en términos de cumplimiento de los principios del artículo 4 y los deberes del título VI****. Esa mayor carga de diligencia se deberá también traducir en materia sancionatoria administrativa y penal".*

En este contexto, el uso de datos biométricos requiere una atención especial por parte del responsable del tratamiento, debido a los riesgos elevados que puede implicar para los derechos fundamentales del titular.

Para garantizar la validez del tratamiento, especialmente en entornos digitales de alta automatización, los responsables deberán, al momento de la recolección, informar al titular sobre las finalidades específicas para las cuales se recolectan los datos, así como una explicación de porqué el tratamiento de los datos biométricos es necesario para la prestación de los servicios y el consumo de los productos financieros. En este sentido deberá especificar de forma detallada sus finalidades, tales como prevención del fraude, autenticación o verificación de usuarios, controles de acceso, actualización de datos personales o validación de transacciones con alto riesgo.

Además, el responsable del tratamiento deberá tomar otras medidas para la protección de dicha información durante todas las etapas del tratamiento. En este sentido, deberá implementar medidas de seguridad técnicas, jurídicas y organizativas reforzadas para proteger estos datos, garantizar que su uso sea proporcional al nivel de riesgo asociado a la finalidad perseguida, abstenerse de compartir la información con terceros (sobre todo para evitar la construcción de bases de datos biométricas centralizadas), y proceder al borrado de los datos biométricos cuando su tratamiento ya no sea necesario, se hayan concluido las relaciones contractuales y transcurra un tiempo prudencial, que puede ser el de 4 años, sin que el titular no haya contactado a la Fintech o no haya solicitado un nuevo producto o servicio.

Sobre la instrucción 8

Esta instrucción se fundamenta en el principio de transparencia, consagrado en el artículo 4 de la Ley 1581 de 2012, el cual impone al responsable del tratamiento el deber de garantizar al titular el acceso, en cualquier momento y sin restricciones, a información sobre la existencia de datos que le conciernan. Este principio atraviesa todas las etapas del tratamiento de datos personales, y

adquiere especial relevancia en contextos donde se emplean tecnologías automatizadas.

En las fintech, estas tecnologías son habituales en procesos como el perfilamiento de usuarios, análisis de riesgo, otorgamiento de créditos, monitoreo de operaciones y detección de fraude. Por ello, la transparencia en su uso no puede ser discrecional, ya que es indispensable para que los titulares comprendan cómo se tratarán sus datos y cuáles pueden ser los efectos sobre sus derechos e intereses.

La instrucción no prohíbe ni restringe el uso de tecnologías automatizadas, sino que promueve el cumplimiento efectivo del principio de transparencia en su aplicación. Aunque la legislación colombiana no contempla un régimen específico sobre decisiones automatizadas como el del Reglamento General de Protección de Datos de la Unión Europea (RGPD), los principios generales de la Ley 1581 de 2012, en particular, los de transparencia y finalidad, se aplican plenamente al uso de estas tecnologías. En este sentido, la instrucción no impone nuevas cargas regulatorias, sino que orienta la aplicación de normas vigentes en un entorno tecnológicamente intensivo.

En armonía con estos principios, la instrucción dispone que los responsables, deben garantizar la transparencia en el uso de tecnologías automatizadas en procesos que generen efectos jurídicos desfavorables al titular. En particular, deberán informar de manera clara y suficiente a los titulares sobre la utilización de este tipo de herramientas. Esta información deberá estar disponible desde el momento de la recolección de los datos en la Política de Tratamiento de la Información, así como en los términos y condiciones y/o mediante mensajes específicos durante el proceso de registro o solicitud del servicio, todo ello en un lenguaje comprensible para el usuario promedio.

El titular tendrá, además, el derecho a conocer las razones objetivas que dieron lugar a una decisión automatizada desfavorable. Cuando las tecnologías utilizadas correspondan a sistemas de inteligencia artificial, los responsables y encargados deberán aplicar lo dispuesto en la Circular Externa No. 002 del 21 de agosto de 2024, que contiene los "Lineamientos sobre el Tratamiento de Datos Personales en Sistemas de Inteligencia Artificial".

Sobre la instrucción 9

La instrucción 9 fue eliminada, en tanto su contenido fue integrado en la instrucción 8, con el fin de consolidar en un solo cuerpo de lineamientos relacionados con el tratamiento automatizado de datos personales.

Sobre la instrucción 10

La instrucción retoma el principio de seguridad, consagrado en el literal g) del artículo 4 de la Ley 1581 de 2012, que establece que los responsables y encargados del tratamiento deben adoptar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Esta obligación tiene carácter general, pero su implementación concreta debe ser proporcional al nivel de riesgo asociado al tipo de datos tratados, al contexto del tratamiento y a la tecnología empleada. Por tanto, la instrucción no impone un estándar unificado o fijo de seguridad, sino que orienta a los actores instruidos a adoptar medidas razonables y ajustadas a su realidad operativa y a los riesgos específicos identificados. En el entorno fintech, donde se utilizan tecnologías emergentes, infraestructuras en la nube, autenticaciones biométricas y sistemas automatizados de decisión, el nivel de riesgo es generalmente elevado, lo cual demanda una gestión activa y actualizada de las medidas de seguridad.

La instrucción se ajustó considerando que las medidas implementadas deben ser verificables, es decir, permitir su evaluación por parte de las autoridades competentes, incluyendo la Superintendencia de Industria y Comercio, para efectos de vigilancia, control y mejora continua. Esta exigencia no genera una nueva obligación**,** sino que se deriva directamente del principio de responsabilidad demostrada o *accountability*, el cual exige a los responsables demostrar que han tomado acciones razonables y verificables para proteger los datos personales bajo su custodia.

Sobre la instrucción 11

La instrucción se fundamenta en el artículo 21 del Decreto 1377 de 2013, que establece que los responsables y encargados del tratamiento deben habilitar mecanismos sencillos, eficaces y de acceso permanente para que los titulares puedan ejercer sus derechos.

En consecuencia, los responsables del tratamiento deben garantizar la existencia de canales efectivos para el ejercicio del derecho al habeas data, sin imponer barreras técnicas, jurídicas o administrativas que dificulten su ejercicio. La instrucción no introduce una carga nueva, sino que reitera una obligación central del responsable del tratamiento: facilitar el ejercicio permanente y real de los derechos del titular.

La instrucción fue fortalecida para precisar que los sujetos obligados deben establecer mecanismos ágiles, simples y permanentemente disponibles para que los titulares puedan ejercer, de manera efectiva, sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales, en concordancia con el artículo 15 de la Constitución, la Ley 1266 de 2008, la Ley 1581 de 2012 y la jurisprudencia constitucional.

El procedimiento habilitado para la recolección o captura de datos personales debe ser igual de ágil y sencillo que el previsto para su rectificación, actualización o supresión. Esta garantía debe estar reflejada de forma clara en la Política de Tratamiento de Datos o en cualquier otro medio visible y de fácil acceso, que permita a los titulares conocer y utilizar los mecanismos dispuestos para el ejercicio de sus derechos.

El propósito de esta instrucción es promover la efectividad del habeas data en entornos digitales, y contribuir al fortalecimiento de la confianza de los usuarios frente a la gestión responsable de sus datos personales por parte de las empresas del sector fintech.

Sobre la instrucción 12

La instrucción 12 fue eliminada del texto de la circular. Sin embargo, es importante precisar que los fundamentos que motivaban su inclusión siguen siendo relevantes, especialmente en el entorno fintech, donde es común que terceros puedan realizar tratamiento de datos personales a nombre del responsable del tratamiento. En estos contextos, los responsables del tratamiento deben seguir adoptando medidas técnicas y organizativas que permitan rastrear, registrar y documentar dichos accesos, con el fin de garantizar su transparencia, trazabilidad y eventual supervisión.

Sobre la instrucción 13

Esta instrucción no sustituye ni modifica las obligaciones legales vigentes, sino que las refuerza a través de estrategias prácticas que permiten a los titulares ejercer de manera efectiva su derecho de habeas data. Asimismo, estas estrategias pueden constituir buenas prácticas en el marco del principio de responsabilidad demostrada, el cual exige a los responsables del tratamiento evidenciar proactivamente el cumplimiento de las obligaciones legales en materia de protección de datos.

Atendiendo a los comentarios recibidos, la instrucción fue ajustada para reafirmar su naturaleza orientadora y no prescriptiva, evitando la imposición de un único modelo o formato sobre cómo debe presentarse la información al titular. No obstante, se conserva el énfasis en la utilidad de estas estrategias para fortalecer la confianza del usuario y garantizar un cumplimiento efectivo en servicios financieros mediados por tecnología.

En esta versión fortalecida, se indica que los responsables del tratamiento deben implementar medidas que mejoren la comprensión del titular sobre cómo se realiza el tratamiento de sus datos personales. Estas medidas incluyen mecanismos visibles e intuitivos que permitan a los titulares gestionar sus preferencias de privacidad y decidir sobre la entrega de sus datos personales.

Adicionalmente, se establece que deben habilitarse mecanismos accesibles y continuos para informar a los titulares sobre sus derechos en materia de protección de datos y los riesgos asociados al tratamiento de su información personal. Por tanto, se exhorta a los sujetos obligados a asumir un rol activo en la sensibilización y educación de sus clientes y usuarios, contribuyendo así a una cultura de protección de datos más robusta y participativa.

Sobre la instrucción 14

La instrucción se limita a reiterar obligaciones legales vigentes aplicables a los actores del ecosistema fintech que desarrollan actividades de cobranza directa o indirecta, especialmente aquellas derivadas de la Ley 2300 de 2023, en concordancia con las Leyes 1266 de 2008 y 1581 de 2012, y lo señalado por la Circular Externa 001 del 26 de junio de 2024 de esta Superintendencia. El contacto a terceros sin su consentimiento vulnera los principios de finalidad, libertad y circulación restringida del régimen de protección de datos personales.

La instrucción se ajustó considerando los comentarios recibidos, para reforzar que no se está creando una regla adicional o restrictiva, sino que se está

recordando una prohibición legal expresa, especialmente, si conlleva un tratamiento indebido de datos personales o un uso abusivo de canales de contacto.

En este contexto, donde las gestiones de cobranza pueden ser automatizadas, tercerizadas o delegadas mediante cesión de cartera, esta instrucción es relevante para:

- Evitar prácticas invasivas que comprometan la protección de datos de las personas no vinculadas contractualmente con la obligación.
- Reforzar el deber de los responsables de establecer límites contractuales y operativos claros en la relación con terceros.
- Asegurar el cumplimiento normativo transversal tanto en el régimen de protección de datos como en la normativa de protección al consumidor financiero.

Sobre la instrucción 15

La instrucción fue eliminada como disposición independiente y su contenido se integró de manera complementaria en la instrucción 13 para evitar duplicidades y reforzar el enfoque desde el principio de transparencia. La legislación vigente, en particular el numeral 2 del artículo 27 del Decreto 1377 de 2013, establece que las organizaciones deben considerar *"La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación".*

Sin embargo, en el contexto del ecosistema fintech, donde el tratamiento de datos personales se realiza en entornos altamente digitalizados, con tecnologías automatizadas y modelos de negocio basados en el uso intensivo de datos, la implementación voluntaria de acciones de educación, sensibilización e información dirigida a los titulares constituye una buena práctica altamente valorada por la autoridad de protección de datos.

Este tipo de medidas promueven el ejercicio informado de los derechos por parte de los titulares, la reducción de riesgos asociados al desconocimiento o mal uso de la información personal, una cultura organizacional basada en la transparencia, la confianza y el respeto por los datos personales. Por ello, la Superintendencia las reconoce como parte del principio de responsabilidad demostrada, conforme al cual los responsables deben poder evidenciar que han

implementado mecanismos proactivos y verificables para cumplir con sus deberes legales y garantizar los derechos de los titulares.

Sobre la instrucción 16

La instrucción se limita a reiterar las obligaciones legales vigentes contenidas en la Ley 1581 de 2012 y sus decretos reglamentarios, aplicándolas a las características propias del ecosistema fintech, sin crear un régimen especial ni imponer cargas diferenciadas.

En particular:

- El artículo 3 de la Ley 1581 distingue con claridad las calidades de responsable y encargado del tratamiento. La correcta identificación de estos roles es fundamental para definir obligaciones, riesgos y responsabilidades dentro del ciclo de tratamiento de datos personales.
- En virtud del principio de responsabilidad demostrada, los actores que intervienen en el tratamiento deben documentar formalmente su rol, y cuando se realicen transmisiones de datos, deben suscribirse contratos de transmisión (cuando hay relación responsable–encargado), conforme a lo dispuesto en el artículo 25 del Decreto 1377 de 2013.

La instrucción también aclara un punto relevante: la forma no puede prevalecer sobre la realidad jurídica del tratamiento. Es decir, si un actor es formalmente designado como encargado, pero en la práctica determina los fines y medios del tratamiento, debe ser considerado responsable del tratamiento, con todas las consecuencias que ello implica. Esta doctrina es consistente con los criterios de esta Superintendencia, y responde a la necesidad de evitar figuras contractuales que simulen o desdibujen el cumplimiento efectivo del régimen de protección de datos.

Dada la complejidad operativa y la pluralidad de actores en el entorno fintech (proveedores tecnológicos, aliados comerciales, plataformas, entidades financieras, pasarelas de pago, entre otros), es fundamental dejar claros los roles desde el inicio, tanto para evitar conflictos, como para garantizar la protección efectiva de los derechos del titular. Esta claridad no puede limitarse a la autorización del titular, ya que la autorización no sustituye ni reemplaza la obligación de establecer contratos o acuerdos entre los intervinientes del tratamiento.

Por tanto, esta instrucción:

- No genera desequilibrios normativos, ya que no impone reglas nuevas al sector fintech, sino que aplica las disposiciones generales a sus dinámicas específicas.
- Fortalece la gobernanza de datos personales, fomenta la claridad contractual y facilita la trazabilidad de las responsabilidades.
- Es coherente con los estándares de buenas prácticas de cumplimiento, especialmente bajo el principio de responsabilidad demostrada.

Sobre la instrucción 17

La instrucción 17 no introduce una nueva obligación, sino que reproduce de manera sistemática y clara las reglas vigentes en Colombia sobre la transferencia y transmisión internacional de datos personales, en especial aquellas contenidas en el artículo 26 de la Ley 1581 de 2012 y el Título V de la Circular Única de la Superintendencia de Industria y Comercio, particularmente en los numerales 3.1, 3.2 y 3.3.

Se parte de una distinción fundamental:

- Transmisión internacional de datos personales: envío de datos personales desde Colombia a un encargado del tratamiento fuera del país, para su tratamiento por cuenta del responsable.
- Transferencia internacional de datos personales: envío de datos personales a un responsable ubicado fuera del país, que decide por sí mismo los fines y medios del tratamiento.

Ambas figuras están reguladas en la legislación colombiana y no deben ser confundidas. No obstante, la Circular Única establece expresamente que las reglas aplicables a las transferencias también pueden aplicarse, en lo pertinente, a las transmisiones internacionales, en la medida en que ambas implican el tratamiento de datos fuera del país y, por tanto, un riesgo transfronterizo para los derechos de los titulares.

La instrucción reitera los pasos que deben seguir los responsables ubicados en Colombia, en cumplimiento de la ley, cuando sus modelos de negocio o procesos tecnológicos impliquen el tratamiento internacional de datos personales.

La instrucción no genera desequilibrios ni confusiones, ya que distingue adecuadamente entre los tipos de tratamiento transfronterizo y sigue el marco legal vigente, el cual es aplicable a todos los modelos de negocio intensivos en datos, incluidos los del ecosistema fintech. Su propósito es guiar el cumplimiento ordenado y seguro de las obligaciones legales, promoviendo buenas prácticas de protección de datos en entornos digitales globalizados.

Sobre la instrucción 18

La instrucción 18 no impone una obligación jurídica nueva. Se trata de una sugerencia por parte de la autoridad, que señala una de las herramientas recomendadas para facilitar el cumplimiento del principio de responsabilidad demostrada en contextos de transferencia y transmisión internacional de datos personales.

La Guía de implementación de Cláusulas Contractuales Modelo para la Transferencia Internacional de Datos Personales (TIDP) de la Red Iberoamericana de Protección de Datos (RIPD) es un instrumento técnico de referencia regional, respaldado por múltiples autoridades nacionales de protección de datos. Su adopción puede ser especialmente útil para:

- Establecer garantías contractuales equivalentes a las exigidas por el ordenamiento colombiano en materia de protección de datos.
- Establecer condiciones claras y simétricas entre el exportador e importador de los datos personales.
- Reducir riesgos regulatorios y facilitar la cooperación internacional, en especial en sectores como el fintech, donde los datos suelen fluir entre jurisdicciones por diseño del modelo de negocio.

La suscripción de estas cláusulas, aunque no es obligatoria, sí constituye una medida idónea, verificable y alineada con buenas prácticas internacionales, y puede ser valorada positivamente por la Superintendencia de Industria y Comercio como parte del cumplimiento del principio de *accountability*, particularmente en procesos de supervisión.

En este sentido, la instrucción tiene el propósito de dar visibilidad a herramientas útiles y reconocidas que pueden fortalecer la gobernanza del tratamiento internacional de datos personales, sin generar cargas normativas adicionales ni modificar el marco vigente.