

 INFORME DE OBSERVACIONES DE LOS PROYECTOS ESPECÍFICOS DE REGULACIÓN		Código: GJ05-F06		
Registro de observaciones a los proyectos de carácter general suscritos por el Superintendente de Industria y Comercio, en atención a lo previsto en el numeral 8 del artículo 8 de la Ley 1437 de 2011.		Versión: 3		
De conformidad con el Título III de la Ley Estatutaria 1712 de 2014, el presente documento se garantizan las excepciones de acceso a la información.		Fecha: 2024-09-25		
Información general del proyecto				
Área responsable del proceso	Delegatura para la Protección de Datos Personales - Juan Carlos Upegui Mejía			
Nombre del proyecto	Lineamientos sobre el tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros.			
Objetivo del proyecto	Instruir a los responsables, encargados, fuentes, operadores y usuarios que presten servicios financieros por medio de tecnología			
Fecha de publicación del proyecto	2025-05-06			
Descripción de la consulta				
Tiempo total de duración de la publicación	25			
Fecha de inicio	2025-05-07			
Fecha de finalización	2025-05-31			
Enlace donde estuvo la consulta pública	https://www.sucop.gov.co/entidades/sic/Normativa?IDNorma=21112			
Canales o medios dispuestos para la difusión del proyecto	Página web de la Superintendencia de Industria y Comercio Sistema Único de Consulta Pública - SUCOP			
Canales o medios dispuestos para la recepción de comentarios	Correo electrónico: delegaturadatos@sic.gov.co			
Resultados de la consulta				
Número de Total de participantes	12			
Número total de comentarios recibidos	240			
Número de comentarios aceptados	85	%	28%	
Número de comentarios parcialmente aceptados	87	%	36%	
Número de comentarios no aceptados	85	%	35%	
Número total de artículos del proyecto	18			
Número total de artículos del proyecto con comentarios	18	%	100%	
Número total de artículos del proyecto modificados	17	%	94%	
Consolidado de observaciones y respuestas				
No.	Remitente	Observación recibida	Estado	Respuesta
1	Bold Co S.A.S. y Bold Capital S.A.S.	<p>Precisiones sobre el ámbito de aplicación del Proyecto de Circular</p> <p>El Proyecto de Circular hace referencia al "ecosistema fintech" como ámbito de aplicación. Sin embargo, consideramos necesario contar con mayor precisión sobre qué entidades y servicios quedan comprendidos dentro de este concepto. Esta claridad resulta fundamental para garantizar la seguridad jurídica y la aplicación uniforme de las obligaciones establecidas. El sector financiero colombiano se caracteriza por su diversidad, incluyendo: (i) entidades tradicionales que operan principalmente a través de canales presenciales; (ii) entidades tradicionales en proceso de transformación digital que combinan canales presenciales y digitales; y (iii) nuevos participantes como las Compañías Bold, que prestan servicios principalmente o exclusivamente a través de canales digitales. Esta heterogeneidad hace necesario delimitar con precisión qué actores quedan sujetos a las instrucciones propuestas.</p> <p>La ausencia de criterios específicos para determinar qué constituye el "ecosistema fintech" podría generar diferentes interpretaciones sobre la aplicabilidad de la norma, creando potenciales asimetrías regulatorias entre actores que prestan servicios similares.</p> <p>Adicionalmente, podría presentarse una situación donde entidades de otros sectores digitales (como e-commerce, marketplaces o retail) que también procesan datos sensibles con finalidades similares, queden excluidas sin una justificación técnica clara.</p> <p>Por lo anterior, sugerimos respetuosamente establecer criterios objetivos para delimitar el alcance de la circular, basados en elementos como: (i) el tipo específico de servicio financiero prestado; (ii) el nivel de supervisión al que está sometida la entidad; (iii) la naturaleza de los datos procesados; y (iv) el nivel de riesgo inherente a la actividad. Asimismo, consideramos conveniente diferenciar las obligaciones según la categoría de entidad, lo cual permitiría una aplicación proporcional y efectiva de las medidas de protección de datos personales.</p>	Aceptada	Se precisará el ámbito de aplicación de la norma
2	Bold Co S.A.S. y Bold Capital S.A.S.	<p>Instrucciones 1 y 2. Sobre el criterio de necesidad que se incluye para el tratamiento de datos.</p> <p>Las Instrucciones 1 y 2 establecen que el tratamiento de datos debe limitarse a aquellos que sean pertinentes, adecuados y necesarios para cumplir con finalidades legítimas. Este enfoque busca fortalecer la protección de los derechos de los titulares en el ecosistema fintech. Entendemos que estas instrucciones desarrollan el principio de finalidad establecido en la Ley 1581 de 2012, y por lo tanto consideramos que el Proyecto de Circular representa una oportunidad para precisar el alcance de este principio en el sector fintech. Para las entidades que prestan servicios financieros digitales, las finalidades legítimas necesariamente incluyen: (i) prevención de fraude y suplantación de identidad; (ii) seguridad de las transacciones; (iii) prevención de lavado de activos y financiación del terrorismo; (iv) cumplimiento de obligaciones regulatorias de conocimiento del cliente; y (v) gestión de riesgos operacionales y cibernéticos, entre otros.</p> <p>Reconocer expresamente estas finalidades como legítimas en el contexto fintech permitiría a las entidades implementar controles de seguridad adecuados con certeza jurídica, logrando el equilibrio necesario entre la minimización de datos y la protección efectiva de los consumidores financieros. Esto resulta especialmente relevante en un entorno donde las amenazas digitales evolucionan constantemente y representan riesgos significativos tanto para las entidades como para los usuarios del sistema financiero.</p>	No aceptada	No es adecuado establecer una lista taxativa o enunciativa de finalidades en tanto estas dependen del modelo de negocio de cada compañía
3	Bold Co S.A.S. y Bold Capital S.A.S.	<p>Consideraciones sobre la instrucción 3.</p> <p>La Instrucción 3 establece requisitos detallados sobre la información que debe proporcionarse al titular previo a la recolección de datos, incluyendo la especificación de cada acceso a funcionalidades del dispositivo. Si bien la transparencia es fundamental, consideramos que el nivel de granularidad propuesto podría generar dificultades operativas que afecten la experiencia del usuario y la prestación efectiva de los servicios financieros digitales.</p> <p>Requerir autorización específica para cada acceso individual (ubicación, cámara, galería) de manera detallada podría resultar en procesos de autorización excesivamente complejos que desincentiven el uso de servicios financieros digitales. Esta situación podría ser contraproducente, alejando a los usuarios de canales seguros y regulados hacia alternativas informales con menores estándares de protección.</p> <p>Por lo anterior, sugerimos respetuosamente que la instrucción se oriente hacia garantizar que los consumidores tengan claridad sobre qué categorías de datos son necesarias para la prestación del servicio y con qué finalidades específicas, sin requerir una granularidad de autorización por cada funcionalidad técnica. Este enfoque permitiría cumplir con el principio de transparencia establecido en la normativa de protección de datos, mientras se mantiene la operatividad necesaria para la prestación ágil y segura de servicios financieros digitales.</p>	No aceptada	<p>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:</p> <ul style="list-style-type: none"> •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. <p>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.</p>

4	Bold.Co S.A.S. y Bold Capital S.A.S.	<p>Consideraciones sobre las instrucciones 4, 6 y 7 en relación con el uso de datos sensibles</p> <p>La Instrucción 6 establece una prohibición de condicionar servicios financieros al suministro de datos biométricos, mientras que la Instrucción 7 señala que la recolección de estos datos debe ser excepcional. Consideramos importante revisar esta aproximación a la luz de las tendencias internacionales en el sector financiero, donde la biometría se ha posicionado como una herramienta clave para la protección de los consumidores.</p> <p>La autenticación biométrica se ha consolidado como el estándar internacional para la verificación de identidad en servicios financieros. En un contexto donde el fraude digital se ha incrementado en un 45% entre 2023 y 2024, desincentivar las herramientas más efectivas de prevención resulta contraproducente.</p> <p>Adicionalmente, con la sofisticación del fraude a través de nuevas herramientas como los "deepfakes", el fraude habilitado por inteligencia artificial generativa se plantea como la gran próxima amenaza en materia de seguridad para los mismos consumidores. Frente a estas nuevas amenazas, la biometría con detección de vida es una de las pocas defensas efectivas.</p> <p>Su prohibición en términos como los expuestos en la Instrucción 6 dejan a los consumidores y entidades que prestan servicios financieros vulnerables a este tipo de ataques.</p> <p>Por lo anterior, sugerimos respetuosamente que la redacción de estas instrucciones se oriente hacia garantizar la adecuada finalidad en la recolección de datos biométricos, reconociendo su importancia para la seguridad del ecosistema financiero. Asimismo, respecto a la Instrucción 7, consideramos que el requisito de informar detalladamente sobre cada tipo de dato sensible podría afectar la experiencia del usuario sin aportar valor significativo a su protección. La instrucción debería propender por la transparencia sobre las categorías de datos sensibles y sus finalidades, sin requerir un nivel de granularidad que haga inoperante el proceso de autorización.</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, si no que retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece:</p> <p>"Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. (...) Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles".</p>
5	Bold.Co S.A.S. y Bold Capital S.A.S.	<p>Comentarios a la instrucción 9</p> <p>La Instrucción 9 aborda las decisiones basadas en tratamiento automatizado de datos personales, estableciendo derechos de información e impugnación para los titulares. Al respecto, consideramos importante precisar que en el sector fintech los procesos de decisión automatizada implementan reglas y criterios previamente definidos por equipos humanos especializados.</p> <p>En efecto, las decisiones automatizadas en servicios financieros son el resultado de políticas establecidas por las entidades según su apetito de riesgo, mercado objetivo y estrategia comercial. Los modelos de scoring crediticio, límites de exposición y parámetros de aceptación de clientes son definidos, monitoreados y ajustados por profesionales en gestión de riesgos, cumpliendo con estándares técnicos y regulatorios específicos del sector financiero.</p> <p>Para las entidades vigiladas por la Superintendencia Financiera de Colombia (sobre las que no habría claridad si están cobijadas por el Proyecto de Circular), estos procesos de decisión ya se encuentran regulados y supervisados por dicha entidad. La normativa de la Superfinanciera establece requerimientos detallados sobre modelos de otorgamiento de crédito, sistemas de administración de riesgos y procedimientos de vinculación de clientes que incluyen la revisión y validación de herramientas automatizadas de decisión.</p> <p>Por lo anterior, sugerimos respetuosamente que la implementación de esta instrucción considere las competencias y regulaciones existentes en materia financiera, particularmente para entidades vigiladas que ya cuentan con marcos normativos específicos sobre la materia. Esto permitiría evitar duplicidades regulatorias y garantizar coherencia en la supervisión del sector financiero.</p>	Aceptada	Se eliminará la instrucción 9
6	Bold.Co S.A.S. y Bold Capital S.A.S.	<p>Régimen de transición</p> <p>Las instrucciones contenidas en el Proyecto de Circular implican ajustes tecnológicos y operativos que pueden representar cambios significativos para las empresas del sector fintech.</p> <p>La implementación de nuevos procedimientos, actualización de sistemas y modificación de flujos de autorización requiere tiempo considerable de desarrollo, pruebas y despliegue.</p> <p>Por lo anterior, sugerimos respetuosamente establecer un régimen de transición que permita a las entidades realizar las adecuaciones necesarias de manera ordenada. Consideramos que un plazo de al menos un año desde la publicación de la Circular sería apropiado, particularmente para aquellas instrucciones que impliquen modificaciones a prácticas actuales del mercado que se encuentran alineadas con la normativa vigente y que ahora serán reguladas con mayor detalle.</p>	No aceptada	No se incluye periodo de transición, debido a que se elimina instrucciones relativas a adecuaciones de sistemas de información
7	Certicámara	<p>Comentarios a la instrucción 3</p> <p>Se sugiere revisar la redacción en el apartado correspondiente al consentimiento, específicamente en lo relacionado con el tratamiento de datos personales sensibles, para garantizar coherencia con el estándar legal vigente y el numeral 6 de la presente circular.</p> <p>Por último, se recomienda mencionar ejemplos de buenas prácticas aplicables.</p> <p>En ese sentido, proponemos que se incluya expresamente que el consentimiento para el tratamiento de datos sensibles debe ser "expreso, previo y por escrito", tal como lo establece el artículo 6 de la Ley 1581 de 2012. A su vez, podría mantenerse la referencia a que este consentimiento debe ser inequívoco en el contexto general de los demás tipos de datos, pero diferenciando claramente los requisitos reforzados cuando se trata de información sensible.</p>	Parcialmente aceptada	Se ajustó la redacción de esta instrucción
8	Certicámara	<p>Comentarios a la instrucción 5</p> <p>Desde la perspectiva de los servicios prestados por Certicámara S.A., tanto de forma directa como mediante terceros, se resalta la importancia de que el proyecto de circular distinga claramente entre:</p> <p>a. Finalidades estrictamente necesarias para la prestación del servicio (ej. verificación de identidad, emisión de firma digital, autenticación biométrica), y</p> <p>b. Finalidades adicionales o accesorias, como contacto para fines comerciales, marketing o alianzas estratégicas.</p> <p>Si bien el numeral 5 acierta al exigir que el consentimiento para finalidades adicionales sea diferenciado, sugerimos reforzar la claridad en dos aspectos:</p> <p>1. Uso de mecanismos diferenciados y explícitos por finalidad:</p>	Parcialmente aceptada	Se ajustó la redacción de esta instrucción
9	Certicámara	<p>Comentarios a la instrucción 6</p> <p>Se pone de presente a la SIC que esto constituye una restricción para servicios en los que sólo se dispone de mecanismos de validación a través de datos biométricos. Además deberá tenerse en cuenta que acá se está parametrizando que la autorización de datos sensibles se haga por escrito o por mensaje de datos. Se sugiere su armonización con el numeral 4 para que se trate coherencia en los mecanismos.</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos y se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas.</p> <p>En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, sino que retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece:</p> <p>"Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley. (...) Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles".</p>
10	Certicámara	<p>Comentarios a la instrucción 8</p> <p>Se sugiere a la SIC precisar que la obligación de informar sobre el uso de tecnologías automatizadas debe ser proporcional al impacto que tenga la automatización sobre los derechos del titular. Por ejemplo, para verificación de identidad mediante huella digital y la autenticación, que implica una decisión automatizada con efectos significativos. Contrario a lo anterior, la automatizaciones operativas pueden no tener efectos jurídicos y decisiones automatizadas con consecuencias jurídicas o similares (ej. aprobación o rechazo de productos financieros).</p> <p>Texto sugerido (adición normativa):</p> <p>"La obligación de informar sobre tecnologías automatizadas deberá aplicarse en especial cuando dichas tecnologías conduzcan a decisiones que produzcan efectos jurídicos o afecten de manera significativa al titular, conforme a criterios de proporcionalidad"</p> <p>Esto es importante para Certicámara, ya que 1) evita que se exijan explicaciones extensas que son procesos automáticos pero no decisivos. 2) Protege la experiencia de usuario evitando sobrecargar los mensajes de consentimiento.</p> <p>3) Define límites frente a exigencias regulatorias futuras sobre explicabilidad algorítmica.</p>	No aceptada	<p>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.</p>
11	Certicámara	<p>Comentarios a la instrucción 9</p> <p>Se reitera que ante la posibilidad de la impugnación se diferencie tanto en el numeral 8 como en el 9 entre tecnologías automatizadas de soporte y aquellas que conducen a decisiones que generan efectos jurídicos o sustanciales sobre los titulares.</p>	Aceptada	Se elimina la instrucción 9 así como la impugnación frente a decisiones automatizadas.
12	Certicámara	<p>Comentarios a la instrucción 10</p> <p>Se valora positivamente el enfoque integral adoptado en este numeral, que recoge medidas tecnológicas, humanas y contractuales, así como la obligación de actualización periódica conforme al riesgo y al estado del arte.</p> <p>Sin embargo, se sugiere aclarar que el principio de proporcionalidad debe guiar la implementación de las medidas de seguridad, especialmente para actores de menor escala tecnológica o con modelos operativos limitados, evitando cargas excesivas.</p> <p>Texto sugerido (complementario):</p> <p>"Las medidas deberán ser razonables y proporcionales considerando la capacidad operativa del actor, sin perjuicio de las obligaciones de seguridad exigidas por la ley."</p> <p>Esto facilitaría la implementación gradual y realista por parte de actores pequeños del ecosistema fintech, sin debilitar el estándar de seguridad.</p>	No aceptada	Los responsables, encargados, fuentes, operadores y usuarios deben cumplir con la legislación nacional en igualdad de condiciones

13	Certicámara	<p>Comentarios a la instrucción 12 Se valora positivamente la inclusión de obligaciones específicas sobre trazabilidad de accesos realizados por terceros autorizados por el titular. Este deber ya se encuentra implementado por entidades vigiladas por la Superintendencia Financiera, conforme a lo establecido en la Circular Básica Jurídica (C.E. 029 de 2014), y ha sido trasladado contractualmente a proveedores tecnológicos.</p> <p>No obstante, se sugiere que el numeral precise: Que los registros podrán ser llevados por el responsable, el encargado o ambos, conforme a las obligaciones contractuales vigentes, siempre que se garantice su disponibilidad frente a los titulares y autoridades. Que los registros podrán adaptarse a modelos de trazabilidad automatizada y transaccional, en aquellos casos donde la frecuencia de acceso lo justifique, sin desdibujar la trazabilidad exigida por la autoridad.</p>	No aceptada	Se eliminará la instrucción 12
14	Certicámara	<p>Comentarios a la instrucción 13 Se valora positivamente la incorporación del enfoque de diseño legal orientado al usuario como herramienta para fortalecer el principio de transparencia y el ejercicio de derechos por parte de los titulares.</p> <p>No obstante, se recomienda precisar que la implementación de mecanismos de gestión de privacidad deberán ser diferenciados para evitar exigir funcionalidades técnicas que no son aplicables o necesarias en todos los contextos.</p> <p>Adicionalmente, se recomienda mayor precisión en la definición de información "clara y suficiente".</p>	Aceptada	Se eliminará la expresión "diseño legal"
15	Certicámara	<p>Comentarios a la instrucción 15 Se valora positivamente la introducción de un enfoque proactivo de educación y sensibilización del titular, alineado con el principio de responsabilidad demostrada.</p> <p>No obstante, se sugiere que el numeral precise que el deber recae sobre el responsable del tratamiento de los datos personales, quien es el directamente vinculado al titular. Los encargados podrán apoyar esta labor cuando sea parte del alcance contractual.</p> <p>Así mismo, se recomienda que la SIC clarifique qué tipo de mecanismos podrían considerarse "accesibles y continuos" y qué nivel de trazabilidad se espera en la medición de impacto, permitiendo adaptabilidad conforme al tamaño, recursos y modelo de negocio del actor fintech.</p> <p>Texto complementario sugerido: "La definición de mecanismos accesibles y continuos deberá ser proporcional al tipo de servicio, canal de interacción y capacidad del actor, pudiendo incluir medios digitales, campañas visuales, mensajes dentro de la aplicación o cualquier otro canal que garantice comprensión efectiva por parte del titular."</p>	Parcialmente aceptada	Se ajustó la redacción de la instrucción 8
16	Certicámara	<p>Comentarios a la instrucción 16 Se valora positivamente la inclusión del criterio funcional para calificar a un actor como responsable, aun cuando esté formalmente designado como encargado, por cuanto permite evitar simulaciones contractuales y garantiza la aplicación sustancial del régimen. Se sugiere a la SIC revisar el uso del término "contrato de transmisión", ya que la Ley 1581 de 2012 y el Decreto 1074 de 2015 no exigen formalmente esa denominación, sino que establecen la obligación de formalizar las condiciones bajo las cuales un encargado realiza el tratamiento por cuenta del responsable.</p> <p>Así mismo, se recomienda que se aclare que dicha formalización puede hacerse mediante un contrato independiente o una cláusula dentro de un contrato principal, o incluso las normas corporativas vinculantes.</p>	No aceptada	El contrato de transmisión de datos personales se encuentra establecido en el artículo 25 del Decreto 1377 de 2013. Es considerado una medida proactiva en el manejo de la información personal por parte del Encargado del Tratamiento. Este es un contrato accesorio al contrato principal del contrato celebrado entre responsable y encargado, y también puede cumplirse dichos requisitos a través de cláusulas específicas plasmadas en el contrato principal.
17	Certicámara	<p>Comentarios a la instrucción 17 Se valora positivamente la estructura jerárquica y gradual del presente numeral, la cual facilita el cumplimiento normativo frente a operaciones internacionales de tratamiento de datos personales.</p> <p>No obstante, se sugiere que el numeral incluya una precisión técnica sobre la diferencia entre transferencia y transmisión internacional, remitiendo a las definiciones oficiales de la SIC, para evitar ambigüedades en su aplicación práctica, especialmente en modelos tecnológicos apalancados en la nube.</p> <p>Así mismo, se propone que se mencione expresamente que la suscripción de cláusulas contractuales modelo o equivalentes constituye una medida válida para acreditar estándares de protección en jurisdicciones sin reconocimiento previo de adecuación, tal como se menciona en el numeral 18.</p>	No aceptada	No se considera oportuno aclarar la diferencia entre transmisión y transferencia en tanto dichas definiciones se encuentran en el Decreto 1377 de 2013. No se acepta la inclusión de cláusulas contractuales modelo o equivalentes, pues el numeral siguiente ya contiene dicha disposición y hacerlo sería reiterativo.
18	Certicámara	<p>Comentarios a la instrucción 18 Se recomienda a la SIC aclarar que la suscripción de las Cláusulas Contractuales Modelo es una buena práctica sugerida, pero no constituye el único mecanismo válido para cumplir con el principio de responsabilidad demostrada en transferencias internacionales de datos.</p> <p>Así mismo, se propone permitir que las entidades ajusten dichas cláusulas a su realidad contractual, siempre que se respete el estándar de protección equivalente exigido por la legislación colombiana.</p> <p>Texto propuesto (adicción normativa): "Las cláusulas contractuales podrán ser adaptadas por los responsables o encargados del tratamiento, siempre que conserven el estándar adecuado de protección y permitan demostrar responsabilidad demostrada."</p>	No aceptada	La suscripción de las Cláusulas Contractuales Modelo es una buena práctica sugerida y así se establece en la instrucción, no es un criterio establecido de manera obligatoria. El numeral anterior ya contiene otros mecanismos válidos para cumplir con el principio de responsabilidad demostrada en transferencias internacionales de datos. Además, es pertinente aclarar que las Cláusulas Contractuales Modelo son las incluidas en la "Guía de implementación de cláusulas contractuales modelo para la Transferencia internacional de Datos personales (TIDP)" de la Red Iberoamericana de Protección de Datos y su anexo "Modelo de Cláusulas Contractuales", en ese sentido, no se considera apropiado su ajuste.
19	UcreditSkills S.A.S.	<p>Comentarios a la instrucción 9 Celebramos el reconocimiento de las decisiones automatizadas como parte integral del modelo Fintech. No obstante, sugerimos que la circular aclare la distinción entre decisiones 'exclusivamente automatizadas' y 'automatizadas con intervención humana'. Esto es clave para evitar interpretaciones restrictivas.</p> <p>En Europa, el Reglamento General de Protección de Datos (GDPR) permite decisiones automatizadas siempre que exista intervención humana significativa en la revisión. Proponemos adoptar una definición similar y establecer un umbral técnico claro. Además, sugerimos incorporar la obligación de informar explícitamente al titular cuando una decisión automatizada afecte significativamente sus derechos (ej., negación de crédito)</p>	Aceptada	Se eliminará la instrucción 9
20	UcreditSkills S.A.S.	<p>Comentarios a la instrucción 4 La segmentación del consentimiento por finalidad es una buena práctica, pero su aplicación rígida puede afectar la experiencia de usuario digital. Sugerimos incorporar el concepto de 'consentimiento contextualizado', utilizado por la Agencia Española de Protección de Datos, que permite agrupar finalidades accesorias cuando tienen coherencia funcional y bajo nivel de riesgo. Esto evitaría la saturación de pantallas emergentes o formularios excesivos que desincentiven al usuario a completar procesos de onboarding digital.</p>	Aceptada	Se reformuló la instrucción de acuerdo al comentario
21	UcreditSkills S.A.S.	<p>Solicitamos aclaración sobre si tecnologías de autenticación no invasivas como OTP, behavioral biometrics (ej. dinámica de tipo, patrones de navegación) o validación facial pasiva, son consideradas datos biométricos bajo esta Circular.</p> <p>En países como Reino Unido, la ICO aclara que solo se considera dato biométrico aquel que permite identificar de forma inequívoca a una persona. Proponemos incorporar este criterio y definir los límites de 'dato sensible biométrico' para evitar inseguridad jurídica en el desarrollo de tecnologías de validación.</p>	No aceptada	La circular no trata de este asunto
22	UcreditSkills S.A.S.	<p>Comentarios a la instrucción 17 Recomendamos que la Circular incluya un listado dinámico de países con nivel adecuado de protección de datos personales, similar al listado de la Comisión Europea. Esto facilitaría la gestión de transferencias transfronterizas, especialmente con proveedores SaaS ubicados en EE.UU., México, Brasil y otros países estratégicos.</p> <p>Así mismo, solicitamos que se habilite una herramienta tipo repositorio o sandbox regulatorio donde las empresas puedan consultar cláusulas contractuales tipo ya avaladas por la SIC.</p>	No aceptada	Dicho listado ya se encuentra en otra circular de la SIC
23	UcreditSkills S.A.S.	<p>Comentarios a la instrucción 12 La trazabilidad es esencial, pero en ambientes altamente digitalizados, como los servicios Fintech basados en API, llevar un registro detallado de cada acceso a nivel de dato individual puede generar una carga técnica desproporcionada.</p> <p>Sugerimos permitir la implementación de logs por transacción o por lote, conforme a los estándares de auditoría interna y mejores prácticas de ciberseguridad como ISO 27001.</p>	Aceptada	Se eliminará la instrucción 12
24	UcreditSkills S.A.S.	<p>Comentarios a la instrucción 8 Valoramos el enfoque de accesibilidad y claridad en el lenguaje de los formularios. Recomendamos que la SIC adopte una guía de "UX legal" o buenas prácticas, como lo hace la CNIL de Francia, que evalúa cómo debe presentarse el consentimiento de manera legal y amigable.</p> <p>Además, sería útil permitir validaciones voluntarias por parte de grupos de usuarios o testers acreditados que certifiquen la comprensibilidad de los formularios digitales</p>	No aceptada	No se considera oportuno limitar por medio de un único instrumento el cumplimiento de las obligaciones legales

25	UcreditSkills S.A.S.	<p><u>Comentarios a la instrucción 3</u></p> <p>Solicitamos que la Circular aclare que el acceso a funcionalidades del dispositivo (como cámara o micrófono) será legal cuando sea solicitado contextualmente, durante la prestación del servicio, y con consentimiento específico y temporal.</p> <p>Esto es consistente con los modelos de consentimiento dinámico utilizados en Estados Unidos y Europa, donde se permite acceso funcional siempre que el usuario esté informado y dé su autorización explícita en el momento del uso.</p>	Parcialmente aceptada	Se ajustó la redacción de esta instrucción
26	UcreditSkills S.A.S.	<p>La aplicación uniforme de las instrucciones puede resultar ambigua dada la diversidad de modelos Fintech. Un originador de crédito no opera bajo los mismos flujos de datos que una billetera digital o una insurtech.</p> <p>Proponemos que la SIC emita guías diferenciadas por tipo de Fintech, con ejemplos prácticos y matrices de cumplimiento específicas. Esto facilitaría la implementación adecuada y evitaría el uso genérico de cláusulas que no se ajusten al contexto de cada modelo de negocio.</p>	No aceptada	El régimen de protección de Datos Personales debe ser garantizado y cumplido por todos los sujetos obligados, independientemente del tipo de Fintech
27	UcreditSkills S.A.S.	<p><u>Comentarios a la instrucción 9</u></p> <p>La circular impone límites generales a la toma de decisiones automatizadas sin intervención humana, lo cual, si bien busca proteger al titular, entra en tensión con los principios de eficiencia, escalabilidad e inclusión financiera que impulsa el open finance. Modelos como scoring alternativo, asesoría financiera automatizada (robo-advisors) y comparadores digitales requieren de procesamiento automático de datos. Considero que el foco regulatorio debe estar en garantizar transparencia algorítmica y explicabilidad, no en limitar su uso por se.</p>	Aceptada	Se eliminará la instrucción 9
28	Abroad Financial Technologies	<p><u>Comentarios a la instrucción 4</u></p> <p>Se observa una exigencia de formas de consentimiento previas, expresas e incluso escritas, que no se ajustan a los modelos digitales interoperables que demanda el open finance. El ecosistema requiere consentimiento digital, trazable y revocable, como lo propone el proyecto de decreto del Ministerio de Hacienda. Este tipo de exigencias formales pueden convertirse en barreras de entrada y generar inseguridad jurídica para las plataformas tecnológicas.</p>	Parcialmente aceptada	Se ajustó la redacción de esta instrucción
29	Abroad Financial Technologies	<p><u>Comentarios a la instrucción 2</u></p> <p>Si bien la minimización es un principio fundamental de protección de datos, su aplicación restrictiva puede limitar el desarrollo de soluciones que dependen del análisis holístico del perfil financiero del consumidor. El open finance parte de la premisa de que el usuario es dueño de sus datos y puede decidir libremente compartirlos de manera amplia si así lo desea, con terceros autorizados. Limitar este derecho en nombre de una sobreprotección puede restringir el ejercicio de la autonomía del titular y frenar el desarrollo de servicios más personalizados y útiles.</p>	No aceptada	El principio de minimización exige que únicamente se haga tratamiento de los datos personales que sean necesarios para las finalidades constitucionalmente legítimas. No se trata de una prohibición a la recolección o circulación de datos personales.
30	Abroad Financial Technologies	<p>El enfoque de la circular mantiene una visión bilateral clásica de "responsable y encargado", sin consideración del nuevo esquema de gobernanza sectorial e interoperable que propone el marco de open finance. Esta desconexión genera el riesgo de "doble ventanilla regulatoria" y puede dificultar la implementación técnica y operativa de un sistema que requiere coordinación institucional entre la SIC y la Superintendencia Financiera.</p>	No aceptada	No se está creando una regulación contradictoria con el esquema de finanzas abiertas. Todo lo contrario, se busca articular la regulación del sector financiero mediado por las tecnologías con los altos estándares de protección de datos que exige el esquema de finanzas abiertas.
31	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No. 2: La prohibición de que las aplicaciones de las entidades fintech soliciten acceso a datos como la galería o los contactos, aunque entendemos busca aplicar el principio de minimización, resulta general y no contempla el trasfondo técnico, ya que existen usos legítimos y proporcionales —como en transferencias P2P que se espera sean cada vez más comunes con la entrada en operación de Bre-B— que mejoran la experiencia del usuario y cuentan con su consentimiento informado. Esta restricción puede limitar la innovación y afectar la competitividad frente a aplicaciones extranjeras.</p> <p>Por ello, se recomienda permitir dichos accesos cuando estén debidamente justificados, sean funcionalmente necesarios y el usuario los autorice de forma clara. Preocupa en gran medida que la Superintendencia disponga ex-ante que no existen modelos de negocios, servicios, empresas multiservicio (que presenten servicios Fintech y otros servicios adicionales) o futuras aplicaciones en las que el acceso a ciertos datos no sea necesario o útil, especialmente en este tipo de industrias disruptivas como la Fintech que se encuentran en constante evolución e innovación.</p> <p>En ejercicio de las funciones de inspección, vigilancia y control, destacamos que la autoridad debiera determinar, caso a caso, y previo ejercicio del derecho de defensa, si un tratamiento particular fue legítimo. Declarar como contrario a la ley el tratamiento de ciertos datos a un sector de la economía o modelo de negocio incluso con autorización de su titular podría constituir, una discriminación en contra de los actores del "ecosistema Fintech" y un posible prejuzgamiento de futuros casos.</p>	Parcialmente aceptada	<p>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".</p> <p>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.</p> <p>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 del servicio ofrecido, su tratamiento se considera excesivo y, por tanto, contrario a la ley.</p>
32	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No. 5. Esta instrucción introduce una exigencia no prevista en la ley respecto al otorgamiento de la autorización por parte del titular. La normativa aplicable, en particular el artículo 5 del Decreto 1377 de 2013 y el artículo 12 de la Ley 1581 de 2012, exige que el Responsable del Tratamiento informe de manera clara y expresa los datos personales que serán recolectados, el tratamiento al cual serán sometidos y la finalidad de este. Si bien es cierto que las finalidades adicionales a las estrictamente necesarias para la prestación del servicio deben ser informadas al titular al momento de solicitar su autorización, la normativa no contempla la necesidad de segmentar o fraccionar la autorización del titular frente a dichas finalidades.</p> <p>Desde una perspectiva práctica, exigir una autorización diferenciada para cada finalidad adicional impone una carga operativa y técnica significativa para los actores del ecosistema fintech, cuyos modelos de negocio se fundamentan en el uso ágil y eficiente de tecnologías para personalizar servicios financieros, mejorar la experiencia del usuario y generar valor a partir del análisis de datos. Esta exigencia ralentizaría procesos clave como el onboarding digital o la activación de servicios complementarios, y afectaría la interoperabilidad de plataformas y el desarrollo de innovaciones basadas en análisis predictivo y automatización.</p> <p>Vemos que no sería procedente imponer esta obligación, ya que representa una carga no prevista por la ley de protección de datos personales ni por su reglamentación. Pues, aunque esta propuesta se alinea con estándares como el RGPD europeo, su adopción inmediata y obligatoria en el contexto colombiano genera preocupaciones:</p> <ol style="list-style-type: none"> 1. Desarticula modelos de negocio basados en ecosistemas integrados, donde múltiples sociedades de un mismo grupo (e.g. pagos, créditos, logística) comparten información bajo un consentimiento general y una infraestructura común. 2. Disminuye significativamente la tasa de aceptación para usos como perfilamiento, marketing o alianzas, lo cual impacta directamente en ingresos, funcionalidades y personalización de los servicios. 	Parcialmente aceptada	Se reformuló la instrucción de acuerdo al comentario

33	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No. 6. La prohibición de condicionar el acceso a servicios financieros al suministro de datos biométricos, prevista en el numeral 6 del proyecto, si bien busca proteger el derecho al habeas data, desconoce la realidad operativa y regulatoria del sector financiero, donde la biometría es esencial para validar identidades en entornos digitales, prevenir fraudes y cumplir con obligaciones legales de KYC y LA/FT. Esta restricción, al ignorar el principio de proporcionalidad y sin prever excepciones para casos justificados, podría comprometer la seguridad del ecosistema financiero y generar conflictos normativos con directrices vigentes como la Circular Externa 029 de 2019 de la SFC. Se recomienda, por tanto, permitir su uso en condiciones específicas y bajo salvaguardas adecuadas o, por lo menos, que la Superintendencia reconozca que el análisis de la aplicación de la prohibición debe hacerse caso a caso.</p> <p>Agradecemos considerar que, los datos biométricos son herramientas esenciales para:</p> <ol style="list-style-type: none"> 1. Garantizar una verificación robusta de identidad en entornos 100% digitales, donde no existe presencialidad. 2. Prevenir suplantaciones, fraudes digitales y toma de cuentas (ATO). 3. Cumplir con normativas sobre conocimiento del cliente (KYC) y prevención de LA/FT, emitidas por la Superintendencia Financiera de Colombia (SFC). <p>La Circular Externa 029 de 2019 de la SFC reconocen el uso de la biometría como una medida idónea de autenticación reforzada para transacciones no presenciales. Las razones que justifican este tipo de medidas en el sistema financiero son plenamente aplicables al ecosistema fintech, en donde, se reitera, resultan fundamentales dada la naturaleza digital y no presencial de sus servicios. Su prohibición generalizada no solo reduce los niveles de seguridad, sino que expone a los actores del sistema financiero a mayores brechas regulatorias, incluyendo el incumplimiento de estándares del GAFI sobre identificación digital y debida diligencia del cliente.</p> <p>El alcance de los procedimientos de conocimiento del cliente en Colombia, para las entidades vigiladas por la Superintendencia Financiera de Colombia, ha sido establecido principalmente en la PARTE I – TÍTULO IV – CAPÍTULO IV numeral 4.2.2.1.8. y 4.2.2.2.1.1.1 de la Circular Básica Jurídica, donde dicha norma especial ha resaltado la necesidad de adelantar una adecuada y efectiva gestión del riesgo LA/FT conforme a su análisis de riesgo LA/FT incluyendo entre sus procedimientos y política la verificación efectiva de la identidad de los potenciales clientes al momento de su vinculación utilizando datos e información de fuentes confiables e independientes. En este sentido para dichos efectos, las entidades vigiladas pueden utilizar biometría, conforme a las instrucciones impartidas por esta Superintendencia en el Capítulo I del Título II de la Parte I de esta CBJ.</p>	Parcialmente aceptada	Se reformuló la instrucción de acuerdo al comentario
34	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No. 7. Manifestamos que el apartado según el cual el tratamiento de datos personales sensibles debe ser excepcional, constituye una instrucción que no encuentra sustento en la ley vigente de protección de datos personales ni en sus normas reglamentarias. La ley permite a los responsables tratar datos sensibles en cumplimiento de los requisitos aplicables, sin establecer que dicho tratamiento deba ser excepcional</p>	No aceptada	La legislación colombiana sí contempla que el tratamiento de datos personales sensibles es excepcional. De ahí que el artículo 6 de la Ley 1581 de 2012 contemple una prohibición general con algunas excepciones.
35	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No. 12. Solicitamos respetuosamente tener en cuenta que ni la Ley 1581 de 2012 ni el Decreto 1377 de 2013 establecen como obligación para los responsables y/o encargados llevar este tipo de registro. En consecuencia, mediante una circular externa, la SIC estaría creando nuevas obligaciones y excediendo sus competencias legales, tal como se explicó al inicio del presente documento</p>	Aceptada	Se eliminará la instrucción 12
36	Cámara Colombiana de Comercio Electrónico	<p>Lineamiento No 13. "Los responsables y encargados deberán implementar estrategias de diseño legal orientadas a mejorar la comprensión del titular sobre el uso de su información personal (...)".</p> <p>A pesar de que los responsables y encargados tienen la obligación legal de suministrar información a los titulares respecto del tratamiento que se le da a su información personal, el marco de protección de datos personales vigente no establece que se deban utilizar estrategias de "diseño legal" para "mejorar la comprensión del titular sobre el uso de su información personal".</p>	Aceptada	Se eliminará la expresión "diseño legal"
37	Cámara Colombiana de Informática y Telecomunicaciones	<p>El uso reiterado de la expresión "finalidades constitucionales legítimas", sin definición precisa, puede derivar en inseguridad jurídica e interpretaciones restrictivas por parte de la autoridad. Las finalidades del tratamiento deben evaluarse caso a caso con base en criterios de necesidad, proporcionalidad y expectativa razonable del titular, conforme al principio de responsabilidad demostrada.</p> <p>En ese orden de ideas, se sugiere precisar la expresión por expresiones como: finalidades legales, contractuales o legítimas según el caso concreto, o alinearla con normas comparadas.</p>	No aceptada	<p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p>
38	Cámara Colombiana de Informática y Telecomunicaciones	<p><u>Comentarios a la instrucción 5</u></p> <p>En relación con lo establecido en este numeral, en el que se establece que "dicha autorización deberá otorgarse de manera diferenciada", consideramos necesario que la autoridad precise el alcance de dicha disposición. En particular, resulta indispensable que se aclare qué "autorizaciones diferenciadas" y "finalidades diferenciadas". Esto con el fin de determinar si ello implica la obligación de presentar solicitudes de autorización separadas para cada finalidad que no se encuentre directamente relacionada con el servicio principal ofrecido, así como permitir al titular decidir de manera individual respecto de cada una de estas finalidades.</p> <p>Lo anterior, en tanto que el marco normativo vigente establece la obligación de informar al titular sobre las finalidades del tratamiento de sus datos personales y de obtener su autorización, sin que ello se traduzca necesariamente en una obligación de recabar autorizaciones de forma fraccionada por cada finalidad.</p> <p>Esta instrucción introduce una exigencia no prevista en la Ley respecto al otorgamiento de la autorización por parte del titular. La normativa aplicable, en particular el artículo 5 del Decreto 1377 de 2013 y el artículo 12 de la Ley 1581 de 2012, únicamente exige que el Responsable del Tratamiento informe de manera clara y expresa los datos personales que serán recolectados, el tratamiento al cual serán sometidos y la finalidad del mismo. Si bien es cierto que las finalidades adicionales a las estrictamente necesarias para la prestación del servicio deben ser informadas al titular al momento de solicitar su autorización, la normativa no contempla la necesidad de segmentar o fraccionar la autorización del titular frente a dichas finalidades. Desde una perspectiva práctica, exigir una autorización diferenciada para cada finalidad adicional impone una carga operativa y técnica significativa para los actores del ecosistema fintech, cuyos modelos de negocio se fundamentan en el uso ágil y eficiente de tecnologías para personalizar servicios financieros, mejorar la experiencia del usuario y generar valor a partir del análisis de datos. Esta exigencia ralentizaría procesos clave como el onboarding digital o la activación de servicios complementarios, y afectaría la interoperabilidad de plataformas y el desarrollo de innovaciones basadas en análisis predictivo y automatización.</p> <p>Por lo anterior, consideramos que no es pertinente imponer esta obligación, ya que representaría una carga no prevista por la Ley de protección de datos personales ni por su reglamentación</p>	Parcialmente aceptada	<p>Se ajustó la redacción de esta instrucción. 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.</p> <p>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:</p> <ul style="list-style-type: none"> -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. <p>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.</p> <p>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.</p> <p>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:</p>
39	Cámara Colombiana de Informática y Telecomunicaciones	<p><u>Comentarios a la instrucción 6</u></p> <p>Consideramos que debe existir un adecuado equilibrio entre la protección de los datos personales y la necesidad de validar la identidad del usuario. Si bien coincidimos en que no debe condicionarse la prestación del servicio a la entrega de datos biométricos, también debe evitarse una interpretación que impida la implementación de mecanismos de verificación adecuados, teniendo en cuenta los riesgos de suplantación. En el caso de los servicios prestados por actores del sistema Fintech, la validación de identidad es un elemento esencial para la seguridad de las operaciones.</p> <p>Adicionalmente, exigir autorización escrita o por mensaje de datos para datos sensibles puede desconocer la validez de los consentimientos digitales o trazables mediante logs, tokens o mecanismos de trazabilidad, comunes en operaciones móviles. En ese orden de ideas, se sugiere permitir mecanismos de validación digital equivalentes, siempre que haya trazabilidad, autenticación y almacenamiento seguro. El borrador de Circular exige que la autorización para datos sensibles sea por escrito o mensaje de datos, sin embargo, la Ley 1581 de 2012 no exige que sea por escrito, solo consentimiento previo, expreso e informado.</p>	Aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece:</p> <p>"Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.</p> <p>(...)</p> <p>Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles."</p>

40	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la Instrucción 7. Manifiestamos que el apartado, según el cual el tratamiento de datos personales sensibles debe ser excepcional, constituye una instrucción que no encuentra sustento en la Ley vigente de protección de datos personales ni en sus normas reglamentarias. La Ley permite a los responsables tratar datos sensibles en cumplimiento de los requisitos aplicables, sin establecer que dicho tratamiento deba ser excepcional. Por lo tanto, solicitamos la supresión de este apartado.	No aceptada	La legislación colombiana sí contempla que el tratamiento de datos personales sensibles es excepcional. De ahí que el artículo 6 de la Ley 1581 de 2012 contemple una prohibición general con algunas excepciones.
41	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la Instrucción 9. Respetuosamente proponemos eliminar la palabra 'especialmente' del texto actual por las siguientes razones. En primera instancia, la inclusión de 'especialmente' crea un derecho innecesariamente amplio para impugnar decisiones automatizadas. Si bien es fundamental proteger a los consumidores de resultados adversos basados en IA, también debemos equilibrar este objetivo con la necesidad de fomentar la innovación tecnológica en el sector fintech. Adicionalmente, muchos sistemas automatizados en servicios financieros (como notificaciones de saldo o categorización de transacciones) aportan valor sin generar consecuencias negativas. Permitir impugnaciones a estos procesos inofensivos podría crear cargas operativas innecesarias y desalentar el desarrollo de herramientas financieras útiles. Asimismo, la eliminación de 'especialmente' permitiría enfocar el derecho de impugnación en las decisiones verdaderamente relevantes - aquellas con impactos potencialmente negativos como denegaciones de crédito o cierres de cuenta.	Aceptada	Se eliminará la instrucción 9
42	Cámara Colombiana de Informática y Telecomunicaciones	Instrucción 12. Solicitamos respetuosamente la supresión de esta instrucción, ya que ni la Ley 1581 de 2012 ni el Decreto 1377 de 2013 establecen como obligación para los responsables y/o encargados del tratamiento el llevar este tipo de registro. En consecuencia, mediante una Circular externa, la SIC estaría creando nuevas obligaciones y excediendo sus competencias legales.	Aceptada	Se eliminará la instrucción 12
43	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto a las instrucciones 13 y 15. En relación con estos numerales, consideramos que los titulares también tienen el deber de mantenerse informados respecto de sus derechos en materia de protección de datos personales. Si bien se trata de un derecho fundamental, ello conlleva una responsabilidad compartida, y que no debe recaer exclusivamente sobre los responsables o encargados del tratamiento el deber de mantener permanentemente informados a los titulares, en la medida en que esto podría exceder el alcance del deber de información establecido por la normativa vigente. A pesar de que los responsables y encargados del tratamiento tienen la obligación legal de suministrar información a los titulares respecto del tratamiento que se le da a su información personal, el marco de protección de datos personales vigente no establece que se deban utilizar estrategias de "diseño legal" para "mejorar la comprensión del titular sobre el uso de su información personal".	Parcialmente aceptada	Se eliminará la expresión "diseño legal"
44	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto a la instrucción 18. Respetuosamente solicitamos eliminar este numeral, considerando que las Cláusulas Contractuales Modelo de la Red Iberoamericana no reflejan adecuadamente la diversidad de relaciones comerciales en el ecosistema fintech. Las transferencias de datos entre diferentes actores (fintechs, proveedores de software, servicios en la nube) requieren enfoques adaptados a sus circunstancias específicas.	No aceptada	La suscripción de las Cláusulas Contractuales Modelo es una buena práctica sugerida y así se establece en la instrucción
45	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la Instrucción 8. Comentarios respecto a la transparencia sobre tecnologías automatizadas. Frente a la disposición que señala que "los actores del ecosistema Fintech deberán garantizar la transparencia en el uso de tecnologías automatizadas", sugerimos respetuosamente precisar el alcance del deber de informar de manera "clara y suficiente", a fin de evitar ambigüedades que puedan dar lugar a interpretaciones dispares y exigencias desproporcionadas en la implementación de procesos automatizados.	Parcialmente aceptada	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 conciernen. 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...
46	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la Instrucción 13. Comentarios respecto a la información sobre terceros en el tratamiento de datos. En relación con el apartado que establece, como obligación del responsable, "garantizar que el titular reciba información clara y suficiente sobre los terceros que tendrán acceso a sus datos, indicando la calidad en la que actúan (responsables, encargados o terceros autorizados)", sugerimos que se precise el alcance de dicha obligación. Específicamente, consideramos necesario aclarar si esta implica identificar de manera individualizada a los terceros, incluyendo su objeto social y el rol que desempeñan, tanto al momento de obtener la autorización como ante cualquier modificación posterior; o si, por el contrario, resulta suficiente con describir las categorías, funciones u objeto social de los terceros que podrían acceder a los datos personales.	Aceptada	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.
47	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la Instrucción 15. Comentarios respecto a las acciones de sensibilización a cargo de los actores del ecosistema Fintech. El proyecto señala que "la trazabilidad sobre estas acciones podrá evidenciarse a través de indicadores y cualquier otro medio idóneo". Sugerimos delimitar con mayor precisión el alcance del término "indicador", ya que su interpretación puede generar incertidumbre en cuanto a los niveles de cumplimiento esperados. Asimismo, resultaría conveniente establecer directrices sobre los criterios mínimos que deben cumplir dichos indicadores.	Parcialmente aceptada	Se ajustó la redacción de la presente instrucción
48	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto a las definiciones incluídas en la circular. Sugerimos respetuosamente una mayor precisión en la definición de términos clave como "ecosistema Fintech", "modelos de negocio", "datos personales", "datos sensibles" y "tecnologías automatizadas", con el propósito de evitar interpretaciones ambiguas que dificulten la correcta identificación de los sujetos obligados y el alcance del proyecto regulatorio.	Parcialmente aceptada	Se aclarará el significado de la expresión "fintech". Las otras expresiones se explican por sí mismas.

49	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto a la proporcionalidad de las obligaciones Sugerimos revisar la proporcionalidad de las obligaciones impuestas a las entidades Fintech, en especial para aquellas empresas que no prestan servicios financieros directamente, tales como startups o desarrolladores tecnológicos. La exigencia de implementar estudios de impacto de privacidad y medidas de seguridad avanzadas podría representar una inversión significativa en cuanto a tiempo y recursos, por lo que las medidas deberían ser proporcionales al alcance e impacto en la prestación del servicio financiero.	No aceptada	Las instrucciones son proporcionales y deben responder al contexto de cada sujeto obligado. El cumplimiento de la ley no debe modificarse según el actor.
50	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto de las medidas de seguridad En relación con las medidas de seguridad adicionales relacionado con la captura de datos biométricos sugerimos revisar el alcance de la instrucción. Asimismo, señalamos que no resulta clara la calificación de la recolección de datos sensibles como "excepcional", especialmente en sistemas que requieren dichos datos como herramienta para controlar y aplicar medidas de control contra el fraude. Adicionalmente, sugerimos que la obligación de información no se centre exclusivamente en advertir que el titular no está obligado a suministrarlos, sino en aplicar el principio de transparencia, permitiendo al titular otorgar su consentimiento de manera libre, previa e informada.	Parcialmente aceptada	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.
51	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la instrucción 14 Comentarios respecto a las limitaciones impuestas a las actividades de cobranza. Consideramos que es necesario revisar que se mantenga un balance entre la protección de datos personales y el derecho legal a cobrar una acreencia. Las obligaciones previstas presentan desafíos similares a los que ha planteado la Ley y deberían ajustarse a sus parámetros, en virtud del principio de reserva de ley.	No aceptada	La aplicación conjunta de las Leyes 1266 de 2008, 1581 de 2012 y 2300 de 2023 garantiza que las gestiones de cobranza se realicen de manera legal, ética y respetuosa de los derechos fundamentales, en especial de la intimidad
52	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios respecto a datos biométricos Respetuosamente solicitamos aclarar el alcance de la definición de 'datos biométricos', específicamente en relación con: 1) Tecnologías de device fingerprinting que recopilan información como tamaño de pantalla, modelo de dispositivo y aplicaciones instaladas para reducir requisitos de autenticación, y 2) Biometría conductual, incluyendo patrones de pulsación de teclas y dinámica de uso del dispositivo. Al respecto, es fundamental establecer si estas tecnologías se considerarán datos sensibles al mismo nivel que la biometría tradicional (huellas dactilares, reconocimiento facial) para garantizar claridad en su tratamiento y obligaciones asociadas.	No aceptada	La circular no trata de este asunto
53	Cámara Colombiana de Informática y Telecomunicaciones	Comentarios a la instrucción 17 Comentarios respecto a la transferencia internacional de datos personales En relación con la transferencia internacional de datos personales, sugerimos revisar el alcance de las normas de soft law referidas, ya que no resulta clara la competencia de la SIC para regular de manera autónoma aspectos que, por su naturaleza, podrían requerir una habilitación legal expresa.	No aceptada	La instrucción se fundamenta en los artículos 21 y 26 de la Ley 1581 de 2012. En su calidad de Autoridad Nacional de Protección de Datos Personales, la SIC tiene el deber de velar por la garantía efectiva de los derechos de los titulares en el contexto de operaciones transfronterizas, asegurando que dichas transferencias se realicen conforme a los principios, estándares y mecanismos previstos en la Ley 1581 de 2012 y su reglamentación.
54	Asociación Latinoamericana de Internet	Comentario general: Consideramos que algunas de las instrucciones contenidas en el proyecto normativo exceden las funciones asignadas a la SIC por la Ley Estatutaria 1581 de 2012, cuyo artículo 21 establece que la Superintendencia de Industria y Comercio ejercerá las funciones de: "Velar por el cumplimiento de la legislación en materia de protección de datos personales (...) Impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación de las operaciones de los Responsables del Tratamiento y Encargados del Tratamiento a las disposiciones previstas en la presente ley (...)" (negrilla fuera de texto). De igual forma, la Ley 1266 de 2008, en su artículo 17, otorga a la Superintendencia la facultad de: "(...) Impartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones [legales] relacionadas con la administración de la información financiera, crediticia, comercial, de servicios y la proveniente de terceros países; fijar los criterios que faciliten su cumplimiento y señalar procedimientos para su cabal aplicación (...)" (negrilla fuera de texto). En virtud de lo anterior, es claro que la competencia de la SIC en materia de protección de datos personales se limita a impartir parámetros operativos o procedimentales para el cumplimiento de la normativa vigente. Su función se circunscribe a la emisión de instrucciones que desarrollen, aclaren o guíen la aplicación de las disposiciones legales, sin introducir obligaciones adicionales ni modificar el contenido del marco normativo. Por lo tanto, no resulta procedente que la SIC incorpore en la circular normas no previstas en la legislación de protección de datos personales, tales como restricciones adicionales, requisitos o formalidades no exigidas, el desconocimiento de excepciones expresamente reconocidas, o la imposición de condiciones más estrictas al alcance de la autorización otorgada por los titulares. Adicionalmente, advertimos que algunas de las instrucciones propuestas, al no estar alineadas con el marco legal vigente, podrían desincentivar la innovación, obstaculizar el desarrollo tecnológico en el sector financiero y dificultar la administración de información financiera, crediticia, comercial y de servicios, contrariando el propósito de promover el uso responsable y eficiente de los datos personales en estos modelos de negocio. Lo anterior, en la medida en que las obligaciones derivadas de la circular serían aplicables únicamente a este sector, sin justificación para tal diferenciación. Por otra parte, es importante señalar que, al no existir una definición legal de "actores del sistema fintech", no resulta claro el ámbito de aplicación del proyecto de circular, ya que no se especifica quiénes serían los sujetos obligados a cumplir con las instrucciones. Esta situación afecta la seguridad jurídica. Solicitamos, en consecuencia, que la SIC precise el ámbito de aplicación de la circular, estableciendo definiciones claras para la industria.	No aceptada	La Superintendencia de Industria y Comercio no está excediendo sus facultades legales y constitucionales en tanto las instrucciones de la presente circular reiteran las disposiciones contenidas en la Ley 1581 de 2012 y el Decreto 1377 de 2013.
55	Asociación Latinoamericana de Internet	Instrucción 5. "En los casos en que se solicite autorización para el tratamiento de datos personales con finalidades adicionales a aquellas estrictamente necesarias para la prestación del servicio, dicha autorización deberá otorgarse de manera diferenciada. Para solicitar la autorización en estos casos, se sugiere usar palabras sencillas y expresiones breves, que sean comprensibles por los titulares. Se podrían señalar, entre otras, las siguientes finalidades diferenciadas: para perfilamiento y mejor conocimiento de los gustos y necesidades; para activar alianzas con comercios aliados; para compartir con entidades vinculadas con fines comerciales y/o publicitarias; para realizar contacto con fines comerciales y/o publicitarios (...)" Esta instrucción introduce una exigencia no prevista en la ley respecto al otorgamiento de la autorización por parte del titular. La normativa aplicable, en particular el artículo 5 del Decreto 1377 de 2013 y el artículo 12 de la Ley 1581 de 2012, únicamente exige que el Responsable del Tratamiento informe de manera clara y expresa los datos personales que serán recolectados, el tratamiento al cual serán sometidos y la finalidad del mismo. Si bien es cierto que las finalidades adicionales a las estrictamente necesarias para la prestación del servicio deben ser informadas al titular al momento de solicitar su autorización, la normativa no contempla la necesidad de segmentar o fraccionar la autorización del titular frente a dichas finalidades. Desde una perspectiva práctica, exigir una autorización diferenciada para cada finalidad adicional impone una carga operativa y técnica significativa para los actores del ecosistema fintech, cuyos modelos de negocio se fundamentan en el uso ágil y eficiente de tecnologías para personalizar servicios financieros, mejorar la experiencia del usuario y generar valor a partir del análisis de datos. Esta exigencia ralentizaría procesos clave como el onboarding digital o la activación de servicios complementarios, y afectaría la interoperabilidad de plataformas y el desarrollo de innovaciones basadas en análisis predictivo y automatización. Por lo anterior, consideramos que no es procedente imponer esta obligación, ya que representa una carga no prevista por la ley de protección de datos personales ni por su reglamentación.	Parcialmente aceptada	Se reformuló parcialmente esta instrucción para eliminar la obligación de solicitar autorización para cada finalidad. En el nuevo proyecto de Circular se indica que: "Los responsables deben solicitar la autorización diferenciando las finalidades al menos en dos grupos: las finalidades necesarias y las finalidades accesorias".
56	Asociación Latinoamericana de Internet	Instrucción 7. "La recolección y el tratamiento de datos personales sensibles, en especial de datos biométricos, requiere una diligencia reforzada por parte del responsable del tratamiento. Por eso, al momento de la recolección que en todo caso debe ser excepcional, el responsable del tratamiento deberá informar al titular: (...)". Manifiestamos que el apartado en negrilla, según el cual el tratamiento de datos personales sensibles debe ser excepcional, constituye una instrucción que no encuentra sustento en la ley vigente de protección de datos personales ni en sus normas reglamentarias. La ley permite a los responsables tratar datos sensibles en cumplimiento de los requisitos aplicables, sin establecer que dicho tratamiento deba ser excepcional. Por lo tanto, solicitamos la supresión del apartado resaltado.	No aceptada	La legislación colombiana sí contempla que el tratamiento de datos personales sensibles es excepcional. De ahí que el artículo 6 de la Ley 1581 de 2012 contemple una prohibición general con algunas excepciones.

57	Asociación Latinoamericana de Internet	Instrucción 12. "Los actores del ecosistema fintech deben implementar procedimientos que garanticen el mantenimiento de registros detallados sobre las solicitudes de acceso a datos personales por parte de terceros autorizados por el titular. Dichos registros deberán incluir, como mínimo, la identidad del solicitante, el origen de los datos, el destinatario, la finalidad del acceso y las fechas en que se realizaron dichas acciones". Solicitamos respetuosamente la supresión de esta instrucción, ya que ni la Ley 1581 de 2012 ni el Decreto 1377 de 2013 establecen como obligación para los responsables y/o encargados llevar este tipo de registro. En consecuencia, mediante una circular externa, la SIC estaría creando nuevas obligaciones y excediendo sus competencias legales.	Aceptada	Se eliminará la instrucción 12
58	Asociación Latinoamericana de Internet	Instrucción 13. "Los responsables y encargados deberán implementar estrategias de diseño legal orientadas a mejorar la comprensión del titular sobre el uso de su información personal (...)". A pesar de que los responsables y encargados tienen la obligación legal de suministrar información a los titulares respecto del tratamiento que se le da a su información personal, el marco de protección de datos personales vigente no establece que se deban utilizar estrategias de "diseño legal" para "mejorar la comprensión del titular sobre el uso de su información personal".	Aceptada	Se eliminará la expresión "diseño legal"
59	CredibanCo S.A.	En este sentido, consideramos necesario que la Superintendencia de Industria y Comercio (SIC) precise detalladamente qué debe entenderse por "ecosistema Fintech", así como, a qué tipo de Fintech le son aplicables las instrucciones. Lo anterior, debido a que en Colombia no existe una definición legal de Fintech, aun cuando la industria ha venido asociando el término Fintech para referirse a entidades que prestan servicios financieros o apoyan procesos del sistema financiero mediante el uso tecnologías innovadoras, ya sea, directamente o mediante plataformas digitales, aplicaciones móviles, algoritmos, inteligencia artificial, blockchain, entre otros. Lo que implicaría que cualquier empresa que utilice tecnologías innovadoras para prestar servicios financieros podría ser considerada potencialmente una Fintech.	Aceptada	Se aclaró el ámbito de aplicación de la circular
60	CredibanCo S.A.	Adicionalmente, es pertinente que la SIC revise el posible desequilibrio que podría generarse al imponer exigencias robustas exclusivamente al sector Fintech, cuando otros sectores —como el comercio electrónico o de remesas— también ofrecen servicios mediante tecnologías innovadoras.	No aceptada	No se general desequilibrios. La actividad de tratamiento de datos personales es una actividad regulado y por lo tanto se debe cumplir la ley. La instrucción no crea obligaciones diferenciadas a un sector, sino que aplica la ley a un sector y sus dinámicas particulares.
61	CredibanCo S.A.	En igual sentido, es relevante ver con detalle las instrucciones impartidas frente a las finalidades legítimas para el tratamiento de datos personales, toda vez que, si bien, dichas instrucciones están orientadas a proteger al titular del dato, estas podrían generar restricciones en modelos de negocio basados en analítica de datos e innovación predictiva, mismos que aún están en desarrollo en el país, y en donde las finalidades no siempre están plenamente definidas desde la captura del dato. A este respecto, cabe resaltar que la misma SIC ha estimado la flexibilización de la regulación para equilibrarla con necesidades de mercado como, por ejemplo, viabilizando las aceptaciones fáciles inequívocas. En línea con lo anterior, actualmente se encuentra en revisión reglamentación asociada a los parámetros para el uso de los datos en el entrenamiento de tecnología basada en Inteligencia Artificial (IA)1, dado que, existe una finalidad superior consistente en democratizar la información y el acceso a productos financieros, el cual, podría verse limitado al mantener barreras que incentiven el uso de procesos basados en documentos físicos o procesos manuales, para ello, la SIC podría considerar el permitir que, mediante una autorización diferenciada, los titulares autoricen el uso de los datos personales para el entrenamiento de la IA y, de esta forma, se promuevan los ejes estratégicos del CONPES 4144 el cual, básicamente, busca fortalecer la utilización de la IA para generar una economía del conocimiento partiendo de la investigación, desarrollo e innovación (I+D+I).	No aceptada	Todos los modelos de negocio basados en datos deben cumplir la ley
62	CredibanCo S.A.	En línea con lo expuesto, respecto al principio de minimización de datos, para el ecosistema Fintech se sugiere que se implementen excepciones justificadas de acuerdo con estudios de impacto o criterios técnicos definidos.	No aceptada	No es posible flexibilizar la aplicación de la ley. El principio de minimización no exige abstenerse de realizar tratamiento de datos personales en absoluto, sino únicamente realizar tratamiento de datos personales sobre los datos que resulten necesarios para las finalidades constitucionalmente legítimas
63	CredibanCo S.A.	Comentarios a la instrucción 9 Por otra parte, se aprecia que las instrucciones asimilan las tecnologías de automatización con el uso de tecnologías que permiten el aprendizaje de patrones para la toma de decisiones como, por ejemplo, el machine learning (ML) o la IA, por lo que, se estima apropiado definir el alcance del derecho de impugnación frente a "decisiones automatizadas", especialmente en plataformas que operan de forma continua y con alta carga transaccional donde se hace necesario una operación en tiempo real y a través de canales digitales.	Parcialmente aceptada	Se eliminará la instrucción 9
64	Credintegral S.A.S.	Sobre el numeral 2: Minimización de datos y restricciones tecnológicas "Las aplicaciones [...] no deben solicitar acceso a información innecesaria como la galería de imágenes del dispositivo o la lista de contactos." Observación: La prohibición generalizada puede afectar servicios Fintech legítimos que requieren estos accesos, por ejemplo, para validación de identidad, análisis de riesgo crediticio alternativo o funcionalidades de pago social (contactos). Sugerencia de redacción: "Las aplicaciones no deben solicitar acceso a información como la galería de imágenes o lista de contactos, salvo que dicho acceso sea estrictamente necesario, proporcional y justificado en función del servicio financiero ofrecido, y así se informe al titular en los términos del artículo 12 de la Ley 1581 de 2012."	Parcialmente aceptada	Se ajustó la redacción de esta instrucción en tanto la prohibición aplica para fines de cobranza
65	Credintegral S.A.S.	2. Sobre el numeral 5: Finalidades adicionales y consentimiento "Para solicitar la autorización en estos casos, se sugiere usar palabras sencillas y expresiones breves [...]". Observación: La Circular debe reconocer que el diseño de experiencia de usuario en Fintech ya incorpora medios interactivos e inteligentes para capturar el consentimiento de forma granular, sin necesidad de simplificación excesiva que afecte la precisión jurídica. Sugerencia: Se sugiere reemplazar el texto señalado al principio por el siguiente "Se recomienda el uso de mecanismos interactivos e inteligentes para el usuario, tales como formularios dinámicos, configuraciones por capas, o sistemas de gestión de consentimiento que permitan al titular comprender y controlar de forma diferenciada las finalidades adicionales.	No aceptada	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.

66	Credintegral S.A.S.	<p>Sobre el numeral 6: Prohibición de uso de biometría como requisito</p> <p>"Está prohibido condicionar la realización de actividades financieras [...] al suministro de datos personales sensibles, en especial, datos biométricos."</p> <p>Observación: La biometría es fundamental para el onboarding digital, la autenticación segura y la prevención del fraude. La redacción actual podría restringir mecanismos válidos de seguridad en canales digitales.</p> <p>Redacción alternativa: "Se prohíbe condicionar la prestación del servicio financiero al suministro de datos sensibles cuando existan mecanismos equivalentes de autenticación que no requieran dicho tratamiento. En los casos en que el uso de biometría sea necesario para proteger el servicio o al titular, su implementación deberá cumplir con los principios de necesidad, proporcionalidad, y reforzar las medidas de seguridad técnica y legal."</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece: "Artículo 6°. De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.</p> <p>(...)</p> <p>Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.</p>
67	Credintegral S.A.S.	<p>Sobre el numeral 8: La transparencia en el uso de tecnologías automatizadas</p> <p>"Los actores del ecosistema Fintech deberán garantizar la transparencia en el uso de tecnologías automatizadas en sus procesos de tratamiento de datos personales."</p> <p>Observación: Este mandato es adecuado, pero se recomienda que la Circular reconozca expresamente que estas tecnologías pueden hacer parte del núcleo operativo del servicio Fintech y que su uso no está prohibido, sino sujeto a condiciones específicas de información y responsabilidad.</p> <p>Redacción alternativa: "El uso de tecnologías automatizadas deberá hacerse con base en principios de transparencia, información y trazabilidad, en cumplimiento de los derechos del titular y del principio de responsabilidad demostrada."</p>	No aceptada	La instrucción no está prohibiendo el uso de tecnologías automatizadas sino promoviendo la transparencia cuando se usen
68	Credintegral S.A.S.	<p>Sobre el numeral 9: las decisiones basadas exclusivamente en tratamiento automatizado</p> <p>"Ningún titular podrá ser objeto de una decisión basada exclusivamente en el tratamiento automatizado [...]"</p> <p>Observación: Este enunciado entra en tensión con el artículo 12 de la Ley 2439 de 2024, el cual permite decisiones automatizadas siempre que el titular sea informado de forma clara y tenga derecho a impugnar la decisión y obtener intervención humana, es por tanto que el ecosistema Fintech, donde el scoring automatizado es esencial, esta distinción resulta crítica.</p> <p>Sugerencia: "Las decisiones basadas exclusivamente en tratamiento automatizado serán admisibles siempre que se informe previamente al titular y se habiliten mecanismos efectivos para impugnarlas y solicitar revisión humana, conforme al artículo 12 de la Ley 2439 de 2024."</p>	Parcialmente aceptada	Se eliminará la instrucción 9
69	Credintegral S.A.S.	<p>Sobre el numeral 10: Medidas de seguridad</p> <p>"Las medidas de seguridad implementadas deben estar documentadas y ser apropiadas [...] auditable por las autoridades [...]"</p> <p>Observación: Se recomienda que la Circular reconozca la posibilidad de validación a través de certificaciones o estándares internacionales como ISO/IEC 27001 o PCI-DSS, para evitar duplicidad de auditorías y favorecer seguridad jurídica.</p> <p>Sugerencia: "Se valorará positivamente la adopción de estándares internacionales en seguridad de la información, tales como ISO/IEC 27001 o NIST, como mecanismos para evidenciar el cumplimiento del deber de seguridad, sin perjuicio de las verificaciones que adelante la Autoridad."</p>	No aceptada	No es adecuado establecer estándares de seguridad unificados y generales en tanto estos dependen del nivel y tipo de riesgo, que solo puede ser analizado en el caso concreto
70	Credintegral S.A.S.	<p>Sobre el numeral 14: Gestión de cobranza</p> <p>"Los actores [...] deberán abstenerse de contactar a las referencias personales [...]"</p> <p>Observación: Si bien la Ley 2300 de 2023 lo prohíbe, se requiere precisión respecto a la etapa del proceso de cobranza y si la referencia ha sido autorizada como contacto de emergencia o codeudor.</p> <p>Sugerencia: "Deberán abstenerse de contactar referencias personales salvo que exista autorización expresa del titular o vínculo jurídico con la obligación (codeudor, garante). Esta regla aplica a las gestiones de cobranza extrajudicial en fase de mora, conforme a la Ley 2300 de 2023 y la Circular Externa 001 de 2024."</p>	No aceptada	La circular está reiterando las obligaciones derivadas de la Ley 2300 de 2023
71	Credintegral S.A.S.	Incluir una sección de definiciones con términos clave como: "Fintech", "Datos biométricos", "Decisión automatizada", "Perfilamiento crediticio", entre otros	Parcialmente aceptada	Se incluirá una definición de fintech. Sin embargo, los otros conceptos se explican por sí mismos o ya se encuentran definidos en otros instrumentos legales como la Ley 1581 de 2012
72	Credintegral S.A.S.	Abrir espacio a pruebas piloto y entornos de prueba regulatoria (Sandbox) para evaluar la proporcionalidad de las medidas antes de exigir cumplimiento pleno	No aceptada	Este asunto no hace parte de la circular ni puede lograrse a través de un instrumento jurídico de este tipo
73	Credintegral S.A.S.	Incluir remisión expresa al principio de sostenibilidad e innovación del ecosistema digital, reconociendo que la protección de datos debe armonizarse con el desarrollo empresarial (arts. 333 y 334 CPol., Ley 2439 de 2024, art. 3).	No aceptada	No se considera oportuno hacer referencia al principio de sostenibilidad en tanto la circular busca instruir sobre el tratamiento de datos personales en un sector, no sobre el desarrollo tecnológico y empresarial
74	Alianza In Colombia	<p>Instrucción 1.</p> <p>Se propone adicionar una frase al final de la instrucción, para acopiar el proyecto de circular con el artículo 11 del Decreto 1377 de 2013, que incluye la obligación de conservar información por motivos administrativos, contables y fiscales; para de esta manera, garantizar seguridad jurídica y coherencia en las obligaciones de conservación de la información: "El tratamiento de datos personales en el ecosistema fintech y los modelos de negocio, aplicaciones y procesos que utilizan medios tecnológicos para la prestación de servicios financieros solo puede adelantarse para satisfacer finalidades constitucionalmente legítimas. Únicamente se puede realizar tratamiento de datos personales durante el tiempo que resulte razonable y necesario, de acuerdo con las finalidades que lo justificaron, atendiendo las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información."</p>	No aceptada	La instrucción se refiere únicamente a la conservación de datos personales y esto puede depender, no solo de las disposiciones aplicables a cada materia como se propone, sino también a la finalidad del tratamiento

75	Alianza In Colombia	<p>Instrucción 3.</p> <p>Se propone la eliminación de parte del texto de la instrucción, en razón a los siguientes argumentos:</p> <ul style="list-style-type: none"> - La disposición puede resultar innecesaria, pues la gran mayoría de aplicaciones cobijadas por esta instrucción piden por defecto permiso de acceso a algunas funcionalidades del dispositivo, teniendo el usuario la potestad de autorizarlas no en su dispositivo. - La expresión "deberá informarse de manera clara la finalidad de cada acceso" podría interpretarse en el sentido que dicha obligación debe materializarse cada vez que la aplicación vaya a acceder a la ubicación o la cámara del dispositivo, lo cual en algunos casos puede ocurrir varias veces en un mismo día, generando una fricción seria en el funcionamiento de las aplicaciones y en la calidad y fluidez de la experiencia de los usuarios."El tratamiento de datos personales en el ecosistema fintech debe incluir procedimientos que aseguren, de manera previa a la recolección de los datos, la obtención de la autorización del titular para dicho tratamiento. Asimismo, se debe informar al titular sobre cuáles son los datos personales que serán recolectados y las finalidades específicas que justifican su tratamiento. Por tanto, en las aplicaciones disponibles para descarga, es el titular quien debe decidir si otorga acceso a su información personal, como, por ejemplo, el acceso a la ubicación o a la cámara. En dicho sentido, deberá informarse de manera clara la finalidad de cada acceso a la ubicación o a la cámara, a fin de que el titular pueda tomar una decisión informada sobre el uso de sus datos." 	No aceptada	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.
76	Alianza In Colombia	<p>Instrucción 4.</p> <p>Se propone la eliminación de la parte final de esta instrucción, pues puede resultar imposible para las empresas Fintech contar con evidencia de las autorizaciones allí mencionadas, cuando éstas se den de forma oral o mediante conductas inequívocas. Tampoco resulta claro si se espera que la disponibilidad para consulta por parte del titular sea una condición permanente, o se cuente con un procedimiento para tal fin.</p> <p>"La autorización para el tratamiento de datos personales la puede expresar el titular de la información por escrito, por un mensaje de datos, de forma oral o mediante conductas inequívocas que permitan determinar de forma razonable que se otorgó la autorización. Para el tratamiento de datos sensibles no procede la autorización mediante conductas inequívocas. Los actores del ecosistema fintech deben contar con evidencia de que el titular de la información efectivamente otorgó su autorización para el tratamiento de sus datos personales. La autorización debe estar disponible para la consulta del titular.</p>	No aceptada	<p>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.</p> <p>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.</p>
77	Alianza In Colombia	<p>Instrucción 5.</p> <p>Se proponen dos cambios en esta instrucción:</p> <ol style="list-style-type: none"> 1. La eliminación de la obligación a solicitar una autorización diferenciada para el tratamiento de datos personales con finalidades adicionales a las estrictamente necesarias para la prestación del servicio, toda vez que se trata de un requisito normativo nuevo que no se desprende de ninguna norma de rango superior que habilite tal restricción. Además, esta medida resultaría violatoria del principio de igualdad, al imponer al sector económico objeto de la Circular cargas que no existen en otros sectores de la economía nacional. 2. Se propone la eliminación de la frase final de esta instrucción, toda vez que vulnera el principio de libertad de empresa y carece de una base normativa superior clara. 	No aceptada	<p>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:</p> <ul style="list-style-type: none"> *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.
78	Alianza In Colombia	<p>Instrucción 6.</p> <p>Limitar o desincentivar el uso de biometría en procesos digitales profundizaría la brecha entre las fintech y el sistema financiero tradicional, al restringir el uso de herramientas tecnológicamente avanzadas en modelos que no pueden apalancarse en infraestructura física. A diferencia de las entidades financieras tradicionales, que pueden recurrir a mecanismos presenciales de verificación, las fintech operan en entornos puramente digitales, lo que demanda soluciones de autenticación remota con altos estándares de certeza y robustez. En este escenario, la autenticación biométrica se consolida como uno de los métodos más eficaces y proporcionales para mitigar riesgos de fraude, cumplir con obligaciones de debida diligencia y proteger tanto a las compañías como a los usuarios.</p> <p>Así mismo, se ralentizaría la inclusión financiera de la población de menores ingresos y mayor riesgo crediticio, ya que la autenticación biométrica es un habilitador directo de la inclusión financiera, al permitir que poblaciones sin acceso a sucursales bancarias puedan abrir y gestionar productos financieros desde cualquier ubicación, de manera segura, ágil y verificable.</p> <p>La medida también afectaría el principio de neutralidad tecnológica y crearía una barrera para la innovación en el país, restringiendo el desarrollo de soluciones que actualmente permiten combatir de forma efectiva uno de los principales riesgos del ecosistema digital, como es la suplantación de identidad.</p> <p>Debe recordarse que el fraude por suplantación de identidad es uno de los principales riesgos que enfrentan las fintech y las entidades financieras tradicionales que, cada vez más, ofrecen servicios financieros no basados en la presencialidad. Este fenómeno no solo compromete la seguridad de los usuarios finales, sino que también impacta directamente la viabilidad operativa y regulatoria de las empresas de base tecnológica.</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece: "Artículo 6". De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 6° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.</p> <p>(...)</p> <p>Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.</p>
79	Alianza In Colombia	<p>Instrucción 7.</p> <p>En línea con los comentarios formulados para la Instrucción 6, consideramos altamente inconveniente que el uso de biometría se restrinja a circunstancias excepcionales o solo puedan prestarse de forma opcional. Esto generaría una desventaja competitiva definitiva para las empresas Fintech con respecto a la banca tradicional; afectaría gravemente la inclusión financiera de los colombianos de menores recursos; aumentaría el riesgo de fraude por suplantación personal en operaciones bancarias y Fintech; impactaría negativamente el ecosistema digital y de innovación del país; entre otros. Cuando la biometría es utilizada con los suficientes estándares de calidad y seguridad, no solo es legalmente compatible con el marco normativo colombiano, sino que es indispensable para la sostenibilidad de modelos digitales, la prevención de fraudes, y la democratización del acceso al sistema financiero.</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece: "Artículo 6". De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.</p> <p>(...)</p> <p>Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.</p>
80	Alianza In Colombia	<p>Instrucción 8.</p> <p>De manera atenta, recomendamos que la Circular defina claramente el significado de la expresión tecnologías automatizadas, para así entender por qué es una obligación diferenciada para los actores del ecosistema fintech, teniendo en cuenta que no es una obligación general incluida en las leyes 1266 y 1581 que, como se reconoce en este mismo proyecto de circular, son tecnológicamente neutrales.</p>	No aceptada	La expresión "tecnología automatizada" se explica por sí misma
81	Alianza In Colombia	<p>Instrucción 9.</p> <p>Recomendamos adicionar la frase que se subraya en el siguiente párrafo, para que quede totalmente claro que la posibilidad de impugnación por parte de los usuarios no obliga a la aceptación de su solicitud y que, además, en ese momento las compañías podrán solicitar información adicional: "Ningún titular podrá ser objeto de una decisión basada exclusivamente en el tratamiento automatizado de sus datos personales sin haber sido debidamente informado sobre ello. Asimismo, los titulares tendrán el derecho a impugnar una decisión automatizada a través de los canales dispuestos para la presentación de peticiones o reclamos, especialmente cuando dicha decisión tenga consecuencias negativas o determinantes, como la negación de un crédito o el rechazo en la apertura de un producto o servicio financiero. En todo caso, la impugnación no hace obligatoria la aprobación de la solicitud y se podrá solicitar información y/o documentos que permitan completar el estudio de la solicitud. Cuando corresponda, los responsables y encargados del tratamiento deberán tener en cuenta lo dispuesto en la Circular Externa No. 002 del 21 de agosto de 2024 de esta entidad, sobre "Lineamientos sobre el Tratamiento de Datos Personales en Sistemas de Inteligencia Artificial"."</p>	No aceptada	Se eliminará la instrucción 9
82	Alianza In Colombia	<p>Instrucción 10.</p> <p>Es positivo que el proyecto de circular exija altos estándares de seguridad en el tratamiento de datos personales. Pero el cumplimiento de este propósito se aleja en la medida que se restrinja y desincentive el uso de tecnologías de biometría, como lo hace este proyecto de circular en puntos ya comentados, toda vez que estos desarrollos tecnológicos resultan especialmente sólidos en materia de seguridad de la información, prevención del fraude y ciberseguridad.</p>	Parcialmente aceptada	<p>Se reformularon las instrucciones relacionadas con datos biométricos. Se reformuló la instrucción de acuerdo al comentario con el fin de aclarar que se trata de una práctica legítima que debe cumplir con ciertas reglas. En todo caso, vale la pena recordar que la SIC, no ha generado una nueva regla, retoma las obligaciones establecidas en el artículo 6 de la Ley 1581 de 2012, y el artículo 6 del Decreto 1377 de 2013, el cual establece: "Artículo 6". De la autorización para el Tratamiento de datos personales sensibles. El Tratamiento de los datos sensibles a que se refiere el artículo 5° de la Ley 1581 de 2012 está prohibido, a excepción de los casos expresamente señalados en el artículo 6° de la citada ley.</p> <p>(...)</p> <p>Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.</p>
83	Alianza In Colombia	<p>Instrucción 12.</p> <p>A la luz de las leyes 1266 de 2008 y la 1581 de 2012, no es proporcional ni razonable que se imponga una obligación de procedimiento y registro a los actores del ecosistema fintech sobre un hecho que no es exclusivo de este sector de la economía nacional. Las solicitudes por parte de terceros distintos a los titulares deben cumplir con los requisitos de legitimación previstos en la legislación vigente, sin importar el sector en el que se realice el tratamiento. Por esta razón, ponemos a consideración de ustedes la posibilidad de eliminar este punto de la Circular.</p>	Aceptada	Se eliminará la instrucción 12

84	Banco Finandina Banca libre	Instrucción 1. Consideramos que el término "constitucionalmente legítimas" requiere una definición expresa en la circular o su referencia normativa clara, para evitar interpretaciones subjetivas o divergentes. Se entiende que se refiere a conductas permitidas por la Constitución, pero la precisión técnica facilitaría su correcta aplicación. Similarmente, se recomienda clarificar los alcances de "razonable y necesario" para garantizar certeza jurídica a los responsables del tratamiento.	No aceptada	Esta instrucción retoma la obligación que estableció el artículo 11 del Decreto 1377 de 2013, el cual indica: "Limitaciones temporales al Tratamiento de los datos personales. Los Responsables y Encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información (...)"
85	Banco Finandina Banca libre	Instrucción 2. El Banco sugiere prudencia regulatoria frente a la prohibición categórica de solicitar acceso a ciertos datos, como la galería de imágenes o lista de contactos, dado que en algunos casos el acceso a esta información puede facilitar la operatividad y seguridad de procesos legítimos, tales como validaciones biométricas o agilización de transacciones. Además, consideramos que es necesario claridad sobre el término "actores del ecosistema fintech" y la aplicación de estas disposiciones a entidades vigiladas por la Superintendencia Financiera de Colombia.	Parcialmente aceptada	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 del servicio ofrecido, su tratamiento se considera excesivo y, por tanto, contrario a la ley.
86	Banco Finandina Banca libre	Instrucción 3. Consideramos que la regulación debería ser lo suficientemente flexible y amplia para permitir que las finalidades específicas de cada acceso a datos personales se incorporen y detallen adecuadamente dentro de la política general de tratamiento de datos. Esto evitaría la necesidad de solicitar dicha autorización de manera reiterada cada vez que se utilice el servicio. Por ejemplo, en procesos de validación de identidad es evidente la necesidad de utilizar diversas funcionalidades del dispositivo, cuyas finalidades pueden anticiparse y describirse claramente en la política general de tratamiento de datos. Esta aproximación facilita la operatividad y garantiza transparencia sin generar cargas administrativas excesivas para las entidades.	No aceptada	Aceptar dicha instrucción sería desconocer el régimen normativo de protección de datos, e invalidar los instrumentos que la legislación ha establecido para dicho fin. La Política de Tratamiento de Datos no es el medio idóneo para aceptar las finalidades, sino para informarlas. La legislación es clara en indicar que es a través de la autorización por medio de la cual se informa las finalidades del tratamiento del titular, para que este las autorice o rechace. Al respecto, el artículo 12 de la Ley 1581 de 2012, establece: Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) 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; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento. Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta. Por otro lado, la SIC no ha generado una regla nueva, la legislación es clara, que se debe conservar copia de la autorización para su posterior consulta. Esta puede ser consultada por el titular, o por esta Superintendencia, en calidad de Autoridad de Protección de Datos
87	Banco Finandina Banca libre	Instrucción 4. El Banco considera que la regulación debería permitir que la autorización para el tratamiento de datos personales, incluyendo los datos sensibles, pueda ser recogida y gestionada de forma integral a través de la política general de tratamiento de datos. De esta manera, no sería necesario recabar autorizaciones adicionales o específicas cada vez que se utilicen diferentes funcionalidades o se realicen nuevos accesos, siempre que dichas finalidades estén claramente previstas y descritas en la política. Esta práctica, además de facilitar la operatividad y eficiencia, garantiza la transparencia y el derecho a la consulta por parte del titular, evitando cargas administrativas redundantes y promoviendo un tratamiento ágil y seguro.	No aceptada	"Aceptar dicha instrucción sería desconocer el régimen normativo de protección de datos, e invalidar los instrumentos que la legislación ha establecido para dicho fin. La Política de Tratamiento de Datos no es el medio idóneo para aceptar las finalidades, sino para informarlas. La legislación es clara en indicar que es a través de la autorización por medio de la cual se informa las finalidades del tratamiento del titular, para que este las autorice o rechace. Al respecto, el artículo 12 de la Ley 1581 de 2012, establece: Deber de informar al Titular. El Responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente: a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo; b) 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; c) Los derechos que le asisten como Titular; d) La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento. Parágrafo. El Responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta. Por otro lado, la SIC no ha generado una regla nueva, la legislación es clara, que se debe conservar copia de la autorización para su posterior consulta. Esta puede ser consultada por el titular, o por esta Superintendencia, en calidad de Autoridad de Protección de Datos"
88	Banco Finandina Banca libre	Instrucción 5. El Banco considera que la regulación debe permitir que las finalidades adicionales para el tratamiento de datos personales puedan integrarse de manera clara y detallada en la política general de tratamiento de datos, facilitando así una autorización diferenciada sin necesidad de múltiples solicitudes cada vez que se utilicen distintos servicios o funcionalidades. Esta aproximación contribuiría a simplificar la experiencia del titular, permitiéndole ejercer su derecho a otorgar o negar autorizaciones específicas de forma informada y ágil, sin afectar la prestación del servicio principal. Además, el uso de un lenguaje sencillo y comprensible en la política favorecerá la transparencia y la confianza entre las partes.	Parcialmente aceptada	Se acepta parcialmente, en la medida que se agrupan las finalidades en dos tipos obligatorias y facultativas.
89	Banco Finandina Banca libre	Instrucción 6. El Banco considera que la regulación debe contemplar un marco lo suficientemente amplio y flexible para permitir que, en el contexto de la provisión de servicios financieros a través de medios tecnológicos, las finalidades y condiciones para el tratamiento de datos personales sensibles, incluyendo datos biométricos, puedan estar claramente descritas y autorizadas dentro de la política general de tratamiento de datos. Esto evitaría que se condicione el acceso a servicios o productos financieros a autorizaciones reiteradas que podrían entorpecer la experiencia del usuario y la operatividad del servicio. Además, es fundamental que se mantengan las medidas de seguridad adecuadas y que la autorización del titular sea debidamente registrada y conservada, garantizando así la protección y el consentimiento informado.	No aceptada	Se reitera que la Política de Tratamiento de Datos no es el instrumento llamado a solicitar la autorización del titular del Tratamiento.
90	Banco Finandina Banca libre	Instrucción 7. Diligencia reforzada para datos sensibles Sugerimos aclaración sobre el concepto de "diligencia reforzada" para evaluar su alcance en la regulación actual.	No aceptada	La Corte Constitucional en sentencia C-748 de 2011 ha establecido: "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"
91	Banco Finandina Banca libre	Instrucción 9. Consideramos que la regulación debe buscar un equilibrio adecuado que permita mantener la eficiencia y agilidad en los procesos automatizados, particularmente en operaciones críticas como la aprobación de créditos, las cuales se fundamentan en políticas de riesgo y modelos tecnológicos robustos. En este sentido, es fundamental que los mecanismos de información y los derechos de impugnación se diseñen de forma que no comprometan la operatividad ni impongan cargas excesivas a las entidades, al tiempo que se garantice la protección efectiva de los derechos de los titulares. Asimismo, debe respetarse la autonomía de las entidades vigiladas para definir y emplear las herramientas necesarias para la ejecución de sus políticas de riesgo, las cuales están concebidas no solo para salvaguardar los derechos de los consumidores, sino también para gestionar prudentemente su apetito de riesgo.	Parcialmente aceptada	Se ajusta la instrucción, en la medida en que el titular tiene derecho a conocer las razones que dieron lugar a la decisión negativa automatizada