Superintendencia de Industria y Comercio

CIRCULAR EXTERNA No. 001 DE 2025

(18 de septiembre de 2025)

Para: Sujetos vigilados por la Superintendencia de Industria y Comercio que realicen tratamiento de datos personales en cualquiera de los roles previstos por las leyes de protección de datos personales (responsable, encargado, fuente o usuario) en el contexto de la oferta de productos y prestación de servicios de financiación, depósitos de bajo monto y otros afines que faciliten la inclusión financiera mediante el uso de tecnologías digitales (fintech).

Asunto: Instrucciones sobre el tratamiento de datos personales en la oferta de productos y la prestación de servicios de financiación, depósitos de bajo monto y otros afines que faciliten la inclusión financiera mediante el uso de tecnologías digitales (fintech).

Consideraciones

El dinamismo de los modelos de negocio, aplicaciones y procesos para adelantar operaciones de crédito, ofrecer productos de financiación, depósitos de bajo monto, billeteras digitales y, en general, para la oferta de productos y la prestación de servicios cuasifinancieros[1] utilizando medios tecnológicos tiene un alto impacto democratizador, promueve la inclusión social, económica y financiera, dinamiza la economía, agrega valor y estimula la competencia.

La ampliación del portafolio de productos de financiación, crediticios, depósitos de bajo monto, y otros afines mediante nuevos actores, medios e infraestructuras tecnológicas permite a la ciudadanía acceder a más y mejores servicios.

La innovación en el sistema financiero, en la oferta y comercialización de productos financieros y afines, y en la oferta de servicios financieros y cuasifinancieros mediante el uso de tecnologías digitales se ha resumido bajo el anglicismo "fintech".

[1] Para efectos de esta circular, la expresión servicios cuasifinancieros hace referencia a productos o servicios que se parecen o se asemejan a los productos o servicios financieros pero que no lo son en estricto sentido. Esto incluye, entre otros, operaciones de crédito mediante sistemas de financiación, depósitos de bajo monto, billeteras digitales, operaciones de sociedades especializadas en depósitos y pagos electrónicos, actividades de adquirencia, etc.

Esto incluye, entre otras, las operaciones de crédito otorgadas por personas naturales o jurídicas cuya actividad crediticia no se encuentre bajo la vigilancia o control de una autoridad administrativa específica, así como los contratos de adquisición de bienes o prestación de servicios en los que el productor o proveedor otorgue financiación directa, de conformidad con lo previsto en el artículo 45 de la Ley 1480 de 2011 y en los artículos 2.2.2.35.1 y 2.2.2.35.2 del Decreto 1074 de 2015; las operaciones realizadas por los establecimientos de crédito, las sociedades especializadas en depósitos y pagos electrónicos (SEDPE) y las cooperativas facultadas para desarrollar actividad financiera, en los términos del artículo 2.1.15.1.1 del Decreto 222 de 2020; y las actividades de adquirencia, en los términos del artículo 2.17.1.1.1 del Decreto 1692 de 2020, cuando tales operaciones, servicios, productos y actividades se realizan mediante el uso de tecnologías digitales.

El despliegue de los modelos de negocio fintech, en especial, en lo relacionado con las actividades de tratamiento de datos personales debe realizarse de conformidad con la Constitución Política de 1991 y las leyes aplicables.

La actividad de tratamiento de datos personales por parte de los actores del ecosistema fintech está regulada desde la Constitución Política. Por un lado, la Constitución reconoce el derecho fundamental de toda persona a conocer, actualizar y rectificar la información personal que se haya recogido sobre ella en cualquier base de datos, incluidas las bases de datos personales creadas con ocasión de la prestación de servicios financieros y cuasifinancieros mediante el uso de tecnologías digitales; este derecho fundamental se conoce como habeas data. Por otro lado, la Constitución establece que en la recolección, tratamiento y circulación de la información personal deben protegerse la libertad y las demás garantías consagradas en la Constitución.

Asimismo, la actividad de tratamiento de datos personales está regulada, a nivel legal, por dos leyes estatutarias: la Ley 1266 de 2008 y la Ley 1581 de 2012. Ambas leyes son aplicables a los tratamientos de datos personales por actores que prestan servicios financieros y cuasifinancieros a través de aplicaciones, plataformas u otro tipo de tecnologías digitales. Por un lado, la Ley Estatutaria 1266 de 2008 regula el tratamiento de datos personales relacionados con el nacimiento, ejecución y extinción de obligaciones dinerarias (literal j, artículo 3, Ley 1266 de 2008). Por otro lado, la Ley Estatutaria 1581 de 2012 regula el tratamiento de datos personales en general (art. 2 y literales c y g, artículo 3, Ley 1581 de 2012).

El cumplimiento de los principios y deberes en materia de protección de datos personales y habeas data por parte de los actores del ecosistema fintech, en sus distintos roles, ya como responsables, encargados, fuentes o usuarios, concreta el principio constitucional de primacía de los derechos fundamentales. Dicho cumplimiento, además, genera confianza en el mercado, favorece la igualdad entre distintos actores, promueve un ambiente propicio para el desarrollo de nuevos servicios y funcionalidades, y asegura ventajas competitivas sostenibles y globales.

La legislación sobre protección de datos personales reconoce derechos específicos relacionados con el tratamiento de datos personales, establece los principios para dicho tratamiento y precisa deberes y obligaciones en cabeza de responsables, encargados, fuentes y usuarios, en todas las etapas del tratamiento de los datos personales, desde su recolección, almacenamiento, tratamiento y circulación, hasta su destrucción o supresión definitiva.

Esta circular sistematiza y reitera algunos de estos derechos, principios y deberes, y los presenta de forma sencilla y contextual. Con ella, la Superintendencia de Industria y Comercio concreta su misión institucional de "*velar por el cumplimiento de la legislación en materia de protección de datos personales*" y continúa en el empeño de promover la cultura de protección de datos personales en los nuevos y desafiantes escenarios de la prestación de servicios financieros y cuasifinancieros mediante tecnologías digitales.

Las leyes estatutarias 1266 de 2008 y 1581 de 2012 son neutrales tecnológicamente y sus mandatos se aplican a todo tratamiento de datos personales, incluidos los que se realicen en el marco de la oferta de productos y la prestación de servicios financieros y cuasifinancieros mediante el uso de diferentes tecnologías digitales.

Ante el crecimiento y expansión de los servicios y productos financieros y cuasifinancieros mediados por tecnologías digitales, la Superintendencia de Industria y Comercio ha identificado la necesidad de instruir a sus sujetos vigilados que operan en el ecosistema fintech sobre los principios, derechos y deberes en materia de protección de datos personales.

Las instrucciones que aquí se adoptan no son aplicables a los sujetos que realicen tratamiento de datos personales en el contexto del uso de tecnologías digitales para la prestación de servicios financieros que, de conformidad con el ámbito de aplicación material y personal de la Ley 1266 de 2008, son vigilados por la Superintendencia Financiera de Colombia.

En efecto, según el artículo 17 de la Ley Estatutaria 1266 de 2008, la Superintendencia de Industria y Comercio está llamada a ejercer "*la función de vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial [y] de servicios […], en cuanto se refiere a la actividad de administración de datos personales*", salvo que tales operadores, fuentes y usuarios sean entidades vigiladas por la Superintendencia Financiera de Colombia.

Por todo lo anterior, la Superintendencia de Industria y Comercio, en ejercicio de sus facultades de "*impartir instrucciones sobre las medidas y procedimientos necesarios para la adecuación* [a la ley] *de las operaciones de los Responsables y Encargados del Tratamiento"* que le confiere la Ley 1581 de 2012 (artículo 21, literal e) y de "i*mpartir instrucciones y órdenes sobre la manera como deben cumplirse las disposiciones* [legales] *relacionadas con la administración de la información financiera, crediticia* [y] *comercial*" que le confiere la Ley 1266 de 2008 (artículo 17, numeral 1), **instruye** a sus sujetos vigilados, esto es, a quienes ofrecen productos o prestan servicios de financiación, depósitos de bajo monto y otros afines que faciliten la inclusión financiera mediante tecnologías digitales y para ello realicen tratamiento de datos personales en cualquiera de los roles previstos por las leyes, ya en su condición de responsables, encargados, fuentes o usuarios, en los siguientes términos:

Instrucciones

1. El tratamiento de datos personales en el contexto de las operaciones de crédito, la prestación de servicios de financiación, los depósitos de bajo monto y otros productos o servicios afines que faciliten la inclusión financiera mediante el uso de tecnologías digitales 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 a las normas aplicables a la prestación de dichos servicios y a la celebración de tales contratos, y a los aspectos administrativos, contables, fiscales e históricos de la información.

2. El tratamiento de datos personales debe limitarse a aquellos datos que sean idóneos y necesarios para cumplir las finalidades constitucionalmente legítimas para las cuales se recolectan. Los responsables del tratamiento deben aplicar criterios para minimizar el tratamiento de datos personales, conforme al principio de necesidad. Por ejemplo, las aplicaciones por medio de las cuales se accede al servicio o producto

no podrán acceder a la galería de imágenes del dispositivo o a la lista de contactos del dispositivo con fines de cobranza.

3. El tratamiento de datos personales debe incluir procedimientos que aseguren la obtención, antes de iniciar el tratamiento de los datos personales, de la autorización libre, expresa e informada del titular, salvo las excepciones establecidas en la ley. Asimismo, se debe informar al titular sobre cuáles son los datos personales que serán recolectados, en especial, cuando estos sean considerados sensibles, conforme a los artículos 5 y 6 de la Ley 1581 de 2012, y sobre las finalidades específicas que justifican su tratamiento.

   En las aplicaciones disponibles para instalación es el titular quien debe decidir si otorga acceso a la información personal a través de su dispositivo, como, por ejemplo, el acceso a su ubicación o a la cámara. La autorización podrá solicitarse de forma dinámica, cuando el titular utilice una funcionalidad que requiera dicho acceso. En todo caso, debe informarse de manera clara y sencilla la finalidad de cada acceso en el momento específico en que se otorgue la autorización, a fin de que el titular pueda tomar una decisión informada sobre el uso de sus datos personales.

4. La autorización para el tratamiento de datos personales la puede expresar el titular de la información por cualquier medio y debe estar disponible para la consulta del titular y de la autoridad.

   En los casos en que se solicite autorización para el tratamiento de datos personales con finalidades adicionales a aquellas estrictamente necesarias para la celebración del contrato o la prestación del servicio, las finalidades deben presentarse de manera diferenciada.

   Los responsables deben solicitar la autorización presentando de forma diferenciada las finalidades al menos en dos grupos: las finalidades necesarias y las finalidades accesorias. Por ejemplo, son finalidades accesorias, el envío de publicidad o la oferta de otros servicios.

   El titular tiene el derecho a oponerse, en cualquier momento, al tratamiento de sus datos personales que haya sido autorizado para la realización de finalidades accesorias a la ejecución del contrato o la prestación del servicio, sin que su negativa afecte la continuidad del (o el acceso al) servicio principal.

5. El tratamiento de datos biométricos es particularmente crítico para la adecuada prestación de servicios de financiación, operaciones de crédito, depósitos de bajo monto y otros afines que faciliten la inclusión financiera mediante tecnologías digitales.

   Por su carácter de datos sensibles, la recolección y el tratamiento de datos biométricos está especialmente regulada por la Ley y requiere de una diligencia reforzada, por tanto:

5.1 Al momento de la recolección, el responsable del tratamiento debe:

   a. Informar al titular, de manera específica, las finalidades precisas para las cuales se tratarán sus datos biométricos y por qué la recolección de estos datos es necesaria. Entre las finalidades precisas y necesarias pueden considerarse: la prevención del fraude, la autenticación o verificación de su identidad, los controles de acceso, la actualización de sus datos personales, la validación de transacciones consideradas de riesgo alto y el trámite de reclamaciones relacionadas con la ejecución del contrato.

   b. Obtener del titular la autorización explícita para la recolección y tratamiento de sus datos biométricos, de conformidad con la necesidad y las finalidades precisas informadas.

5.2 Durante todo el ciclo de tratamiento, tanto el responsable como el encargado deben:

   a. Abstenerse de utilizar los datos biométricos para finalidades no explícitamente consentidas por el titular.

   b. Contar con medidas de seguridad adicionales que garanticen la protección de los datos biométricos.

   c. Tomar las medidas razonables para asegurar que el tratamiento de datos biométricos sea proporcional al nivel de riesgo de la actividad de la que se trate.

d. Abstenerse de compartir con terceros los datos biométricos recolectados y de alimentar bases de datos biométricos centralizadas o integradas, sin perjuicio de que los encargados accedan y traten dichos datos personales en cumplimiento de las instrucciones del responsable.

e. Proceder al borrado de los datos biométricos en un término razonable una vez haya terminado la relación contractual con el titular y no subsistan las finalidades precisas para las cuales se autorizó su tratamiento.

6. Los sujetos obligados deben establecer mecanismos sencillos y ágiles, que se encuentren permanentemente disponibles, para el ejercicio de los derechos de los titulares a conocer, rectificar, actualizar y suprimir sus datos personales, en los términos del artículo 15 de la Constitución, la Ley 1266 de 2008, la Ley 1581 de 2012 y la jurisprudencia constitucional.

   El procedimiento para la actualización, rectificación y supresión de los datos personales debe ser igual de ágil y sencillo que el procedimiento para la recolección y captura de los datos personales.

   Una mención a los mecanismos para el ejercicio de estos derechos debe incluirse en la Política de Tratamiento de Datos o en cualquier otro medio que facilite su ubicación y conocimiento por parte de los titulares.

7. Los sujetos obligados deben informar al titular sobre el uso dado o que se le dará a su información personal. Los sujetos obligados deben implementar medidas para la adecuada comprensión del titular sobre cómo se realiza el tratamiento de sus datos personales. La información debe ser completa, clara y de fácil lectura, sin barreras técnicas que impidan su acceso.

   Se recomienda adoptar mecanismos en los que los titulares puedan configurar sus preferencias de privacidad y decidir sobre la entrega de sus datos personales a terceros desde el diseño de las aplicaciones. Implementar estas estrategias con efectividad podrá ser valorado en el contexto del cumplimiento del principio de responsabilidad demostrada.

8. Según el principio de transparencia, el titular tiene derecho a recibir una explicación clara y comprensible sobre cualquier decisión automatizada que le resulte desfavorable. Esta explicación incluirá, como mínimo, una descripción general de la

lógica y criterios principales utilizados por el sistema, así como los factores más frecuentes que puedan influir en el resultado.

Cuando, por la naturaleza del sistema o para proteger secretos comerciales, derechos de propiedad intelectual u otras obligaciones legales, no sea posible explicar con detalle el proceso que llevó a la decisión, la información se presentará de manera general o agrupada por tipos de factores. En todo caso, se asegurará que el titular pueda entender los elementos principales que llevaron a la decisión.

La información relacionada con tratamientos automatizados de datos personales que tengan la vocación de generar un impacto significativo, entendido como aquel que pueda afectar de manera relevante los derechos e intereses de los titulares, deberá estar disponible de forma clara y accesible en la Política de Tratamiento de Datos, así como en los términos y condiciones.

Cuando las tecnologías automatizadas correspondan a sistemas de inteligencia artificial, 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*".

9. Los sujetos obligados deben adoptar medidas de seguridad razonables para la protección de los datos personales sometidos a tratamiento. Por tanto, deben adoptar medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole para evitar la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento de la información personal.

   Las medidas de seguridad implementadas deben revisarse de manera periódica, adaptándose a la evolución de los riesgos y al estado del arte en materia de seguridad de la información. Las medidas de seguridad implementadas deben estar documentadas y ser apropiadas al tipo y nivel de riesgo, así como ser verificables por las autoridades para su evaluación y mejora permanentes.

10. Los sujetos obligados que adelanten gestiones de cobranza de forma directa, por medio de terceros o por cesión de la obligación, deben abstenerse de contactar tanto a las referencias personales suministradas por los titulares, como a las personas relacionadas en la lista de contactos de los dispositivos de los titulares, salvo que para ello se cuente con la debida autorización del titular de los datos. El

cumplimiento de estos deberes es objeto especial de vigilancia y control, conforme a lo establecido en las leyes 1266 de 2008, 1581 de 2012 y 2300 de 2023, y la Circular Externa 001 del 26 de junio de 2024 de esta Superintendencia.

11. Los sujetos obligados deben definir de manera expresa y documentada sus roles en el tratamiento de datos personales, conforme a lo dispuesto en la Ley 1581 de 2012, la Ley 1266 de 2008 y sus normas reglamentarias. Cuando se realicen transmisiones de datos personales, en el marco del principio de responsabilidad demostrada, estas deben formalizarse mediante el respectivo contrato de transmisión de datos personales. En los casos en que la comunicación de datos se realice entre responsables del tratamiento, deben contar con la autorización previa, expresa e informada del titular, salvo las excepciones establecidas en la ley.

    En todo caso, si se evidencia que un sujeto obligado, aun cuando haya sido designado formalmente como encargado del tratamiento, determina en la práctica los fines y los medios del tratamiento de los datos personales, se considerará responsable del tratamiento. En tal condición, asumirá las obligaciones previstas para este rol en el régimen de protección de datos personales.

12. Los sujetos obligados que realicen transferencias o transmisiones internacionales de datos personales deben:

    a. Validar que el encargado o responsable destinatario esté ubicado en un Estado que cuente con un nivel adecuado de protección de datos personales, conforme al numeral 3.2 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

    b. En caso de que la transferencia o transmisión se realice a un Estado que no cuente con un nivel adecuado de protección de datos personales conforme el párrafo anterior, el responsable del tratamiento debe validar que la operación se encuentre dentro de las excepciones establecidas en el artículo 26 de la Ley 1581 de 2012.

    c. En caso de que no se encuentre dentro de las excepciones de la Ley, debe verificar que el Estado al que se transfieren o transmiten los datos personales cumpla con los estándares fijados en el numeral 3.1 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

d. Finalmente, si la transferencia no se encuentra en el escenario anterior, debe solicitar declaración de conformidad ante la Delegatura para la Protección de Datos Personales, en los términos del numeral 3.3 del Título V de la Circular Única de la Superintendencia de Industria y Comercio.

13. Suscribir y adecuar la conducta a las cláusulas contractuales modelo 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*" constituye una medida apropiada y efectiva para demostrar la implementación del principio de responsabilidad demostrada en las transferencias internacionales de datos personales.

CIELO ELAINNE RUSINQUE URREGO

Firmado digitalmente por CIELO ELAINNE RUSINQUE URREGO

CIELO ELAINNE RUSINQUE URREGO
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Daniel Ospina Celis
Revisó: Juan Carlos Upegui
Aprobó: Alejandro Bustos / Juan Carlos Upegui