Superintendencia de Industria y Comercio

BORRADOR PARA COMENTARIOS DE LA CIUDADANÍA

CIRCULAR EXTERNA No. _____ DE 2026
( )

Para: Operadores de telecomunicaciones, entidades crediticias o financieras y demás personas jurídicas o naturales que en el marco de su actividad comercial y el giro ordinario de sus negocios originen obligaciones dinerarias, celebren contratos de mutuo, de apertura de crédito, de financiación o similares con personas naturales, en su condición de sujetos vigilados por la Superintendencia de Industria y Comercio en su rol de Autoridad Nacional de Protección de Datos Personales.

Asunto: Instrucciones sobre mecanismos, herramientas y metodologías para la plena identificación del potencial adquirente de bienes y servicios, en desarrollo del parágrafo 1 del artículo 5 de la Ley Estatutaria 2573 de 2026.

Consideraciones

Sobre la suplantación

El artículo 15 de la Constitución Política de 1991 reconoce a todas las personas el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, y dispone que en la recolección, tratamiento y circulación de datos se respetarán la libertad y las demás garantías consagradas en la Constitución. La suplantación de identidad afecta de manera directa ese derecho. Cuando un tercero adquiere un bien o servicio a nombre de otra persona, la información que se registra en las bases de datos y que luego circula hacia los operadores de información financiera, crediticia y comercial, no es veraz respecto de su titular. La persona suplantada termina asociada a obligaciones que no contrajo, sometida a gestiones de cobro y, con frecuencia, reportada negativamente, con efectos sobre su acceso al crédito, a los servicios y, en general, sobre su vida económica.

A ello se suma la transformación tecnológica del fraude. La inteligencia artificial generativa permite hoy producir documentos sintéticos, fotografías y videos de rostros inexistentes o manipulados y voces clonadas a un costo muy bajo. Un estudio en el contexto de Estados Unidos proyectó que las pérdidas por fraude en el sector bancario podrían pasar de 12.300 millones de dólares en 2023 a 40.000 millones en 2027 como consecuencia del uso indebido de sistemas de inteligencia artificial para facilitar el fraude y la suplantación[1].

[1] Satish Lalchand, Val Srinivas, Brendan Maggiore y Joshua Henderson, "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking", Deloitte Center for Financial

En respuesta a esta problemática, el Congreso de la República expidió la Ley Estatutaria 2573 de 2026, que tiene por objeto "la adopción de medidas, procesos y políticas por parte de los operadores de telecomunicaciones y las entidades financieras-crediticias y demás establecimientos comerciales con esta competencia, para proteger los derechos de las personas suplantadas en su identidad de reportes negativos ante operadores de información y el cobro de obligaciones". Esta ley aborda dos dimensiones. La primera es reactiva y se refiere a lo que debe ocurrir cuando una persona reporta una posible suplantación. La segunda es preventiva y exige que, antes de contratar con una persona natural un bien o servicio, el proveedor adopte medidas que le permitan establecer razonablemente que quien lo solicita es quien dice ser. La presente circular se ocupa de esta segunda dimensión.

Sobre la verificación de identidad

Para precisar el alcance de esa obligación conviene distinguir entre la *identificación* de una persona y la *verificación* de su identidad. En el ordenamiento jurídico colombiano, la identificación de las personas es una función pública atribuida a la Registraduría Nacional del Estado Civil, a la que corresponden "el registro civil y la identificación de las personas" (artículo 266 de la Constitución Política). Es la Registraduría la que asigna a cada persona un número único de identificación, la que expide la cédula de ciudadanía en sus formatos físico y digital y la que custodia el Archivo Nacional de Identificación, que contiene los datos biográficos y biométricos de los ciudadanos.

En ese sentido, los particulares no identifican a las personas, sino que verifican que la identidad que alguien declara efectivamente le corresponde. La verificación de identidad es un proceso de aproximación que se expresa en grados de confianza y no es un proceso cierto y determinista. Por eso, las directrices de identidad digital del Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST, por sus siglas en inglés) definen la comprobación de identidad (*identity proofing*) como el proceso de establecer una relación entre un sujeto y una persona real "con un grado de aseguramiento determinado"[2]. Esa comprobación suele descomponerse en tres resultados verificables, que varios de los insumos recibidos por esta Superintendencia recogen con acierto[3]: la autenticidad y

Services, 29 de mayo de 2024. Disponible en: https://www.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html

[2] Temoshok D, Abruzzi C, Choong YY, Fenton JL, Galluzzo R, LaSalle C, Lefkovitz N, Regenscheid A, Vachino M. (2025). *Digital Identity Guidelines: Identity Proofing and Enrollment*. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-63A-4. Disponible en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63A-4.pdf

[3] Véanse, entre otros, los comentarios remitidos a esta Superintendencia por AlianzaIn, Olimpia IT y la Universidad Externado de Colombia en el marco de la consulta sobre la reglamentación de la Ley 2573 de 2026, abierta al público entre septiembre y octubre de 2026.

vigencia del documento o la credencial que se presenta; la correspondencia entre la persona que solicita el producto y el titular de esa identidad; y, cuando está disponible, la confirmación de los atributos de la identidad contra una fuente oficial. Ninguno de esos resultados aislado basta. Un documento auténtico puede ser presentado por quien no es su titular, y una persona real puede estar presentando atributos de otra[4].

Por lo anterior, la expresión "plena identificación del potencial adquirente", empleada en el parágrafo 1 del artículo 5 de la Ley 2573 de 2026, no puede interpretarse como una exigencia de certeza absoluta o de riesgo cero, que ningún mecanismo técnico está en capacidad de ofrecer. Debe entenderse, en armonía con el numeral 1 del mismo artículo, que exige medidas "suficientes y razonables", como la obtención de evidencia suficiente, verificable y proporcional al riesgo de la operación, que permitan alcanzar un nivel adecuado de confianza en que la identidad declarada corresponda a la persona que pretende adquirir el bien o servicio. El objetivo de la verificación es aproximarse a la identidad de la persona tanto como el riesgo lo requiera para impedir que un tercero se haga pasar por ella.

Los factores o categorías por medio de los cuales una persona puede demostrar su identidad son por lo general tres: algo que se sabe, algo que se tiene y algo que se es[5]. En el contexto de la Unión Europea, por ejemplo, se definen los factores de autenticación en los siguientes términos[6]:

> *"2. «factor de autenticación»: un factor confirmado como vinculado a una persona, que se encuentra en alguna de las categorías siguientes:*
> *a) «factor de autenticación basado en la posesión»: factor de autenticación en el que el sujeto está obligado a demostrar posesión del mismo;*
> *b) «factor de autenticación basado en el conocimiento»: factor de autenticación en el que el sujeto está obligado a demostrar conocimiento del mismo;*
> *c) «factor de autenticación inherente»: factor de autenticación que se basa en un atributo físico de una persona física del cual el sujeto está obligado a demostrar su posesión".*

El factor de conocimiento (lo que se sabe) comprende contraseñas, números de identificación personal y respuestas a preguntas cuya respuesta se presume conocida solo por el titular. El factor de posesión (lo que se tiene) comprende objetos físicos o digitales bajo control del titular, como el documento de identidad, una tarjeta, un teléfono móvil,

---

[4] Paggio, V., Nikolouzou, E. y Dekker M. (2022). *Remote Identity Proofing: Attacks and Countermeasures*. European Union Agency for Cybersecurity, ENISA. Disponible en: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Remote%20Identity%20Proofing%20-%20Attacks%20%26%20Countermeasures.pdf

[5] O'Gorman, L. (2003). "Comparing Passwords, Tokens, and Biometrics for User Authentication." *Proceedings of the IEEE* 91, No. 12, pp. 2019-2040. DOI: 10.1109/JPROC.2003.819605.

[6] Reglamento de Ejecución (UE) 2015/1502 de la Comisión, de 8 de septiembre de 2015. Punto 1 del Anexo. Disponible en: https://eur-lex.europa.eu/eli/reg_impl/2015/1502/oj.

una línea telefónica, un dispositivo registrado, un *token* o una llave criptográfica. El factor de inherencia (lo que se es) comprende características biológicas o de comportamiento de la persona, como el rostro, las huellas dactilares, el iris, la voz o la forma en que interactúa con un dispositivo. La Superintendencia Financiera de Colombia acoge esta misma clasificación en la Circular Básica Jurídica, en la que define los factores de autenticación como "algo que se sabe, algo que se tiene, algo que se es"[7].

Estos factores son vulnerables y, si se implementan de manera aislada, no es posible verificar la identidad de una persona con un alto grado de confianza. En consecuencia, cada factor se encuentra expuesto a distintas causas que materializan el riesgo de fallar en la verificación de la identidad, respectivamente señalamos a continuación lo que compromete a cada uno:

- Los factores de conocimiento se ven comprometidos por las filtraciones masivas de datos y por la ingeniería social.
- Los factores de posesión se ven comprometidos por el robo de dispositivos, la reposición fraudulenta de tarjetas SIM y la portabilidad no autorizada de números, que permiten a un tercero recibir los códigos de un solo uso enviados al titular.
- Los factores de inherencia, por su parte, son vulnerables a los ataques de presentación, en los que se exhibe ante el sensor una fotografía, un video, una máscara o un rostro sintético, y a los ataques de inyección, en los que se sustituye la cámara por una fuente virtual que introduce directamente en el sistema imágenes o videos manipulados, incluidos los generados con inteligencia artificial.

Los avances tecnológicos recientes han posicionado a la biometría como un mecanismo destacado en los procesos de vinculación no presencial. Pero no es el único mecanismo idóneo ni está exento de limitaciones[8]. Varios de los comentarios recibidos advierten con razón que la certificación de prueba de vida, incluso en su nivel más alto, evalúa la resistencia a los ataques de presentación, pero no a los ataques de inyección, que requieren controles y evaluaciones propios. En el mismo sentido, la Agencia Española de Protección de Datos (AEPD) y el Supervisor Europeo de Protección de Datos (SEPD) han advertido que, incluso tratándose de uno de los mecanismos tecnológicamente más avanzados, "sólo utilizar biometría es un proceso de autenticación débil"[9].

---

[7] Superintendencia Financiera de Colombia. Circular Externa 006 de 2025 (Circular Básica Jurídica), Parte I, Título II, Capítulo I, numerales 2.2.5, 2.2.6 y 2.3.3.1.27.
[8] Anil K. Jain, Arun Ross y Salil Prabhakar. (2004). "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology* 14, No. 1, pp. 4-20. DOI: 10.1109/TCSVT.2003.818349.
[9] Agencia Española de Protección de Datos (AEPD). (2020). *14 equívocos con relación a la identificación y autenticación biométrica*. Disponible en: https://www.edps.europa.eu/sites/default/files/publication/joint_paper_14_misunderstandings_with_regard_to_identification_and_auuthentication_es.pdf

De lo anterior se desprende el principio central de la verificación de identidad contemporánea y sobre el que se basan las presentes instrucciones: ningún factor aislado es suficiente cuando el riesgo es significativo. Para generar confianza es necesario combinar múltiples factores de autenticación. Este estándar es coherente con las buenas prácticas internacionales. En el ámbito europeo, por ejemplo, el artículo 4.30 de la Directiva (UE) 2015/2366 (PSD2) define la autenticación reforzada de clientes como la basada en dos o más elementos independientes de las tres categorías arriba mencionadas.

Los mecanismos de verificación deben, además, ser sensibles al contexto. No existe un mecanismo óptimo en abstracto. Su idoneidad depende del riesgo de la operación, que varía según se trate de la apertura de un crédito, de la activación de un plan pospago, de la reposición de una tarjeta SIM o de la consulta de un saldo. Depende también de las características de la operación, como el canal, el monto y la existencia de una relación previa con el titular, y de las condiciones tecnológicas disponibles, como el tipo de dispositivo, la conectividad y el acceso a fuentes oficiales. Por último, depende de la población a la que se dirige el servicio. La Corte Constitucional, al revisar el proyecto que se convirtió en la Ley 2573 de 2026, destacó esta misma idea al señalar que el nivel de seguridad del método de validación "debe ser proporcional al riesgo de una operación o transacción determinada" y que "diferentes sectores pueden enfrentar distintos tipos de amenazas"[10].

La verificación de identidad tampoco se agota en el momento de la vinculación. Con frecuencia, el primer eslabón de un esquema de fraude por suplantación no es la obtención de un crédito o la contratación de un servicio, sino una operación que por sí misma no genera obligaciones económicas, como la reposición de una tarjeta SIM, la actualización de los datos de contacto, la recuperación de las credenciales de acceso o la vinculación de un nuevo dispositivo. Mediante estas operaciones, un tercero toma control de los canales por los que el titular recibe códigos, notificaciones y alertas y, a partir de allí, puede adquirir productos o servicios a su nombre sin que este lo advierta. Por esa razón, en desarrollo del deber de adoptar "medidas de seguridad digital suficientes y razonables" (numeral 1 del artículo 5 de la Ley 2573 de 2026), del principio de seguridad (literal g del artículo 4 de la Ley 1581 de 2012) y del deber de conservar la información bajo las condiciones de seguridad necesarias para impedir su "uso o acceso no autorizado o fraudulento" (literal d del artículo 17 de la misma ley), las presentes instrucciones se orientan también a los procesos de verificación de identidad en las operaciones posteriores a la vinculación que presenten un riesgo alto de suplantación.

Ello no significa que la verificación de identidad de la que trata esta circular se extienda a cualquier operación. Quedan por fuera, por ejemplo, las transacciones y los pagos que el titular realiza en el uso ordinario de sus productos y servicios, cuya seguridad se rige por las normas y los mecanismos de autenticación propios de cada sector.

[10] Corte Constitucional. Sentencia C-413 de 2025, párrafo 496.

Sobre la identidad digital pública

La verificación de identidad no es solamente un asunto del sector privado. La identidad digital se reconoce hoy como uno de los elementos de la infraestructura pública digital. El Marco Universal de Salvaguardas para la Infraestructura Pública Digital, publicado en septiembre de 2024 por la Oficina del Enviado del Secretario General para la Tecnología (hoy Oficina de Tecnologías Digitales y Emergentes) y el PNUD, ofrece lineamientos para que estas infraestructuras sirvan al interés público y protejan los derechos de las personas[11]. Múltiples agencias y organizaciones internacionales se han sumado a la apuesta por la identificación pública. Por ejemplo, el Banco Mundial y otras organizaciones actualizaron en 2021 los *Principios sobre Identificación para el Desarrollo Sostenible*. Dichos principios buscan "establecer una identidad confiable: única, segura y precisa", "utilizar estándares abiertos y evitar la dependencia de proveedores y tecnologías" y "proteger la privacidad y la capacidad de acción de las personas mediante el diseño de sistemas"[12].

La identidad oficial, entendida en ocasiones como fuente de verdad, es una infraestructura sobre la que el sector privado puede construir procesos de verificación más confiables, sin necesidad de replicar bases de datos de identidad ni de multiplicar la recolección de datos biométricos. Colombia ha avanzado de manera significativa en esa dirección. El Decreto 620 de 2020, que subroga el Título 17 del Decreto 1078 de 2015, reglamentó los servicios ciudadanos digitales, que comprenden la interoperabilidad, la carpeta ciudadana digital y la autenticación digital. Esta última se entiende en los siguientes términos:

> *ARTÍCULO 2.2.17.2.1.1. (…)*
>
> *1.2. Servicio de autenticación digital: Es el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin prejuicio de la autenticación notarial.*

Aunque el Decreto 1078 de 2015 define los mecanismos de autenticación únicamente como las firmas digitales o electrónicas, crea el primer escalón en la construcción de un sistema de identidad digital en el país a partir de la identificación por medios digitales:

---

[11] Oficina del Enviado del Secretario General para la Tecnología y PNUD, Universal DPI Safeguards Framework, septiembre de 2024. Disponible en: https://www.dpi-safeguards.org

[12] Banco Mundial y otros, *Principios sobre identificación para el desarrollo sostenible: hacia la era digital*, segunda edición (febrero de 2021). Disponible en: https://documents1.worldbank.org/curated/en/371801496861423208/pdf/Principles-on-Identification-for-Sustainable-Development-Toward-the-Digital-Age.pdf

ARTÍCULO 2.2.17.1.3. Identificación por medios digitales. La identificación por medios digitales, a través de la cédula de ciudadanía digital y por biometría se regirá por las disposiciones que para tal efecto expida la Registraduría Nacional del Estado Civil, en el marco de sus competencias.

En desarrollo de dicho mandato, la Registraduría Nacional del Estado Civil presentó por medio de la Circular Externa No. 011 del 5 de febrero de 2021 la cédula digital, que incorpora un registro de biometría facial. Sin embargo, la Circular Única de la Registraduría Nacional del Estado Civil es clara en establecer que "la cédula de ciudadanía tiene validez en los dos formatos en que se expide, es decir, la cédula amarilla con hologramas y la cédula de ciudadanía digital en sus dos versiones". Esto supone que por ahora la RNEC cuenta con la información del registro facial de quienes han tramitado la cédula digital y no de toda la población.

El estado actual del desarrollo de la infraestructura pública de identidad en Colombia es relevante para los protocolos de los que trata la Ley 2573 de 2026 por al menos tres motivos. Primero, la Registraduría es la única fuente oficial de la identidad de los nacionales colombianos, de modo que el cotejo contra sus bases de datos, cuando sea jurídica y técnicamente posible, ofrece el mayor nivel de confianza en la correspondencia entre una persona y la identidad que declara. Segundo, la disponibilidad del servicio de cotejo contra una base de datos oficial de biométricos faciales es todavía parcial y está sujeta a condiciones de acceso, costos y disponibilidad. Tercero, las instrucciones de esta Superintendencia deben orientar a los sujetos obligados hacia el uso de las infraestructuras públicas de identidad a medida que se habiliten, mas en su ausencia no pueden supeditar el cumplimiento de la ley a una única forma de verificación de identidad.

Los sistemas de identidad digital también permiten la reutilización de identidades ya verificadas mediante credenciales verificables, esto es, declaraciones electrónicas de atributos de una persona emitidas por una entidad confiable, que el titular conserva y presenta cuando lo necesita, y cuya autenticidad, integridad y vigencia puede comprobar quien las recibe sin repetir el proceso de verificación. La Unión Europea adoptó este modelo a partir de la expedición del Reglamento (UE) 2024/1183, que modificó el Reglamento eIDAS y creó la cartera europea de identidad digital. Una verificación robusta, realizada una vez y reutilizada bajo el control del titular, puede reducir el número de veces que una persona entrega su documento o sus datos biométricos a distintas empresas y, con ello, su exposición a filtraciones y suplantaciones. Por tal motivo, las presentes instrucciones valoran como buena práctica la adopción de estos esquemas verificados en los que se minimiza el tratamiento de datos personales biométricos, sin aumentar los riesgos asociados a la suplantación.

Sobre la participación ciudadana y el proceso de reglamentación

En la elaboración de esta circular, la Superintendencia de Industria y Comercio adelantó un proceso de consulta pública en el que recibió más de cien aportes de empresas, gremios,

proveedores de tecnología, universidades, organizaciones de la sociedad civil y ciudadanos. A través de un formulario web que se puso a disposición del público en la sede electrónica de la entidad y sus redes sociales, se formularon dieciséis preguntas sobre distintos asuntos técnicos, jurídicos y de política pública relacionados con los procesos de verificación de identidad. Ochenta y tres personas, organizaciones, empresas o asociaciones respondieron el formulario y compartieron sus insumos con la entidad. Asimismo, la entidad recibió más de veinte documentos con propuestas concretas sobre los protocolos de validación de identidad a través de correo electrónico. De manera complementaria, el equipo de la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio realizó siete sesiones de trabajo técnicas con actores del sector privado relevantes en el proceso de verificación de identidad.

A partir de las propuestas recibidas, de la información recolectada en las sesiones de trabajo, del conocimiento experto de la Superintendencia de Industria y Comercio y de las buenas prácticas y estándares internacionales disponibles, esta entidad publicó para comentarios de la ciudadanía una primera versión de la presente circular el XX de noviembre de 2026. Se recibieron XX comentarios de la ciudadanía y de los actores interesados, los cuales fueron debidamente analizados, respondidos y, cuando correspondió, incorporados al texto de la circular.

Finalizado el proceso de participación ciudadana, la Delegatura para la Protección de Datos Personales sometió el borrador de la regulación al trámite de abogacía de la competencia en virtud de lo dispuesto en el artículo 7 de la Ley 1340 de 2009 bajo el radicado XX.

Asimismo, la Superintendencia de Industria y Comercio realizó múltiples sesiones de coordinación con la Superintendencia Financiera de Colombia y el Ministerio de Tecnologías de la Información y las Comunicaciones en las que se determinó que cada superintendencia expediría una reglamentación autónoma. En todo caso, se buscó que sendos procesos regulatorios fueran armónicos y devinieran en estándares relativamente similares, ajustados a la naturaleza diversa de los sujetos vigilados por cada superintendencia.

Sobre el marco jurídico que fundamenta la presente circular

El artículo 5 de la Ley 2573 de 2026 establece como deber de los operadores de telecomunicaciones, de las entidades financieras o crediticias y de los demás establecimientos comerciales con esta competencia, entre otros, "adoptar las medidas de seguridad digital suficientes y razonables necesarias para establecer la veracidad de la identidad de las personas y los documentos presentados para adquirir sus productos y/o servicios" (numeral 1). En desarrollo de dicho deber, el parágrafo 1 del mismo artículo dispone lo siguiente:

> *Parágrafo 1º. De conformidad con el numeral 1 del artículo 2 del Decreto 1064 de 2020, la Ley 1266 de 2008 y la Ley 1581 de 2012 dentro de los 6 meses siguientes a la expedición de la presente ley, la Superintendencia de Industria y Comercio SIC y la*

Superintendencia Financiera, en coordinación con el Ministerio de Tecnologías de la Información y las Comunicaciones, en el marco de cada una de sus competencias deberán reglamentar los protocolos para atender oportunamente los reportes de posible suplantación por parte de los operadores de telecomunicaciones y las entidades financieras y/o crediticias y demás establecimientos comerciales con esta competencia en procesos de adquirir bienes o servicios de manera física y/o medios electrónicos por parte de particulares. Los protocolos deberán incluir mecanismos, herramientas y metodologías idóneos que permitan la plena identificación del potencial adquirente.

Junto con ese deber, el artículo 5 de la Ley 2573 de 2026 impone a los sujetos obligados el de "adoptar mecanismos suficientes y razonables que permitan validar la información que suministran las personas que adquieren sus productos y/o servicios" (numeral 3), y el de entregar a la persona presuntamente suplantada, a su solicitud, copia de la información y de los documentos aportados para la aprobación del producto o servicio solicitado a su nombre (numeral 7). En la misma línea, el literal d) del artículo 2 de la citada ley consagra el principio de carga dinámica de la prueba, según el cual "tendrá obligación de probar la parte que mejor se encuentre en condiciones de hacerlo", y precisa que, en materia de suplantación, los operadores de telecomunicaciones y las entidades financieras o crediticias deberán entregar la información y los documentos que recibieron para aprobar el bien o servicio.

Estos protocolos tienen consecuencias concretas. El parágrafo 2 del mismo artículo dispone que, cuando se verifique "el incumplimiento de los lineamientos, recomendaciones y protocolos de seguridad expedidos por las autoridades competentes" y el titular haya solicitado la corrección manifestando ser víctima de suplantación, procederán la suspensión de la gestión de cobranza, la modificación del reporte ante las centrales y los operadores de información, y la devolución oportuna de los dineros o la eliminación de las acreencias objeto de defraudación. Las instrucciones contenidas en esta circular constituyen, por tanto, uno de los referentes para valorar la diligencia de los sujetos obligados en la verificación de la identidad del potencial adquirente.

Por su parte, el artículo 7 de la Ley 2573 de 2026 modificó el artículo 7 de la Ley 2157 de 2021, que había adicionado el numeral II del artículo 16 de la Ley 1266 de 2008 con la leyenda "Víctima de Falsedad Personal". Esta leyenda "no podrá tenerse como un reporte negativo ni podrá ser causal de disminución en la calificación de riesgo ni alterar sus estudios financieros o crediticios". En el análisis del riesgo crediticio se tendrá en cuenta "con el único fin de realizar una verificación intensificada de la identidad del titular e impedir que esta situación se presente nuevamente".

Estas obligaciones se integran con el régimen general de protección de datos personales. La Ley 1581 de 2012 consagra, entre otros, el principio de libertad, según el cual el tratamiento "sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular" (literal c del artículo 4); el de veracidad o calidad, que exige que la información sujeta a tratamiento sea "veraz, completa, exacta, actualizada, comprobable y

comprensible" (literal d del artículo 4), y el de seguridad, que obliga a manejar la información con las medidas técnicas, humanas y administrativas necesarias para evitar su "adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento" (literal g del artículo 4). En el mismo sentido, el literal d) del artículo 17 impone a los responsables del tratamiento el deber de conservar la información bajo las condiciones de seguridad necesarias para impedir esos mismos riesgos. La suplantación de identidad supone, precisamente, que un tercero accede de manera fraudulenta a los productos y los datos de otra persona, y que en las bases de datos se registra información que no es veraz respecto del titular.

La Corte Constitucional, mediante la Sentencia C-413 de 2025, efectuó el control previo de constitucionalidad del proyecto de ley estatutaria y declaró exequible, en lo pertinente, el artículo 5. Al examinar la atribución de competencias regulatorias a las superintendencias, la Corte reiteró que "las superintendencias, como autoridades administrativas, son titulares de una potestad reglamentaria residual y subordinada en los temas especializados que hacen parte de la órbita de sus competencias"[13].

En la misma providencia, la Corte se refirió a la posibilidad de los sujetos obligados de seleccionar el mecanismo de validación de identidad que mejor se ajuste a sus necesidades, de la siguiente manera:

> *De otro lado, esta Corte considera que el hecho de que el numeral examinado disponga que el operador de telecomunicaciones o la entidad financiera, crediticia o comercial tiene la potestad de establecer la prueba de validación de identidad, no significa que pueda acudir a métodos que transgredan los derechos fundamentales de las personas. Lejos de dar vía libre al uso de mecanismos inconstitucionales, la disposición es un reflejo del contexto normativo, en el que, atendiendo a parámetros internacionales, se ha otorgado flexibilidad para que las entidades, dentro de un marco mínimo regulatorio, definan sus propias pruebas de validación de identidad, pues ello permite un enfoque más eficiente, adaptable y seguro en el proceso de autenticación, lo que favorece tanto a las empresas como a sus clientes.*
>
> *En ese sentido, permitir la selección del método de validación de identidad, dentro de las posibilidades que otorga el ordenamiento jurídico, es clave por razones como la adaptabilidad al riesgo, lo que significa que el nivel de seguridad del método de validación debe ser proporcional al riesgo de una operación o transacción determinada. Además, diferentes sectores pueden enfrentar distintos tipos de amenazas y asumir variados requisitos, ello sumado a que la capacidad de elegir y cambiar métodos de validación permite a las entidades adaptarse rápidamente frente a amenazas y vulnerabilidades emergentes, lo que en el entorno digital es determinante debido a la velocidad con la que evolucionan tales riesgos*[14]*.*

[13] Corte Constitucional. Sentencia C-413 de 2025, párrafo 465.
[14] Corte Constitucional. Sentencia C-413 de 2025, párrafos 495 y 496.

Por otro lado, el ordenamiento jurídico colombiano establece normas estrictas sobre el tratamiento de datos personales sensibles. El artículo 5 de la Ley 1581 de 2012 define dichos datos como "aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos." Asimismo, el Decreto 1074 de 2015 desarrolla las condiciones para realizar tratamiento de dicha información, así:

> *ARTÍCULO 2.2.2.25.2.3. 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.*
> *En el Tratamiento de datos personales sensibles, cuando dicho Tratamiento sea posible conforme a lo establecido en el artículo 6 de la Ley 1581 de 2012, deberán cumplirse las siguientes obligaciones:*
> *1. Informar al titular que por tratarse de datos sensibles no está obligado a autorizar su Tratamiento.*
> *2. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.*
> *Ninguna actividad podrá condicionarse a que el Titular suministre datos personales sensibles.*

En desarrollo de lo anterior, la Superintendencia de Industria y Comercio recuerda que, entre sus funciones como Autoridad Nacional de Protección de Datos Personales, dispuestas en el artículo 21 de la Ley 1581 de 2012, están las de "velar por el cumplimiento de la legislación en materia de protección de datos personales" e "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". Adicionalmente, el artículo 17 de la Ley Estatutaria 1266 de 2008 le atribuye la vigilancia de los operadores, las fuentes y los usuarios de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países que no estén sometidos a la vigilancia de la Superintendencia Financiera de Colombia.

Por todo lo anterior, la Superintendencia de Industria y Comercio, en ejercicio de la competencia conferida por el parágrafo 1 del artículo 5 de la Ley Estatutaria 2573 de 2026 y de la facultad de impartir instrucciones de la que trata el literal e) del artículo 21 de la Ley 1581 de 2012, instruye a sus sujetos vigilados en los siguientes términos:

Instrucciones

1. Ámbito de aplicación. Las presentes instrucciones se dirigen a los operadores de telecomunicaciones, a las entidades crediticias o financieras y a las demás personas jurídicas o naturales que en el marco de su actividad comercial y el giro ordinario de sus negocios originen obligaciones dinerarias, celebren contratos de mutuo, de apertura de crédito, de financiación o similares con personas naturales, que no se encuentren sometidos a la vigilancia de la Superintendencia Financiera de Colombia, en los procesos de adquisición o apertura de bienes o servicios por parte de particulares, sea de manera física o por medios electrónicos, o en las operaciones que por sus riesgos inherentes requieran verificar la identidad de quien las realiza.

Los sujetos obligados que, por la naturaleza de sus actividades, se encuentren también sometidos a la vigilancia de la Superintendencia Financiera de Colombia deberán adaptar sus operaciones a los lineamientos e instrucciones que expida dicha autoridad.

2. Principios orientadores. Las disposiciones de la presente circular se deben interpretar y desarrollar a la luz de los siguientes principios:

a) Enfoque basado en riesgos. Las medidas y tecnologías de verificación o validación de identidad, así como la intensidad del tratamiento de datos personales que las acompaña, deben ser proporcionales al riesgo de suplantación y a los posibles perjuicios para el titular que se derivarían de una suplantación. A mayor riesgo y mayor perjuicio, más robustas deben ser las medidas implementadas y más intenso puede ser el tratamiento de sus datos personales.
b) Verificación escalonada. La combinación sucesiva de diversos mecanismos y tecnologías de validación de identidad disminuye los riesgos de suplantación. Ningún mecanismo aislado es suficiente y por eso la confianza se construye a partir de la combinación de mecanismos que comprueben factores distintos e independientes.
c) Neutralidad tecnológica. Los sujetos obligados pueden elegir libremente los mecanismos, herramientas, sistemas y proveedores que empleen para cumplir con las instrucciones, siempre que estos garanticen un nivel adecuado de confianza y permitan cumplir con las disposiciones de la Ley 1581 de 2012. Asimismo, podrán adoptar y combinar mecanismos de verificación de identidad y utilizar las tecnologías disponibles que resulten apropiadas para el nivel de riesgo de cada operación.
d) Sensibilidad al contexto. La selección de mecanismos o tecnologías de validación de identidad debe atender al canal por medio del cual se adquiere o abre el bien o servicio, a las características de la operación, a la tecnología disponible y a la población destinataria del servicio.
e) Minimización y privacidad desde el diseño. Solo deben recolectarse los datos estrictamente necesarios y pertinentes para cumplir la finalidad enunciada, y los procesos deben diseñarse de manera que se reduzca el riesgo para el derecho a la protección de datos personales de los titulares.

f) Responsabilidad demostrada. Los sujetos obligados deben ser capaces de demostrar ante esta Superintendencia y ante el titular las medidas adoptadas, su fundamento en el análisis de riesgos y su aplicación en cada caso concreto.
g) Aprovechamiento de la infraestructura pública de identidad. Cuando sea jurídica y técnicamente posible, es deseable acudir a la verificación contra las fuentes de verdad oficiales y los servicios de identidad digital del Estado.
h) Mejora continua. Los mecanismos implementados para verificar la identidad deben evaluarse y actualizarse periódicamente.
i) Inclusión y no discriminación. Los mecanismos de verificación que implementen los sujetos obligados no deben excluir, por su diseño, a sujetos de especial protección constitucional.

3. Definiciones. Para efectos de las presentes instrucciones, se entenderá por:

a) *Identificación:* función pública a cargo de la Registraduría Nacional del Estado Civil, en virtud de la cual se establece y se documenta la identidad de las personas.
b) *Verificación o validación de identidad:* proceso mediante el cual un sujeto obligado obtiene evidencia de que la identidad declarada por quien pretende adquirir un bien o servicio existe, es auténtica y corresponde a esa persona con un nivel adecuado de confianza y proporcional al riesgo de la operación.
c) *Plena identificación del potencial adquirente:* resultado de un proceso de verificación o validación de identidad que, mediante evidencia suficiente, verificable y proporcional al riesgo de la operación, permite alcanzar un nivel suficiente y razonable de confianza en que la identidad declarada corresponde a la persona que pretende adquirir el bien o servicio.
d) *Autenticación:* proceso mediante el cual se confirma que quien interactúa con el sujeto obligado, en una operación posterior a la vinculación, es el mismo titular cuya identidad fue previamente verificada o validada.
e) *Factores de autenticación o verificación:* categorías de elementos con los que una persona puede demostrar su identidad, a saber: algo que se sabe (factor de conocimiento), algo que se tiene (factor de posesión) y algo que se es (factor de inherencia).
f) *Mecanismo de verificación:* procedimiento o tecnología concreta mediante la cual se verifica la identidad de una persona a partir de la comprobación de uno o múltiples factores.

4. Operaciones en las que se debe verificar la identidad. Los sujetos obligados deberán emplear mecanismos de verificación de identidad, como mínimo, en las siguientes operaciones:

a) La vinculación de un nuevo cliente y la apertura o adquisición de un nuevo producto o servicio que genere obligaciones económicas a cargo del titular, como el otorgamiento de créditos, la financiación de bienes, las ventas a plazos y la contratación de servicios de telecomunicaciones en la modalidad pospago.

b) Las operaciones que se consideren de alto riesgo, entre ellas, la reposición o el cambio de la tarjeta SIM, el cambio de titular de un producto o servicio, la actualización de los datos de contacto o de los canales en los que el titular recibe notificaciones, códigos o alertas, la recuperación de credenciales de acceso, la vinculación de un nuevo dispositivo a la cuenta del titular y el aumento del cupo o del monto de una obligación.
c) Las demás que, según un análisis de riesgos, presenten un riesgo relevante de suplantación. En todo caso, se recomienda aplicar mecanismos de verificación de identidad en otras operaciones cuando ello resulte pertinente para prevenir la suplantación.

5. Mecanismos de verificación de identidad. Los sujetos obligados podrán emplear, entre otros, los siguientes mecanismos de verificación de identidad en las operaciones de las que trata la instrucción anterior:

a) Cotejo biométrico facial o dactilar contra la información registrada en un documento de identidad oficial o contra la fuente oficial a través de la Registraduría Nacional del Estado Civil.
b) Análisis de patrones de uso y otros mecanismos de biometría pasiva para operaciones posteriores a la vinculación.
c) Códigos de verificación, tokens, *one time passwords* (OTP) u otros métodos de comprobación a través de factores de posesión.
d) Contraseñas u otros métodos de comprobación a través de factores de conocimiento.
e) Verificación documental a partir del análisis de la autenticidad de los documentos físicos.
f) Lectura de la información almacenada en el chip del documento de identidad, cuando este lo incorpore.
g) Consulta no biométrica de los atributos de identidad contra fuentes oficiales, directamente o a través de los operadores autorizados por la entidad responsable.
h) Autenticación mediante la cédula de ciudadanía digital o los servicios de autenticación digital del Estado.
i) Certificados de firma digital emitidos por entidades de certificación acreditadas, en los términos de la Ley 527 de 1999.
j) Verificación presencial del documento de identidad y de la persona por parte de personal capacitado.

No constituyen por sí solos mecanismos de verificación de identidad la presentación de una fotografía o copia del documento sin verificación de su autenticidad, el suministro de datos estáticos de la persona, como el número o la fecha de expedición del documento, las contraseñas de un solo uso enviadas a canales cuya titularidad no se haya verificado y el cotejo facial sin prueba de vida. Las preguntas sobre información del historial del titular podrán servir como señal complementaria de prevención del fraude, pero no como mecanismo de verificación de identidad.

Cuando esté disponible y sea técnica, jurídica y financieramente viable, los sujetos obligados priorizarán, entre los mecanismos de verificación de identidad, el uso de la infraestructura pública de identidad, en particular el cotejo contra la fuente oficial de la Registraduría Nacional del Estado Civil y los servicios de identidad digital del Estado.

6. Combinación de los mecanismos de verificación. En la vinculación de un nuevo cliente, los sujetos obligados deberán emplear, al menos, dos mecanismos independientes entre sí. En las demás operaciones de que trata la instrucción 4, se considerará una buena práctica si emplean, al menos, dos mecanismos que comprueben factores de autenticación de categorías distintas.

Los mecanismos que se combinen deberán ser, en la medida de lo posible, independientes entre sí, de modo que la vulneración de uno no comprometa al otro.

7. Verificación basada en riesgos. Los sujetos obligados deberán implementar los mecanismos de verificación de identidad en virtud del riesgo asociado a cada operación, canal o usuario. La frecuencia con la que se realiza la verificación, la intensidad del tratamiento de datos personales, la sensibilidad de la información objeto de tratamiento y la fricción para los usuarios son variables que se deben ajustar al riesgo. La robustez de los mecanismos y la fricción para el usuario podrán aumentar a medida que aumenta el riesgo.

Los sujetos obligados deberán contar con un análisis de riesgos de suplantación que sustente los mecanismos de verificación adoptados para cada tipo de operación y usuario. El análisis deberá considerar, como mínimo, el tipo de producto o servicio y el monto de la obligación, el canal (presencial, no presencial, otro), la existencia de una relación previa con el titular, su perfil y su comportamiento habitual, las señales del dispositivo y de la red, los eventos recientes asociados a la línea o la cuenta, el historial de reportes de suplantación y las características de la población a la que se dirige el servicio.

Con base en ese análisis, los sujetos obligados deberán clasificar las operaciones en, al menos, tres niveles de riesgo y asignar a cada nivel los mecanismos de verificación correspondientes. Para un mismo nivel de riesgo, la verificación en canales no presenciales deberá ser al menos igual de exigente que la realizada en canales presenciales.

El análisis de riesgos de suplantación deberá estar documentado y a disposición de esta Superintendencia cuando lo requiera.

8. Alternativas a los mecanismos biométricos. Los sujetos obligados no podrán condicionar la adquisición de un bien o servicio al suministro de datos biométricos. Antes de recolectarlos, deberán informar al titular que su suministro es facultativo y ofrecerle al menos una alternativa de verificación real, efectiva y accesible que permita alcanzar el nivel de confianza exigido para la operación, de acuerdo con el análisis de riesgos de que

trata la instrucción 7. La alternativa podrá implicar un canal distinto, un mayor tiempo de respuesta o, cuando el análisis de riesgos lo justifique de manera objetiva, condiciones distintas en la obligación, como un monto inicial menor.

Excepcionalmente, cuando un sujeto obligado considere que en un canal y para una población determinados no es posible alcanzar el nivel de confianza exigido mediante medidas menos gravosas para los derechos de los titulares que el tratamiento de datos biométricos, deberá acreditarlo en su análisis de riesgos. Dicho análisis deberá examinar cada una de las alternativas señaladas en esta circular, explicar las razones por las cuales no son viables y estar documentado y a disposición de esta Superintendencia cuando lo solicite. Esta Superintendencia valorará dicha acreditación de manera estricta y en cada caso concreto, en atención a que la imposición de mecanismos biométricos solo podría encontrarse justificada ante la absoluta imposibilidad de cumplir las obligaciones legales mediante medidas menos gravosas para los derechos de los titulares. En ese caso, el sujeto obligado deberá informar al titular, antes de recolectar sus datos, que sin ellos no podrá realizar la operación por ese canal.

9. Credenciales verificables y reutilización de la identidad verificada. La emisión y la aceptación de credenciales verificables que permitan reutilizar una identidad previamente verificada se considerarán medidas apropiadas y efectivas para demostrar el cumplimiento del principio de responsabilidad demostrada de que trata el artículo 2.2.2.25.6.1 del Decreto 1074 de 2015, en la medida en que limitan los riesgos de suplantación y disminuyen el tratamiento de datos personales, en particular de datos biométricos, al evitar que el titular deba someterse a un nuevo proceso de verificación ante cada sujeto obligado. Para efectos de esta instrucción, se entiende por credencial verificable la declaración electrónica de atributos de identidad de una persona, emitida como resultado de un proceso de verificación que cumpla las presentes instrucciones, que el titular conserva bajo su control y cuya autenticidad, integridad y vigencia puede comprobar quien la recibe.

Los sujetos obligados que acepten credenciales verificables deberán:

a) Comprobar la autenticidad, la integridad y la vigencia de la credencial, incluido que no haya sido revocada.
b) Comprobar, mediante un mecanismo adicional proporcional al riesgo de la operación, que quien presenta la credencial es su titular.
c) Solicitar únicamente los atributos de identidad necesarios para la operación.

Los sujetos obligados que emitan credenciales verificables deberán revocarlas cuando adviertan que el proceso de verificación que les dio origen fue fraudulento o que la credencial se encuentra comprometida. En la vinculación de un nuevo cliente, la credencial verificable y el mecanismo de que trata el literal b) se considerarán mecanismos independientes para efectos de la instrucción 6, siempre que la verificación que originó la credencial haya cumplido dicha instrucción. El uso de credenciales verificables será

facultativo para el titular y su aceptación no traslada a su emisor la responsabilidad del sujeto obligado.

10. Tratamiento de los datos personales. El tratamiento de datos personales con ocasión de la verificación de identidad deberá cumplir integralmente el régimen de protección de datos personales. En particular, los sujetos obligados deberán:

a) Obtener la autorización previa, expresa e informada del titular para el tratamiento de sus datos biométricos, informándole su carácter facultativo, en los términos del artículo 6 de la Ley 1581 de 2012 y del artículo 2.2.2.25.2.3 del Decreto 1074 de 2015.
b) Utilizar los datos recolectados exclusivamente para la verificación de la identidad y la prevención del fraude, y abstenerse de emplearlos para finalidades distintas.
c) Preferir, cuando sea técnicamente posible, el almacenamiento de plantillas biométricas cifradas sobre el almacenamiento de imágenes o videos, y conservar los datos solo durante el tiempo necesario para la finalidad y para atender los requerimientos previstos en la Ley 2573 de 2026.
d) Informar al titular, de manera clara, sobre las condiciones del tratamiento de sus datos personales, sus finalidades, los derechos que le asisten como titular y los mecanismos de consulta a su disposición.
e) Abstenerse de compartir con terceros los datos biométricos recolectados, salvo con su encargado del tratamiento debidamente autorizado o la Registraduría Nacional del Estado Civil, y de alimentar bases de datos biométricos centralizadas o integradas creadas por personas de naturaleza privada.

11. Evidencia y trazabilidad. Los sujetos obligados deberán conservar, para cada operación sujeta a verificación, un expediente de verificación que permita reconstruir los mecanismos utilizados, su resultado, la fecha y la hora, el canal, el proveedor y los demás elementos necesarios para demostrar la diligencia empleada, y ponerlo a disposición de esta Superintendencia cuando lo requiera. El expediente de verificación se conservará durante un término mínimo de tres (3) años, contados a partir de la terminación del producto o servicio por cualquier causa, incluida su cancelación. Los documentos y la información que soportaron la aprobación del producto o servicio se conservarán durante diez (10) años, contados en los términos del artículo 28 de la Ley 962 de 2005. Cuando la operación sea objeto de una reclamación por presunta suplantación de identidad, el expediente y los documentos se conservarán, en todo caso, hasta que quede en firme la decisión que ponga fin a la actuación administrativa o judicial correspondiente. Los datos biométricos se conservarán únicamente durante el tiempo necesario para cumplir las finalidades previstas en esta instrucción, de conformidad con el artículo 11 del Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015.

En cumplimiento del numeral 7 del artículo 5 de la Ley 2573 de 2026, los sujetos obligados entregarán a la persona presuntamente suplantada, cuando esta lo solicite, copia de la información y/o documentos aportados para la aprobación del producto o servicio solicitado

a su nombre. La entrega se hará dentro del término previsto en el numeral 4 del mismo artículo. La entrega comprende todo lo aportado por el solicitante, incluidas las imágenes, capturas y registros biométricos recolectados durante la operación. No comprende los elementos generados internamente por el sujeto obligado, como las plantillas biométricas o los parámetros de sus sistemas de detección de fraude. Antes de la entrega, el sujeto obligado validará la identidad del solicitante a través de un canal distinto del utilizado en la operación controvertida, conforme al numeral 5 del artículo 6 de la misma ley. Esta validación no podrá emplearse para negar, condicionar ni dilatar la entrega.

12. Proveedores de servicios de verificación. La contratación de terceros para la prestación de servicios de verificación de identidad no traslada a ellos la responsabilidad del sujeto obligado. Los sujetos obligados deberán verificar que sus proveedores cumplan las presentes instrucciones y el régimen de protección de datos personales, regular contractualmente su condición de encargados del tratamiento y exigirles evidencia del desempeño de sus mecanismos, incluidos los resultados de evaluaciones independientes.

13. Evaluación y actualización de los mecanismos. Los sujetos obligados deberán monitorear periódicamente el desempeño de sus mecanismos de verificación, incluidas las tasas de falsa aceptación y de falso rechazo, las diferencias de desempeño entre grupos de población y la incidencia de casos de suplantación, y ajustar sus mecanismos cuando los resultados lo hagan necesario.

14. Verificación intensificada ante la leyenda «Víctima de Falsedad Personal». Cuando la historia de crédito del potencial adquirente registre la leyenda «Víctima de Falsedad Personal» de que trata el numeral 7 del numeral II del artículo 16 de la Ley 1266 de 2008, los sujetos obligados deberán tratar la operación como de alto riesgo y aplicar una verificación intensificada de la identidad. Para ello deberán, como mínimo:

a) Combinar los mecanismos exigidos en la instrucción 6 con, al menos, un mecanismo adicional que compruebe un factor de una categoría distinta.
b) Cotejar los atributos de identidad del potencial adquirente contra una fuente oficial, cuando ello sea jurídica y técnicamente posible.
c) Cuando exista una relación previa con el titular, confirmar la solicitud a través de un canal de contacto cuya titularidad se haya verificado con anterioridad y que sea distinto de aquel por el que se recibió la solicitud.
d) Dejar constancia de la verificación intensificada en el expediente de verificación.

15. Verificación fallida e indisponibilidad de fuentes o proveedores. Cuando un mecanismo de verificación falle, arroje un resultado no concluyente o no esté disponible, incluida la indisponibilidad temporal de una fuente oficial o de un proveedor, los sujetos obligados no podrán sustituirlo por un mecanismo menos robusto. En esos casos deberán aplazar la operación hasta que el mecanismo esté disponible o aplicar una combinación alternativa que ofrezca un nivel de confianza equivalente y dejar constancia de ello en el expediente de verificación.

Cuando no sea posible alcanzar el nivel de confianza exigido para la operación, los sujetos obligados deberán abstenerse de originar la obligación o de realizar la operación.

16. Decisiones automatizadas y revisión humana. Cuando la verificación de identidad se apoye en sistemas automatizados y el resultado sea desfavorable, los sujetos obligados deberán informar al solicitante, de manera clara y comprensible, el resultado de la verificación, los motivos que sustentan la decisión y los medios con los que cuenta para intentarla de nuevo o solicitar una revisión. Si el resultado desfavorable impide acceder al bien o servicio ofrecido, el solicitante tendrá derecho a que una persona revise el caso o a verificar su identidad mediante un mecanismo alternativo que ofrezca un nivel de confianza equivalente.

La información suministrada al solicitante no deberá revelar detalles de los controles de seguridad que puedan facilitar su evasión.

17. Vigencia. La presente circular rige a partir de su publicación en el Diario Oficial. Las instrucciones contenidas en ella serán exigibles a partir del 1 de julio de 2027 y se aplicarán a las operaciones que se inicien desde esa fecha.

Cordialmente,

SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Elaboró: Daniel Ospina Celis
Revisó:
Aprobó: