



CAPÍTULO PRIMERO - DISPOSICIONES GENERALES

1.1 Identificación del responsable de tratamiento.

El Banco Contactor S.A., constituido y existente conforme a las leyes de la República de Colombia como establecimiento de crédito vigilado por la Superintendencia Financiera de Colombia, actúa como Responsable del Tratamiento de Datos Personales, en los términos definidos por la Ley 1581 de 2012 y normas concordantes.

Para todos los efectos relacionados con el ejercicio de los derechos de los titulares y el cumplimiento del régimen de protección de datos personales, el Banco se identifica a través de los siguientes datos de contacto:

- * Razón social: BANCO CONTACTAR S.A.
- * NIT: 901702583-3
- * Domicilio principal: Carrera 6 No. 22 – 90, Barrio El Ejido, Pasto – Nariño
- * Correo electrónico general: pqrs.banco@bancocontactar.com
- * Teléfono de contacto: 323 2540606

Así mismo, el Banco ha designado a un Oficial de Protección de Datos Personales (OPDP), quien será el responsable interno de velar por la adecuada implementación, cumplimiento, monitoreo y atención de solicitudes relacionadas con el tratamiento de datos personales, conforme a la normativa vigente.

Los datos de contacto del Oficial de Protección de Datos Personales se encuentran disponibles de forma permanente en los canales oficiales del Banco y son los siguientes:

- * Correo electrónico: datospersonales@bancocontactar.com
- * Página web: <https://www.bancocontactar.com>

Para efectos de la presente política, el Banco Contactor S.A. podrá ser denominado indistintamente como la “organización” o el “Banco Contactor”.

1.2 Definiciones.

Para la correcta interpretación y aplicación de la presente Política, se emplearán las siguientes definiciones, conforme a la Ley 1581 de 2012, el Decreto 1074 de 2015 y los lineamientos de la Superintendencia de Industria y Comercio:

- Autorización:** Consentimiento previo, expreso, informado e inequívoco otorgado por el Titular para llevar a cabo el Tratamiento de sus Datos Personales.
- Base de Datos:** Conjunto organizado de Datos Personales que sea objeto de Tratamiento, independientemente del medio en que se encuentren almacenados.





- c. **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- d. **Dato Personal Semiprivado:** Dato que no tiene naturaleza íntima, reservada ni pública, cuyo conocimiento o divulgación puede interesar tanto a su titular como a un grupo determinado de personas o a la sociedad en general.
- e. **Dato Personal Sensible:** Dato que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen origen racial o étnico, orientación política, convicciones religiosas o filosóficas, pertenencia sindical, datos de salud, vida sexual y datos biométricos.
- f. **Dato Biométrico:** Dato personal sensible obtenido a partir de un tratamiento técnico específico, relativo a características físicas, fisiológicas o conductuales de una persona natural que permiten o confirman su identificación única.
- g. **Dato Personal Privado:** Dato que por su naturaleza íntima o reservada solo interesa a su Titular y cuyo Tratamiento requiere autorización.
- h. **Dato Personal Público:** Dato calificado como tal por la Constitución o la Ley, cuyo Tratamiento no requiere autorización del Titular.
- i. **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que realice el Tratamiento de Datos Personales por cuenta del Responsable del Tratamiento.
- j. **Responsable del Tratamiento:** Persona natural o jurídica, pública o privada, que decide sobre la Base de Datos y/o el Tratamiento de los Datos Personales.
- k. **Titular:** Persona natural cuyos Datos Personales son objeto de Tratamiento.
- l. **Tratamiento:** Cualquier operación o conjunto de operaciones realizadas sobre Datos Personales, tales como la recolección, almacenamiento, uso, circulación, transferencia, transmisión o supresión.
- m. **Transferencia:** Tratamiento de Datos Personales en el cual el Responsable o Encargado ubicado en Colombia envía información a un receptor que actúa como Responsable y se encuentra dentro o fuera del país.
- n. **Transmisión:** Tratamiento de Datos Personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia, cuando dicha comunicación tiene por objeto la realización de un Tratamiento por parte de un Encargado, por cuenta del Responsable.
- o. **Incidente de Seguridad de la Información:** Evento que compromete la confidencialidad, integridad o disponibilidad de los Datos Personales y que pueda generar un riesgo para los derechos y libertades de los Titulares.

1.3 Objetivo de la política.

La presente Política de Tratamiento de Datos Personales tiene como finalidad garantizar el cumplimiento del régimen de protección de datos personales en Colombia, en especial lo dispuesto en la Ley 1581 de 2012 y sus normas reglamentarias, estableciendo los principios, lineamientos, criterios y procedimientos bajo los cuales el Banco Contactor S.A. realiza el Tratamiento de los Datos Personales contenidos en sus Bases de Datos físicas y digitales.

De manera específica, esta Política tiene como objetivos:





- * Informar a los Titulares sobre las finalidades para las cuales se recolectan, utilizan y tratan sus Datos Personales.
- * Garantizar el ejercicio efectivo de los derechos de los Titulares.
- * Definir los compromisos y responsabilidades del Banco en su calidad de Responsable y, cuando aplique, de Encargado del Tratamiento.
- * Establecer los mecanismos y procedimientos para el ejercicio de los derechos de acceso, consulta, rectificación, actualización, supresión y revocatoria de la autorización.

1.4 Marco Normativo.

El Tratamiento de los Datos Personales por parte del Banco Contactor S.A. se rige por las siguientes disposiciones legales y administrativas, así como por aquellas que las modifiquen, adicionen o sustituyan:

- * Ley Estatutaria 1581 de 2012.
- * Ley 1266 de 2008, relativa al habeas data financiero, crediticio, comercial y de servicios.
- * Decreto Único Reglamentario 1074 de 2015, Título V.
- * Circular Única de la Superintendencia de Industria y Comercio, Título V – Régimen General de Protección de Datos Personales.
- * Lineamientos, guías y conceptos emitidos por la Superintendencia de Industria y Comercio como autoridad nacional en materia de protección de datos personales.
- * Las demás normas que resulten aplicables de conformidad con la naturaleza jurídica, operativa y vigilada del Banco.

1.5 Alcance de la política.

La presente Política aplica a todo Tratamiento de Datos Personales realizado por el Banco Contactor S.A., ya sea directamente o a través de Encargados del Tratamiento, sobre información contenida en sus Bases de Datos físicas o digitales.

Esta Política es obligatoria para:

- * Todas las áreas, colaboradores, directivos y órganos de administración del Banco.
- * Proveedores y terceros que actúen como Encargados del Tratamiento.
- * Titulares de la información personal y sus representantes legales, respecto de los Datos Personales recolectados por el Banco en el desarrollo de sus actividades.

La Política cubre el Tratamiento de Datos Personales de clientes, usuarios, clientes potenciales, colaboradores, proveedores, aspirantes, visitantes y demás grupos de interés respecto de los cuales el Banco recolecte o trate información personal en el marco de sus funciones legales, contractuales y misionales.





El Banco tratará datos personales solo cuando exista una base jurídica válida, aplicando los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

- * Autorización del titular (consentimiento previo, expreso e informado), incluidos los datos sensibles con autorización explícita y diferenciada.
- * Cumplimiento de un deber legal o reglamentario (p. ej., obligaciones laborales, tributarias, contables, de seguridad social, reportes regulatorios y de supervisión).
- * Ejecución y desarrollo de una relación contractual o precontractual con el titular (p. ej., originación y administración de productos y servicios financieros; relación laboral o formativa).
- * Información pública (en los términos de ley) y datos provenientes de fuentes públicas debidamente habilitadas, tratados bajo principios de minimización y finalidad.
- * Finalidades históricas, estadísticas o científicas, siempre que se apliquen medidas técnicas y organizativas para suprimir identificadores o anonimizar cuando sea posible.
- * Protección de la vida, salud o seguridad del titular o de un tercero en situaciones de urgencia debidamente justificadas.
- * Requerimientos de autoridades competentes (judiciales o administrativas) emitidos con las formalidades legales.
- * El Banco documentará la base jurídica aplicable a cada tratamiento y evidenciará su evaluación en matrices, inventarios o registros internos.

1.6 Principios.

El Banco Contactor aplicará, de manera armónica e integral, los siguientes principios para todo Tratamiento de Datos Personales que realice directa o indirectamente (a través de Encargados), cualquiera sea el medio, canal o tecnología utilizada:

- * **Principio de legalidad:** El Tratamiento es una actividad reglada y se sujeta a la Constitución, la Ley 1581 de 2012, la Ley 1266 de 2008 (hábeas data financiero), el Decreto 1074 de 2015, la Circular Única SIC y demás normas aplicables. Ningún tratamiento se realizará por fuera de la ley.
- * **Principio de finalidad:** El Tratamiento obedecerá a finalidades determinadas, legítimas y explícitas, informadas al Titular. No se realizarán finalidades abiertas o indeterminadas, ni usos incompatibles con las finalidades informadas.
- * **Principio de libertad:** El Tratamiento solo puede ejercerse con autorización previa, expresa e informada del Titular, salvo excepciones legales. La autorización será granular para finalidades accesorias (p. ej., marketing), respetando en todo momento la posibilidad de opt-out y revocatoria sin afectar finalidades necesarias.





- * **Principio de veracidad o calidad:** La información será veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe tratar datos parciales o que induzcan a error. Banco Contactor adelantará actualizaciones cuando tenga conocimiento de cambios o cuando el Titular lo solicite legítimamente.
- * **Principio de transparencia:** Se garantizará al Titular el derecho a obtener información sobre la existencia y el uso de sus datos en cualquier momento, por canales visibles y gratuitos, conforme a los plazos y procedimientos legales (consultas y reclamos).
- * **Principio de acceso y circulación restringida:** El Tratamiento se limita por la naturaleza de los datos y por la normativa. Solo accederán personas autorizadas (o facultadas por la ley) y se mantendrán controles de acceso por roles y trazabilidad. La publicación en medios abiertos solo procederá respecto de información pública o bajo controles técnicos que aseguren acceso restringido.
- * **Principio de seguridad:** Se adoptarán medidas técnicas, organizativas y jurídicas para preservar la confidencialidad, integridad y disponibilidad de los datos, prevenir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento y gestionar incidentes con reporte oportuno a la autoridad cuando aplique.
- * **Principio de confidencialidad:** Quienes intervengan en el Tratamiento guardarán reserva incluso después de finalizada su relación con el Banco o con el encargo. La información solo se suministrará en los eventos autorizados por la ley o por el Titular.
- * **Principios de necesidad, minimización y proporcionalidad:** Se tratarán solo los datos estrictamente necesarios, adecuados y pertinentes para la finalidad. Se evitará la recolección excesiva (p. ej., no se solicitará acceso a contactos o galería del dispositivo para verificación, cobranza o marketing).
- * **Principio de temporalidad o caducidad:** Los datos se conservarán por el tiempo necesario para cumplir la finalidad y las obligaciones legales (regulatorias), y luego serán suprimidos o anonimizados conforme las reglas de retención de esta Política.
- * **Principio de interpretación integral de derechos:** Se protegerán de forma equilibrada los derechos de hábeas data, intimidad, honra, buen nombre, información, debido proceso y no discriminación, en armonía con el interés público y el marco constitucional.
- * **Privacidad desde el diseño y por defecto:** Las actividades, procesos y tecnologías incorporarán la protección de datos desde su concepción (by design) y, por defecto (by default), aplicarán la configuración más protectora para el Titular.
- * **Responsabilidad demostrada (accountability):** El Banco evidenciará el cumplimiento mediante registros, matrices, contratos, auditorías, capacitaciones, RNBD y el funcionamiento del Comité - Mesa de Protección de Datos.

1.7 Autorización para el tratamiento de datos (consentimiento).





El Banco obtendrá autorización previa, expresa e informada del titular y conservará prueba verificable de su otorgamiento por cualquier medio que permita consulta posterior (documento físico o digital, registro electrónico (de clic, audio, voz, firma electrónica u otro mecanismo idóneo). La evidencia identificará finalidades aceptadas, fecha, hora, medio e identidad del otorgante.

- * **Transparencia y granularidad.** El Banco separará las finalidades necesarias (p. ej., ejecución contractual, seguridad, cumplimiento legal) de las accesorias (p. ej., marketing, difusión externa de imagen/voz), de modo que el titular pueda elegir y revocar selectivamente sin afectar la relación principal.
- * **Autorización para datos sensibles.** Para datos sensibles (salud, biometría, imagen, voz en contextos no necesarios), el Banco recabará autorización explícita y diferenciada, informando su carácter facultativo y ofreciendo alternativas no biométricas cuando proceda. Estos datos no se usarán para marketing.
- * **Mecanismos válidos de autorización.** Formularios físicos, digitales, casillas informadas con registro, firma electrónica, grabaciones, flujos de onboarding o cualquier mecanismo que permita trazabilidad y verificabilidad.
- * **Excepciones a la autorización (uso restrictivo).** El Banco aplicará de manera restrictiva las excepciones previstas en la ley (p. ej., información pública; urgencia médica; orden de autoridad; finalidades históricas, estadísticas o científicas con medidas adecuadas; relaciones precontractuales, contractuales en lo estrictamente necesario).
- * **Revocatoria, oposición y opt-out.** El titular podrá revocar total o parcialmente su autorización y oponerse a finalidades accesorias (p. ej., marketing) en cualquier momento, sin afectar el cumplimiento de obligaciones legales ni la conservación probatoria. El Banco dispondrá de canales visibles y procedimientos ágiles para gestionar estas solicitudes.
- * **Avisos de privacidad y capas informativas.** En canales presenciales y no presenciales, el Banco empleará avisos de privacidad claros y, cuando aplique, capas informativas (resumida más ampliada) para explicar quién trata, qué trata, con qué fines, bases jurídicas, derechos, canales, transferencias transmisiones y plazos.

1.8 Tratamiento de datos de Niños, Niñas y Adolescentes (NNA).

El tratamiento de datos de NNA se realizará exclusivamente cuando responda y respete su interés superior, observando minimización, proporcionalidad, confidencialidad reforzada y acceso restringido.

- * **Autorización y participación.** Requiere autorización del representante legal; cuando sea razonable según la edad y madurez, el Banco informará al menor y procurará su participación.





- * Alcance típico en el Banco. (i) Productos de ahorro con titular menor (véase numeral específico de Cap. 2); (ii) beneficiarios de colaboradores ante seguridad social y bienestar; (iii) programas o actividades institucionales que involucren NNA. No se realizará marketing directo al menor. Toda comunicación comercial se dirigirá, en su caso, al representante legal y con consentimiento.
- * Datos sensibles de NNA. El Banco evitará recolectar datos sensibles de NNA; si excepcionalmente una norma lo exige, acotará la recolección a lo indispensable, con autorización explícita del representante, acceso ultra restringido y conservación mínima.

1.9 Participación en grupos empresariales y corresponsabilidad.

Cuando el Banco Contactor S.A. haga parte de un grupo empresarial o tenga vínculos de subordinación conforme a los artículos 260 y ss. del Código de Comercio y la Ley 222 de 1995, podrá compartir y/o integrar Bases de Datos con las sociedades matrices, subordinadas, filiales o vinculadas, exclusivamente para finalidades compatibles, necesarias y previamente informadas a los Titulares, respetando los principios de finalidad, necesidad, proporcionalidad, circulación restringida y seguridad.

Dependiendo del rol efectivo sobre la decisión del Tratamiento, las sociedades del grupo podrán actuar como:

- * Responsables independientes, cuando decidan por sí mismas sobre las Bases de Datos y las finalidades;
- * Corresponsables, cuando determinen conjuntamente finalidades y medios del Tratamiento;
- * Encargadas, cuando traten los datos por cuenta del Banco.

En los eventos de corresponsabilidad, el Banco y la(s) sociedad(es) vinculada(s) definirán y documentarán de manera clara y verificable sus respectivas obligaciones para facilitar a los Titulares el ejercicio de derechos y para gestionar incidentes de seguridad, sin perjuicio de que el Titular pueda dirigirse indistintamente a cualquiera de los corresponsables.

El intercambio intragrupo de Datos Personales, incluyendo transferencias internacionales cuando existan compañías del grupo en el exterior, se realizará bajo acuerdos de transferencia o transmisión con cláusulas de protección de datos equivalentes o superiores a las exigidas por la legislación colombiana, e incluirá las salvaguardas contractuales, técnicas y organizacionales apropiadas.

1.10 Registro Nacional de Bases de Datos (RNBD) y deber de actualización.

El Banco Contactor S.A. registrará, actualizará y reportará la información de sus Bases de Datos ante el Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio, dentro de los plazos y condiciones establecidos en la normativa vigente.

El Banco mantendrá trazabilidad de sus Bases de Datos (nombre, finalidad, tipo de datos, canal de obtención, población, medidas de seguridad, transferencias, transmisiones,





encargado(es) y políticas aplicables), y asegurará la consistencia entre lo declarado en el RNBD y lo dispuesto en la presente Política.

1.10 Gobierno de datos personales y responsabilidades internas.

Además del Oficial de Protección de Datos Personales (OPDP), el Banco contará con un modelo de gobierno que incluya:

- * Comité o mesa de Protección de Datos Personales (o instancia equivalente) para la dirección y seguimiento del programa;
- * Roles y responsabilidades por área (negocio, tecnología, riesgos, jurídico, gestión humana, comercial, cumplimiento, seguridad de la información);
- * Capacitación y concienciación periódica a colaboradores y terceros; y
- * Matriz de obligaciones normativas y de control para evidenciar responsabilidad demostrada.
- * El Banco promoverá el principio de privacidad desde el diseño y por defecto, integrando la protección de datos en los procesos, productos y tecnologías desde su concepción.

1.9 Coordinación con autoridades de vigilancia.

El Banco Contactor S.A., en su calidad de entidad del sector financiero vigilada por la Superintendencia Financiera de Colombia (SFC) y sujeto a la supervisión de la Superintendencia de Industria y Comercio (SIC) como autoridad nacional de protección de datos, cooperará con ambas autoridades y atenderá sus requerimientos en el ámbito de sus competencias, sin perjuicio de los deberes derivados de la Ley 1266 de 2008 respecto del habeas data financiero.

1.10 Ámbito material y territorial del tratamiento.

La presente Política aplica al Tratamiento de Datos Personales que el Banco realiza dentro y fuera del territorio colombiano, cuando: (i) el Tratamiento sea ejecutado por el Banco, sus Encargados o corresponsables; (ii) los medios de Tratamiento se encuentren en Colombia; o (iii) los datos sean tratados en virtud de transmisiones o transferencias internacionales realizadas por el Banco.

Esta Política también aplica a los encargados y proveedores que traten Datos Personales por cuenta del Banco, quienes deberán cumplir los estándares contractuales y medidas de seguridad definidas.

1.11 Incidentes de seguridad de datos personales.

Se entiende por incidente de seguridad cualquier evento que comprometa la confidencialidad, integridad o disponibilidad de datos personales (p. ej., acceso no autorizado, pérdida, divulgación indebida, cifrado malicioso, destrucción, alteración u otros).





El Banco aplicará su procedimiento interno de respuesta (detección, contención, análisis de impacto, remediación y lecciones aprendidas) y reportará a la autoridad de protección de datos dentro de los quince (15) días hábiles siguientes a su detección, a través del canal que la autoridad disponga.

Contenido mínimo del reporte. Descripción del incidente, tipología de datos comprometidos, número aproximado de titulares, fecha(s), medidas adoptadas, evaluación preliminar de riesgos, estado y acciones de mitigación.

Comunicación a titulares. Cuando del incidente pueda derivarse un riesgo material para los titulares, el Banco comunicará oportunamente el hecho, las medidas adoptadas y las recomendaciones de protección, por canales idóneos.

Registro y evidencias. El Banco conservará registro de incidentes, evidencias técnicas y decisiones adoptadas, y actualizará cuando aplique la información correspondiente en el RNBD.

CAPÍTULO SEGUNDO - TRATAMIENTO DE DATOS

2.1 Tipos de datos personales tratados.

El BANCO CONTACTAR en el desarrollo de sus actividades misionales y comerciales como entidad vigilada por la Superintendencia Financiera de Colombia (SFC), requiere recolectar y realizar el Tratamiento de diversas categorías de Datos Personales, siempre bajo los principios de finalidad, necesidad y minimización, y exclusivamente para las finalidades informadas y autorizadas.

Las categorías de datos sujetas a Tratamiento incluyen, sin limitarse a:

- * **Datos de Identificación:** Nombre completo, tipo y número de documento de identidad (Cédula de Ciudadanía, Cédula de Extranjería, Pasaporte), nacionalidad, estado civil, firma, fecha y lugar de nacimiento, fecha y lugar de expedición.
- * **Datos de Ubicación y Contacto:** Dirección de residencia o domicilio, dirección de correspondencia, teléfonos fijos, teléfonos móviles y correo electrónico.
- * **Datos Académico - Laborales:** Nivel de escolaridad, títulos obtenidos, experiencia laboral, cargo actual; cuando aplique para procesos de selección o gestión de la relación laboral o contractual.
- * **Datos Socioeconómicos y Financieros:** Ingresos, egresos, patrimonio, información tributaria, historial y comportamiento crediticio, datos relativos a productos y servicios financieros (cuentas, depósitos, créditos, inversiones, medios de pago, etc.) y referencias personales o comerciales, con observancia de la Ley 1266 de 2008.
- * **Datos Biométricos (Sensibles):** Huella, reconocimiento facial, voz, patrones de firma u otros equivalentes exclusivamente para autenticación robusta, seguridad física y lógica, control de acceso y prevención de fraude, con autorización explícita y diferenciada, carácter facultativo y mecanismos alternativos no biométricos. No se condicionará el acceso a productos o servicios al suministro de datos sensibles, salvo





en aquellos casos como canales digitales en el que se constituyen como necesarios para la vinculación. En canales no presenciales de alto riesgo, se podrán requerir mecanismos de autenticación reforzada; cuando el titular opte por no utilizar biometría, se habilitará un flujo alternativo equivalente en seguridad (p. ej., OTP/2FA, video identificación), sin menoscabo del derecho, siempre que el Banco cuente con estos mecanismos.

- * **Otros Datos Sensibles (p. ej., salud):** Tratados excepcionalmente y con medidas reforzadas, principalmente para SG-SST y cumplimiento de requerimientos de EPS, ARL, IPS o autoridades.
- * **Datos Técnicos y de Canal Digital:** Identificadores en línea (cookies/ID), registros transaccionales, telemetría, geolocalización estrictamente necesaria para seguridad y autenticación; sin acceso a contactos o galerías del dispositivo del titular.
- * **Datos de Niños, Niñas y Adolescentes (NNA):** Bajo el interés superior del menor, minimización y autorización reforzada del representante legal y, cuando corresponda, del propio menor.

2.2 Tratamiento al cual se someten los datos personales.

Los datos personales objeto de tratamiento por parte del BANCO CONTACTAR están sometidos a las siguientes operaciones, de manera física o digital, manual o automatizada, a lo largo del ciclo de vida del dato:

- * **Recolección:** El Banco recolecta información personal a través de diversos medios en el desarrollo de las actividades relacionadas con su objeto social y sus obligaciones como empleador y/o en el ejercicio de la negociación con proveedores y/o aliados. La información será obtenida: (a) directamente del titular; (b) de un tercero legítimamente autorizado; y (c) de fuentes públicas de información.

La recolección podrá llevarse a cabo a través de medios físicos, digitales o electrónicos y, en cada uno de ellos, se incorporará aviso de privacidad y autorización cuando aplique, cumpliendo los requisitos regulatorios y los principios de libertad y finalidad de la Ley 1581. En canales digitales, el Banco utilizará textos informativos claros, conservará prueba verificable de las autorizaciones, y aplicará controles de suplantación (p. ej., segundo factor, video identificación), evitando la recolección excesiva (no solicitará acceso a contactos o galerías para fines de cobranza, marketing).

- * **Almacenamiento:** El almacenamiento de la información personal contenida en las bases de datos o sistemas del Banco se realiza en servidores propios en Colombia, en servidores de terceros (encargados) en otros países, con medidas de seguridad físicas, técnicas y administrativas, y controles de acceso por roles, garantizando el principio de acceso y circulación restringida.

Cuando se utilicen encargados (p. ej., nube/BPO), se incluirán en los contratos acuerdos para la transmisión con cláusulas de seguridad, confidencialidad, subencargo, retorno, supresión y gestión de incidentes, equivalentes o superiores a la normativa colombiana.





La información personal sujeta a requerimientos de ley permanecerá almacenada por los términos legales aplicables y, en los demás casos, mientras la finalidad se mantenga vigente. Vencidos dichos términos, el Banco aplicará supresión o anonimización irreversible.

- * **Circulación:** Por regla general, el Banco no comparte datos personales con terceros; sin embargo, para el cumplimiento efectivo de sus obligaciones puede entregarlos a otras entidades, con fundamento en la regulación (transmisiones por encargo, medidas precontractuales, contractuales con autorización o acuerdo de transmisión). En el ecosistema financiero, el Banco podrá comunicar información a operadores, fuentes y usuarios (p. ej., burós de crédito) conforme a la Ley 1266-2008; y a cámaras de compensación, ACH, redes de pago, corresponsales bancarios, aseguradoras (bancaseguros vinculados), proveedores tecnológicos y aliados estrictamente necesarios para la prestación del servicio, bajo contratos y salvaguardas de la regulación.
- * **Supresión:** La supresión se realizará cuando: (i) no sea necesaria para el cumplimiento de obligaciones legales, contractuales, tributarias, financieras, de auditoría o requerimientos de ley; (ii) afecte la integridad, trazabilidad de las bases o sistemas; (iii) se haya agotado la finalidad; o (iv) sea solicitada por el titular y no contraría las hipótesis anteriores. El Banco podrá anonimizar datos para fines estadísticos o de auditoría.
- * **Transferencias y transmisiones internacionales:** Las transferencias internacionales se realizarán solo a países con nivel adecuado o bajo las excepciones del art. 26 de la Ley 1581, o mediante declaración de conformidad y/o cláusulas contractuales modelo de la SIC (cuando aplique). Las transmisiones a encargados en el exterior se registrarán por contratos de transmisión con exigencias equivalentes. Toda operación será registrada en el RNBD.
- * **Incidentes de seguridad:** Todo incidente que comprometa la confidencialidad, integridad o disponibilidad de datos personales será gestionado y reportado a la SIC dentro de los quince (15) días hábiles siguientes a su detección, a través del RNBD o módulo dispuesto por la autoridad.

2.3 Finalidades del tratamiento de información personal.

El uso o finalidad que se da a la información personal recolectada se describe por categorías de titulares. El marketing es accesorio y requiere consentimiento granular (el titular puede optar por no recibir comunicaciones en cualquier momento).

2.3.1. Clientes Potenciales.

Los datos de los prospectos y/o clientes potenciales que podrán ser tratados corresponden a:





- * Identificación y contacto: nombre, tipo y número de documento, profesión u ocupación (cuando sea pertinente), teléfono(s), correo electrónico, dirección y ciudad.
- * Información socioeconómica: ingresos, egresos, patrimonio, actividad económica (en la medida estrictamente necesaria para la preevaluación del producto de interés).
- * Datos técnicos del canal: trazas mínimas para seguridad/autenticación y funcionamiento de formularios (p. ej., IP/fecha/horario).
- * Datos sensibles (solo si son indispensables): biométricos (p. ej., huella, rasgos faciales) exclusivamente para autenticación reforzada no presencial, con alternativa no biométrica. El Banco no solicitará permisos intrusivos en el dispositivo del prospecto (p. ej., lista de contactos o galería) para fines de verificación, cobranza o marketing.

Finalidades del tratamiento:

Los datos personales del titular serán tratados para las siguientes Finalidades:

- * Recibir, registrar y gestionar solicitudes de información, cotizaciones y simulaciones.
- * Realizar pre-evaluaciones y medidas precontractuales para productos del activo (microcrédito y cualquier modalidad de crédito) y del pasivo (cuentas, depósitos, CDT), medios de pago y servicios conexos.
- * Efectuar verificación y validación de identidad, autenticación reforzada (incluida biometría si se ofrece, con alternativa no biométrica), control de suplantación y prevención de fraude.
- * Desarrollar análisis estrictamente necesarios para segmentación precontractual y gestión del riesgo (crédito, operativo y fraude) vinculada al producto solicitado.
- * Establecer y mantener canales de contacto (correo, SMS, llamadas, mensajería) sobre el estado de la solicitud.
- * Marketing del Banco (promociones, educación financiera), y de aliados solo con autorización; opt-out disponible en todo momento.
- * Cumplir obligaciones legales (p. ej., consultas de listas restrictivas y LA/FT cuando aplique en fase precontractual).
- * Soportar y auditar la trazabilidad de la interacción; atender requerimientos de autoridades administrativas o judiciales y de supervisión.
- * Biometría (si aplica): únicamente para autenticación o constancia de consentimiento; no se usará para marketing; conservación mínima

Terceros necesarios y encargados:

- * Plataformas, formularios, CRM, mensajería (email, SMS) y nube que operen por cuenta del Banco mediante contratos de transmisión con obligaciones de seguridad, confidencialidad, devolución y supresión.
- * Aliados únicamente cuando el prospecto autorice recibir comunicaciones.
- * Autoridades competentes cuando exista requerimiento formal y procedente.
- * Si alguna plataforma se aloja en el exterior, se aplicarán las reglas de transferencias, transmisiones internacionales y, cuando corresponda, el registro en el RNBD.

Tratamiento de datos sensibles:





- * Biométricos: facultativos, con alternativa no biométrica; finalidad exclusiva de autenticación; plazo de conservación mínimo.

Conservación y uso post-interés:

Hasta por un (1) año desde la última manifestación de interés o interacción, o antes si el titular solicita supresión o revoca consentimientos; Podrá conservarse por un término superior solo por obligación legal o proceso en curso; Durante la conservación residual, los datos no se usarán para fines distintos a los aquí descritos (no marketing).

2.3.1. Clientes.

La información de los clientes objeto de tratamiento por parte Banco Contactor corresponde a datos requeridos para la vinculación y administración de los productos, servicios y canales del Banco, entre estos las siguientes Categorías de datos tratados (mínimas y necesarias).

- * Identificación y contacto del cliente y, cuando aplique, de representantes y autorizados.
- * Información contractual y transaccional: productos y servicios contratados, reglas operativas, trazabilidad de transacciones y canales.
- * Información socioeconómica y financiera: ingresos, egresos, patrimonio, actividad económica, referencias, información tributaria, contable proporcional a la finalidad.
- * Riesgo y seguridad: variables necesarias para originación, administración y monitoreo del producto/servicio; eventos SOC y registros de acceso (logs).
- * Datos sensibles (solo si son indispensables): biométricos (autenticación) y salud (en coberturas, seguros vinculados cuando aplique), imagen, voz.(CCTV, llamadas, reuniones por razones de calidad, seguridad y evidencia). El Banco no solicitará permisos intrusivos (p. ej., contactos, galería) para verificación, cobranza o marketing.

Finalidades del tratamiento:

a) Vinculación, operación y seguridad.

- * Vinculación y administración de productos, servicios (apertura, originación, desembolso, constitución, modificaciones, renovaciones, cancelación).
- * Identificación, verificación y autenticación (incluida biometría con alternativas y MFA), controles anti-suplantación y prevención de fraude.
- * Operación de productos del activo (crédito en cualquiera de sus modalidades, microcrédito, refinanciaciones) y del pasivo (cuentas, depósitos, CDT), medios de pago, oficinas, corresponsales y canales electrónicos.
- * Autorización, validación de transacciones, monitoreo de operaciones inusuales y gestión de ciberseguridad (registros de acceso y eventos SOC).

b) Riesgo, cumplimiento y supervisión.

- * Gestión de riesgos (crédito, mercado, liquidez, operativo y fraude): construcción y recalibración de modelos, perfilamiento y scoring; pruebas de eficacia y validación de modelos.





- * Cumplimiento regulatorio: obligaciones contables, tributarias; reportes a SFC, UIAF y demás autoridades; SARLAFT; revisoría fiscal y auditorías internas, externas.
- * Hábeas data financiero: circulación y reporte a operadores, fuentes y usuarios (p. ej., burós de crédito) sobre comportamiento y cumplimiento, conforme a la normativa especial.

c) Servicio, cobranza y gobierno del dato.

- * Cobranza y recuperación de cartera (interna, terceros) con prácticas no intrusivas (sin acceso a contactos, galería, ni contacto a referencias para cobranza). El Banco observará buenas prácticas de cobranza responsable y no empleará mecanismos intrusivos ni agresivos, en especial el acceso a contactos, galería del dispositivo o la contactabilidad de referencias personales con fines de cobro
- * Servicio al cliente y PQRS, encuestas de satisfacción, educación financiera; notificaciones sobre cambios contractuales y de tratamiento.
- * Gestión de alianzas necesarias (ACH, cámaras, redes de pago, corresponsales, aseguradoras en bancaseguros vinculados, BPO, nube) bajo contratos de transmisión y salvaguardas aplicables (incluida internacionalización cuando proceda).
- * Actualización, normalización y depuración de datos; notificaciones sobre cambios en condiciones o tratamiento.
- * Defensa judicial, administrativa y atención a inspecciones, requerimientos de SFC y SIC.
- * Grabación de llamadas (call center, líneas de atención, mensajería instantánea corporativa) y sesiones virtuales para trazabilidad, calidad y evidencia.

Terceros necesarios y encargados:

- * Burós de crédito, operadores, fuentes, usuarios (hábeas data financiero); SFC, UIAF, autoridades (reportes); revisoría fiscal y auditores.
- * Proveedores encargados: ACH/cámaras, redes de pago, corresponsales, aseguradoras (bancaseguros), BPO, nube, plataformas de onboarding y prevención de fraude, que actúan por cuenta del Banco con contratos que incluyen acuerdos de transmisión y medidas equivalentes o superiores.
- * Para plataformas o almacenamiento en el exterior, se aplicarán reglas de transferencias/transmisiones internacionales y, cuando corresponda, el registro en el RNBD.

Tratamiento de datos sensibles:

- * Biometría: autenticación, prevención de fraude.
- * Salud: únicamente en el marco de seguros vinculados o por requerimiento de autoridad y/o aseguradoras autorizadas.
- * Imagen, voz: CCTV, llamadas, reuniones solo para seguridad, calidad, constancia y evidencia.

Geolocalización y notificaciones (opt-in): cuando el titular active la geolocalización en los canales digitales del Banco, se usará para: (i) indicarle puntos de atención cercanos, (ii)





enviar notificaciones push informativas y comerciales con consentimiento y opt-out disponible, (iii) fortalecer prevención de fraude y seguridad del canal, y (iv) analítica para mejorar experiencia y ubicación de servicios, aplicando minimización y sin compartir ubicación con terceros salvo cuando sea necesario para la operación o exista consentimiento para fines comerciales.

Conservación y uso post-relación:

- * Vigencia de la relación más 10 (diez) años, exclusivamente para cumplimiento legal/regulatorio, defensa judicial, archivo histórico y auditoría (no marketing), o por el término superior que establezca una norma especial o un proceso en curso;
- * Vencidos los plazos, se procederá a la supresión o anonimización; durante la conservación residual los datos no se usarán para fines distintos a los aquí descritos.

2.3.2. Usuarios (no clientes).

El Banco trata la información estrictamente necesaria de los usuarios no clientes (personas que interactúan con el Banco sin haber formalizado aún una relación contractual), que incluye:

- * Identificación y contacto: nombre, tipo y número de documento, firma (cuando aplique), dirección, teléfono(s) y correo electrónico.
- * Datos de la solicitud o trámite: asunto, descripción y documentos que el propio usuario aporte.
- * Datos técnicos del canal: registros mínimos para seguridad, autenticación y funcionamiento de los sistemas (p. ej., fecha/horario de interacción y datos técnicos necesarios).
- * Datos sensibles (solo si son indispensables): voz e imagen en grabaciones de llamadas o reuniones virtuales, cuando se utilicen dichos canales, exclusivamente para fines de trazabilidad, calidad y evidencia.
- * El Banco no solicitará permisos intrusivos en dispositivos del usuario (como lista de contactos o galería) para atender solicitudes, realizar verificación o desarrollar comunicaciones comerciales.

Finalidades del tratamiento:

- * Identificación y verificación de identidad, y prevención de suplantación, en la atención de la solicitud o trámite presentado.
- * Registro en los sistemas del Banco y atención integral de solicitudes, aclaraciones, quejas o reclamos, incluyendo su seguimiento y cierre.
- * Análisis estadístico y de calidad del canal, de manera proporcional, para mejorar la atención y eficiencia operativa, sin perfilamiento comercial.
- * Encuestas de satisfacción y calidad del servicio (participación voluntaria).
- * Comunicaciones comerciales del Banco orientadas a promover la consolidación de una relación comercial, opcional y con mecanismos de opt-out disponibles en todo momento; no se emplearán permisos intrusivos del dispositivo.





- * Grabación y conservación de llamadas y reuniones virtuales, cuando se utilicen dichos canales, únicamente para trazabilidad, control de calidad, constancia y soporte probatorio frente a autoridades.
- * Cumplimiento de obligaciones legales y regulatorias, y atención de requerimientos de autoridades; defensa judicial y administrativa y soporte de auditoría.

Terceros necesarios y encargados:

Para cumplir las finalidades anteriores, el Banco podrá transmitir datos solo en lo indispensable a:

- * Proveedores encargados de plataformas de atención al usuario, CRM, mesas de servicio, mensajería (correo/SMS) y servicios en la nube, que actúan por cuenta del Banco mediante contratos de transmisión con obligaciones de seguridad, confidencialidad, subencargo autorizado, devolución y supresión al cierre.
- * Autoridades competentes, cuando exista requerimiento formal y procedente.
- * Cuando alguna de estas plataformas esté ubicada fuera de Colombia, el Banco aplicará las garantías previstas para transferencias o transmisiones internacionales y, cuando corresponda, realizará los registros ante el RNBD.

Tratamiento de datos sensibles:

- * Voz e imagen en grabaciones de llamadas o reuniones virtuales: uso limitado a trazabilidad, calidad y evidencia; acceso restringido a personal autorizado; conservación por el plazo estrictamente necesario para cumplir dichas finalidades y los términos legales aplicables.

Conservación y uso post-trámite:

- * La información de usuarios no clientes se conservará hasta por diez (10) años solo cuando sea necesaria para trazabilidad, cumplimiento legal, defensa judicial o administrativa y auditoría.
- * En los demás casos, los datos serán suprimidos una vez se cumpla la finalidad que dio origen al tratamiento.
- * Durante cualquier término de conservación residual, la información no se utilizará para marketing ni para finalidades distintas a las aquí descritas.

2.3.3. Aspirantes o Participantes en procesos de selección.

La información de los candidatos objeto de tratamiento por parte del Banco corresponde a datos entregados por el titular para este proceso. La información de los candidatos es tratada manual y automáticamente con la finalidad de:

- * Gestión integral del proceso de selección (convocatorias, entrevistas, pruebas).
- * Verificación de referencias y estudios de seguridad proporcionados y autorizados, proporcionales al cargo.
- * Pruebas psicotécnicas y psicofísicas estrictamente necesarias.





- * Exámenes médicos de ingreso (dato de salud exclusivo para aptitud ocupacional) y SG-SST.
- * Comunicaciones sobre el proceso; registro y trazabilidad.
- * Cumplimiento de obligaciones legales y atención de autoridades; defensa y auditoría.
- * Biometría (si aplica): solo para autenticación y firma, con alternativas y conservación mínima.

La información recolectada de aspirantes será conservada por el término que dure el respectivo proceso de selección al cual el candidato aplico, y un (1) año adicional para fines históricos y de mejora del proceso, salvo requerimiento legal superior o supresión a solicitud del titular.

2.3.4. Colaboradores (activos), beneficiarios, aprendices, pasantes y exempleados.

Para efectos de esta Política, la expresión “colaboradores” comprende a las personas vinculadas al Banco mediante contrato de trabajo (empleados activos), a aprendices y pasantes vinculados por contrato de aprendizaje o convenios formativos y a los exempleados una vez finaliza su vínculo. Cuando se mencionan beneficiarios, se refiere a familiares o personas acreditadas como tales ante el Sistema de Seguridad Social o programas de bienestar del Banco, contacto. De acuerdo con las siguientes categorías:

- * Identificación y contacto: nombre, tipo y número de documento, nacionalidad, estado civil, firma, fecha y lugar de nacimiento; dirección, teléfonos, correo electrónico.
- * Laborales, compensación y socioeconómicos: cargo, área, fechas de vinculación, terminación, tipo de contrato o convenio, novedades, nómina y prestaciones, auxilios, beneficios, información de seguridad social y parafiscales (afiliaciones, aportes, novedades), certificaciones de ingresos y retenciones y demás soportes exigidos por la normativa aplicable.
- * Beneficiarios: identificación, parentesco, fecha de nacimiento y datos estrictamente requeridos por EPS, ARL, AFP, Cajas de Compensación u otros administradores de beneficios (p. ej., escolaridad para cuotas monetarias), limitados a lo indispensable.
- * TI y seguridad de la información: usuarios, perfiles y credenciales; registros de acceso (logs), trazabilidad técnica mínima para ciberseguridad y continuidad.
- * Datos sensibles (solo cuando sean indispensables y con autorización explícita cuando proceda):
- * Salud: exclusivo para SG-SST y aptitud ocupacional o cuando lo exija autoridad/EPS/ARL/IPS.
- * Biométricos (huella, rasgos equivalentes): solo para autenticación, control de acceso y acreditación de consentimiento.
- * Imagen, voz: CCTV (seguridad), fotografías (carné y documentación interna), grabación de llamadas, reuniones virtuales (calidad y evidencia) y registro de eventos.
- * NNA (beneficiarios): tratamiento bajo el interés superior del menor, minimización y autorización del representante legal (y del propio menor cuando corresponda).

El Banco no solicitará permisos intrusivos en dispositivos personales (p. ej., lista de contactos o galería) para fines laborales, disciplinarios o comerciales.





Finalidades del tratamiento:

a) Gestión integral del vínculo laboral y cumplimiento normativo.

- * Vinculación, administración y terminación de la relación laboral: afiliaciones, novedades, creación y actualización del expediente, formalización y archivo de documentos, certificaciones y constancias.
- * Nómina y compensación: cálculo y pago de nómina, prestaciones y beneficios, anticipos y reembolsos; registros contables y obligaciones tributarias.
- * Seguridad social y beneficios: trámites ante EPS, ARL, AFP, Cajas de Compensación y aseguradoras (afiliaciones, novedades, incapacidades, licencias, reclamaciones).
- * Sistema de Gestión de Seguridad y Salud en el Trabajo (SG-SST): exámenes de ingreso, periódicos y de retiro; vigilancia de la salud; seguimiento de indicadores y síntomas de salud cuando sea requerido por norma; gestión e investigación de incidentes, accidentes de trabajo; determinación de origen y pérdida de capacidad laboral (PCL); atención de requerimientos de EPS/ARL/IPS y autoridades; planificación y registro de acciones correctivas y preventivas.
- * Cumplimiento de la normatividad vigente y atención de requerimientos judiciales o administrativos; revisoría fiscal y auditorías internas, externas; conservación de evidencias.
- * Prevención del lavado de activos y financiación del terrorismo (cuando aplique): debida diligencia proporcional al cargo (p. ej., posiciones de confianza o manejo de recursos), consultas a listas restrictivas y demás verificaciones necesarias.
- * Trámites pensionales y ante entidades de previsión social a nombre del trabajador, cuando aplique.

b) Desarrollo, desempeño, comunicaciones y bienestar.

- * Evaluación del desempeño, habilidades y competencias, planes de mejora y/o procesos disciplinarios con debido proceso.
- * Formación y desarrollo: registro y seguimiento de entrenamientos, talleres y capacitaciones; ejecución del plan de formación; promoción interna y campañas de promoción laboral.
- * Bienestar y clima organizacional: planificación y ejecución de actividades recreativas o culturales; entrega de dotación; programas de apoyo y calidad de vida.
- * Comunicaciones y notificaciones relacionadas con la relación laboral por los medios autorizados (correo, teléfono, SMS/MMS, mensajería instantánea o físico).
- * Actualización de datos e información sobre cambios en el tratamiento de datos personales.
- * Contacto a familiares en caso de emergencia.

c) Seguridad física, lógica, continuidad y evidencias

- * Creación y administración de usuarios, perfiles y contraseñas; gestión de privilegios para acceso a plataformas y correo; control de cambios y trazabilidad técnica.





- * Control de acceso e identidad: ingreso a instalaciones y control horario mediante mecanismos de autenticación (incluida biometría con autorización explícita y alternativa no biométrica disponible).
- * Videovigilancia (CCTV): seguridad de personas, bienes e instalaciones; verificación de cumplimiento de políticas internas; entrega a autoridades cuando proceda; señalización visible y conservación limitada.
- * Grabación de llamadas (p. ej., en call center): mejora de la calidad del servicio, constancia y/o atención de autoridades de vigilancia y control.
- * Teleconferencias y reuniones virtuales: registro de la realización de los encuentros y consulta interna posterior. Eventos internos o institucionales: registro y, con autorización, difusión interna o externa (incluidos medios de comunicación).

d) Imagen, publicaciones y autorizaciones diferenciadas.

- * Identificación y carnetización: uso de fotografía para carné y formularios internos.
- * Publicación de imagen y/o voz en canales internos o externos del Banco (sitio web, redes sociales, intranet y piezas gráficas o audiovisuales).

e) Estudios de seguridad e integridad.

- * Estudios de seguridad proporcionales al cargo (pudiendo incluir visitas domiciliarias y, en cargos de alta confianza, pruebas de integridad como polígrafo, cuando sean legalmente procedentes y con consentimiento explícito), con acceso estrictamente restringido y finalidad exclusiva de idoneidad

f) Beneficiarios (familiares o autorizados por el colaborador).

- * Afiliaciones, novedades a seguridad social y beneficios; acceso y administración de programas (subsidios, cuotas monetarias, recreación y apoyo), limitando los datos a lo que exija cada trámite.
- * Comunicaciones de bienestar y soporte histórico de la condición de beneficiario.
- * NNA: aplicación del estándar reforzado (autorización del representante; minimización).

g) Exempleados (fase post-relación).

- * Cumplimiento legal y atención de autoridades: respuesta a requerimientos judiciales o administrativos (inspección de trabajo, UGPP, DIAN, judicatura, entre otros).
- * Soporte histórico del vínculo: conservación de la evidencia mínima para acreditar la relación, sus condiciones y la correcta terminación.
- * Certificaciones y constancias (tiempo, cargo, ingresos, retenciones) a pedido del titular o por exigencia legal.
- * Referencias laborales a terceros solo con autorización del excolaborador o en hipótesis legales permitidas.
- * Auditoría y defensa: soporte de auditorías internas, externas y revisoría fiscal; prevención, atención de controversias y defensa judicial o administrativa.





Exclusiones: no se efectuarán perfilamientos comerciales ni se usarán datos de colaboradores, beneficiarios, aprendices, exempleados para marketing.

Terceros necesarios y encargados (transmisiones, transferencias):

Para cumplir las finalidades anteriores, el Banco podrá transmitir (encargar) o transferir datos en lo estrictamente necesario a:

- * EPS, ARL, AFP, Cajas de Compensación y demás entidades del Sistema de Seguridad Social;
- * Aseguradoras, intermediarios (si existieren pólizas asociadas al vínculo o a beneficios);
- * Revisoría fiscal y auditores internos, externos; autoridades competentes;
- * Proveedores encargados que soportan nómina, RR. HH., plataformas de talento/capacitación, servicios en la nube/BPO, medicina laboral, ocupacional, mensajería y archivo/digitalización, quienes actúan por cuenta del Banco mediante contratos de transmisión con obligaciones de confidencialidad, seguridad, subencargo autorizado, devolución y supresión al cierre;
- * Filiales, subsidiarias, fondos de empleados o proveedores, inversionistas, fondeadores cuando la relación contractual, operativa lo exija y exclusivamente para los fines autorizados.
- * Cuando exista tratamiento internacional (p. ej., plataformas de RR. HH. archivo en el exterior), se aplicarán las garantías para transferencias o transmisiones internacionales y, cuando corresponda, se realizarán los registros en el RNBD.

Tratamiento de datos sensibles (régimen reforzado):

- * Salud (SG-SST): exclusivo para finalidades de SST, aptitud ocupacional o por requerimiento de EPS/ARL/IPS/autoridad; acceso restringido a personal autorizado; conservación mínima.
- * Biometría: solo para autenticación, control de acceso, horario o acreditación de consentimiento; uso facultativo y alternativas no biométricas disponibles; no se usa para fines comerciales.
- * Imagen, voz: CCTV y grabaciones solo para seguridad, calidad, constancia y evidencia; acceso restringido y plazos limitados (ver conservación).

Conservación y uso post-relación:

- * SG-SST: 20 (veinte) años desde la terminación del vínculo (soportes exigidos por normativa de SST).
- * Historia laboral, seguridad social y aportes: hasta 80 (ochenta) años desde la terminación (prueba de aportes, novedades).
- * Resto del expediente y evidencias de seguridad: vigencia del vínculo + 10 (diez) años, exclusivamente para cumplimiento legal, auditoría, archivo y defensa (no marketing).
- * CCTV: conservación limitada (usualmente ≤ 6 meses), salvo requerimiento de autoridad o investigación que exija un término superior.





- * Beneficiarios: conservación mientras subsista la condición y por el tiempo necesario para trazabilidad y cumplimiento (si los soportes integran el expediente, aplican los plazos del colaborador).
- * Vencidos los plazos, el Banco procederá a la supresión o anonimización irreversible; durante la conservación residual, los datos no se usarán para fines distintos a los descritos.

2.3.6. Proveedores y demás terceros con los que se celebren acuerdos.

Este numeral aplica a personas naturales y a personas jurídicas (por medio de sus representantes, personal asignado o contacto operativo) con quienes el Banco celebre acuerdos para la provisión de bienes y servicios, la operación de procesos, servicios compartidos, encargos de tratamiento, acuerdos de corresponsabilidad y demás relaciones contractuales o precontractuales necesarias. De acuerdo con las siguientes categorías de datos tratados:

- * Identificación y contacto: nombre y apellidos, tipo y número de documento, nacionalidad, firma, cargo, área, teléfono(s), correo(s), dirección(es); razón social y NIT cuando aplique.
- * Profesional, negocio: experiencia, certificaciones, habilitaciones, personal asignado, matriz de funciones, perfiles técnicos, información bancaria estrictamente necesaria para pagos.
- * Económico-tributaria: RUT y otra información tributaria/contable proporcional a los requisitos legales y del proceso (p. ej., certificaciones para facturación, autorretención).
- * Datos sensibles (solo si son indispensables): imagen (carné/CCTV), voz (grabación necesaria de reuniones, llamadas para constancia, calidad) y biometría (p. ej., huella) exclusivamente para validación de identidad y control de accesos. El suministro de datos sensibles es facultativo y contará con alternativas no biométricas razonables.
- * El Banco no solicitará permisos intrusivos en dispositivos del tercero (como lista de contactos o galería) para verificación, cobranza o fines comerciales.

Finalidades del tratamiento:

a) Vinculación, evaluación y formalización

- * Registro y homologación del proveedor (tercero); verificación de existencia, representación, habilitaciones (licencias), experiencia y continuidad.
- * Debida diligencia proporcional al riesgo del bien, servicio, acuerdo: verificación en fuentes legítimas (comerciales, disciplinarias y, cuando aplique, listas restrictivas) necesaria para decidir la contratación.
- * Formalización contractual: emisión, firma de contratos, órdenes, convenios, NDA, ANS/SLA, acuerdos de seguridad de la información y acuerdos de encargo o corresponsabilidad en protección de datos.

b) Administración del acuerdo y cumplimiento





- * Gestión operativa: planificación, comunicaciones, seguimiento de entregables, control de calidad, tratamiento de incidencias, cambios, documentación de hitos y evidencias de cumplimiento.
- * Cumplimiento legal-regulatorio: atención de requerimientos de autoridades, revisoría fiscal y auditorías internas - externas; soporte de reportes contables, tributarios.
- * Seguridad física y lógica: emisión de carnés; control de accesos a instalaciones (con biometría facultativa y alternativas); CCTV para seguridad con señalización y conservación limitada; asignación de usuarios, perfiles y registros de acceso (logs) a plataformas del Banco cuando proceda.
- * Reuniones virtuales (teleconferencias): registro o grabación cuando sea necesario para acta, constancia, calidad del servicio y seguimiento.
- * Actualización de datos e información sobre cambios en el tratamiento.
- * Facturación, pagos y gestiones económicas: recepción y validación de facturas/soportes; pagos por canales y portales dispuestos; cruces contables y obligaciones tributarias.
- * Gestión de incumplimientos: aplicación de medidas contractuales y procedimientos de reclamación (prejurídica, jurídica).
- * Cuando aplique por el tipo de tercero, servicio, el Banco realizará verificaciones para prevención de LA/FT en el marco de sus sistemas internos (en alcance y profundidad proporcionales al riesgo del acuerdo).

Terceros necesarios y encargados (transmisiones, transferencias)

Para las finalidades anteriores, el Banco podrá transmitir (encargar) o transferir datos solo en lo indispensable a:

- * Autoridades competentes, revisoría fiscal y auditores internos/externos (evidencias de contratación, ejecución).
- * Entidades financieras y operadores de pago (procesamiento de facturas y pagos).
- * Proveedores encargados que soportan procesos del Banco (BPO, nube, plataformas de compras, contratación, gestión documental, mensajería, service desk), quienes actúan por cuenta del Banco mediante contratos de transmisión con obligaciones de confidencialidad, seguridad, subencargo autorizado y retorno/supresión al cierre.
- * Filiales, subsidiarias, aliados cuando el acuerdo lo exija (p. ej., servicios compartidos), en calidad de encargados o corresponsables según la operación.
- * Si se usa infraestructura o plataformas ubicadas en el exterior (p. ej., nube de contratación y aprobaciones, sistemas de archivo), el Banco aplicará las garantías exigidas para transferencias o transmisiones internacionales y, de ser el caso, efectuará los registros ante el RNBD.

Tratamiento de datos sensibles y grabaciones

- * Biometría: solo para identidad y acceso a sedes; facultativa con alternativas; no se utiliza con fines comerciales.
- * Imagen/voz: CCTV: uso para seguridad, acceso restringido y plazo de conservación limitado. Reuniones/llamadas: grabación solo como evidencia, acta y para calidad; acceso restringido y uso interno.





Conservación y uso post-relación

- * La información de proveedores (terceros) se conservará durante la vigencia del acuerdo y por diez (10) años adicionales exclusivamente para cumplimiento legal, tributario, contable, auditoría, archivo y defensa judicial, administrativa.
- * CCTV: conservación limitada (usualmente ≤ 6 meses), salvo requerimiento y/o investigación.
- * Vencidos los plazos, el Banco procederá a la supresión o anonimización irreversible; durante la conservación residual, los datos no se usarán para finalidades distintas a las descritas.

2.3.7. Miembros de Junta Directiva.

El Banco trata la información estrictamente necesaria para acreditar, gestionar y documentar la investidura y actuación de sus Miembros de Junta Directiva, entre ellas:

- * Identificación y contacto: nombre, documento, nacionalidad, estado civil, firma, fecha y lugar de nacimiento; direcciones, teléfonos y correos electrónicos.
- * Información societaria y profesional: cargo, condición de miembro, designación, periodos, integración de comités, formación, experiencia, certificaciones exigidas por normativa aplicable.
- * Económico tributaria (proporcional): datos bancarios para pago de honorarios, RUT y soportes tributarios requeridos por ley.
- * TI y seguridad: usuarios, perfiles, credenciales y registros de acceso (logs) necesarios para seguridad de la información y continuidad del negocio.
- * Datos sensibles (solo si son indispensables): imagen (fotografías/CCTV), voz e imagen en reuniones virtuales o eventos, y biométricos (p. ej., huella) exclusivamente para autenticación, ingreso. El suministro de datos sensibles es facultativo, su uso será proporcional y el Banco ofrecerá alternativas no biométricas razonables. El Banco no solicitará permisos intrusivos en dispositivos personales (p. ej., contactos o galería) para fines de verificación o comunicaciones.

Finalidades del tratamiento:

a) Acreditación, gestión y documentación societaria.

- * Vinculación y actualización del Miembro de Junta: registro de designación, aceptación, posesión y calidades; inscripciones en el libro de actas, cámara de comercio u otras autoridades cuando proceda.
- * Convocatorias, comunicaciones y notificaciones sobre sesiones, comités, agenda y documentos de trabajo, por medios autorizados (correo, teléfono, mensajería).
- * Sesiones y actas: gestión, soporte y archivo de actas y anexos (incluidas reuniones virtuales cuando se convoquen bajo la normatividad aplicable).
- * Capacitaciones y actualización: evidencia de participación cuando aplique.
- * Constancias y certificaciones: emisión de constancias relativas al ejercicio del cargo o a decisiones del órgano colegiado, en lo pertinente al objeto social del Banco.





b) Cumplimiento normativo, vigilancia y control.

- * Cumplimiento legal y atención de autoridades: dar trámite a requerimientos de vigilancia y control (p. ej., SFC, SIC, Cámara de Comercio) y de autoridades judiciales, administrativas; revisoría fiscal y auditorías internas, externas; conservación de evidencias.
- * Prevención de LA/FT (cuando aplique): verificaciones proporcionales a la investidura (p. ej., PEP, listas) cuando así lo exija la normativa, con registro mínimo y finalidad exclusiva de cumplimiento.
- * Transparencia y gobierno corporativo: mantener información y soportes para asegurar trazabilidad de decisiones y debida diligencia del órgano directivo.

c) Honorarios, accesos y seguridad.

- * Honorarios y obligaciones tributarias: pago de honorarios y generación de certificaciones, soportes contables-tributarios exigidos por ley.
- * Accesos e identidad: creación y administración de usuarios, perfiles y credenciales para acceso a plataformas del Banco; control de acceso a instalaciones (biometría facultativa con alternativas), y registros de acceso (logs) para ciberseguridad y continuidad.
- * CCTV: seguridad de personas, bienes e instalaciones con señalización visible, acceso restringido y conservación limitada.
- * Reuniones virtuales y eventos: grabación cuando sea necesario para actas, constancia y archivo, y con autorización específica para difusión interna o externa (p. ej., comunicaciones institucionales).

d) Publicaciones e imagen (autorización separada).

- * Uso de imagen, voz con fines de difusión: publicaciones internas o externas (web, redes y piezas institucionales) únicamente con autorización separada, específica y revocable del Miembro de Junta. La negativa no afecta la investidura.

e) Soporte histórico y defensa.

- * Soporte histórico de la relación como Miembro de Junta y defensa judicial o administrativa frente a actuaciones, decisiones del órgano colegiado, en el marco de la normativa aplicable.

Terceros necesarios y encargados (transmisiones/transferencias):

Para cumplir las finalidades anteriores, el Banco podrá transmitir (encargar) o transferir datos solo en lo indispensable a:

- * Cámara de Comercio, SFC y demás autoridades competentes que exijan registros o requieran información.
- * Revisoría fiscal y auditores internos, externos, para verificaciones y certificaciones.
- * Proveedores encargados que soportan la operación del Banco (BPO, nube, plataformas de gobierno corporativo, gestión documental, mensajería), quienes actúan por cuenta





del Banco mediante contratos de transmisión con obligaciones de confidencialidad, seguridad, subencargo autorizado y retorno, supresión al cierre.

- * Entidades financieras para el pago de honorarios.
- * Si existiere tratamiento internacional (p. ej., plataformas en la nube ubicadas fuera de Colombia), el Banco aplicará las garantías para transferencias o transmisiones internacionales y, cuando proceda, realizará los registros ante el RNBD.

Tratamiento de datos sensibles:

- * Biometría: solo para autenticación, control de acceso o acreditación de consentimiento; facultativa, con alternativas no biométricas; no se usa con fines comerciales.
- * Imagen, voz: CCTV para seguridad con acceso restringido y plazo de conservación limitado. Reuniones virtuales y eventos: grabación solo para actas, constancia, archivo; difusión interna o externa únicamente con autorización separada.

Conservación y uso post-relación:

- * La información personal de los Miembros de Junta se conservará durante el ejercicio del cargo y por diez (10) años adicionales exclusivamente para cumplimiento legal (regulatorio), auditoría, archivo y defensa; luego se procederá a la supresión o anonimización irreversible.
- * CCTV: conservación limitada (usualmente ≤ 6 meses), salvo requerimiento de autoridad o investigación que exija un término superior.
- * Durante el término residual de conservación, los datos no se usarán para finalidades distintas a las descritas en esta cláusula.

2.3.8. Accionistas e Inversionistas

La categoría de datos que se tratarán para accionistas e inversionistas personas naturales y/o jurídicas, sus representantes legales y apoderados:

- * Identificación y contacto: nombre, tipo y número de documento, domicilio, teléfonos, correo electrónico.
- * Calidad y condición: accionista o inversionista; número y clase de acciones/valores; participación y variaciones.
- * Información y soporte de registro: inscripciones en el libro, órdenes de transferencia, poderes, formularios, actas y comunicaciones del emisor, depositante.
- * Trazabilidad de comunicaciones: convocatorias, comunicaciones institucionales, constancias de envío, recepción y preferencias de contacto.
- * Datos transaccionales con el emisor, depositante: movimientos en el libro de accionistas, pagos de rendimientos, dividendos, retenciones, certificaciones.

Finalidades del tratamiento:

- * Administrar el libro de accionistas y cumplir los deberes del emisor y, cuando aplique, del depositante (inscripciones, anotaciones, transferencias, cancelaciones y rectificaciones).





- * Atender trámites, quejas y solicitudes de accionistas e inversionistas (incluye certificaciones, constancias y actualización de datos).
- * Cumplir requerimientos de autoridades judiciales, administrativas, de vigilancia y control y de autorregulación, y atender auditorías y revisoría fiscal.
- * Gestionar riesgos (p. ej., LA/FT/anticorrupción) de acuerdo con la normativa aplicable y proporcional al riesgo.
- * Elaborar reportes estadísticos y de gobierno corporativo, así como soportar auditorías, revisoría fiscal.
- * Informar sobre hechos relevantes y actualidad financiera y no financiera del Banco, en los términos de la regulación aplicable.

Terceros necesarios y encargados (transmisiones, transferencias)

Para las finalidades anteriores, el Banco podrá transmitir (encargar) o transferir datos solo en lo indispensable a:

- * Depósitos, administradores del libro de accionistas o de valores (si aplica);
- * Autoridades competentes (judiciales, administrativas), organismos de vigilancia y control y autorreguladores;
- * Revisoría fiscal y auditores internos, externos;
- * Proveedores encargados que soporten procesos del Banco (BPO, nube, gestión documental, mensajería, plataformas de asambleas electrónicas), quienes actúan por cuenta del Banco bajo contratos de transmisión con obligaciones de confidencialidad, seguridad, subencargo autorizado, devolución, supresión al cierre.
- * Si existieren flujos internacionales (p. ej., plataformas de registro o archivo en el exterior), el Banco aplicará las garantías para transferencias o transmisiones internacionales y, cuando corresponda, realizará los registros en el RNBD.

Tratamiento de datos sensibles:

- * Como regla general, no se tratan datos sensibles de accionistas, inversionistas. Si excepcionalmente fuese necesario (p. ej., imagen, voz por reuniones virtuales de asamblea o CCTV en instalaciones): se limitarán al uso estrictamente necesario (seguridad, constancia, calidad y evidencia), con acceso restringido y plazos de conservación limitados ($CCTV \leq 6$ meses, salvo orden o investigación).

Conservación y uso post-relación:

- * Los datos se conservarán durante la vigencia de la relación como accionista, inversionista y por el término legal aplicable exclusivamente para archivo, defensa y auditoría; vencidos los plazos, el Banco procederá a la supresión o anonimización según corresponda.
- * Durante cualquier conservación residual, la información no se usará para finalidades distintas a las aquí descritas.

2.3.9. Visitantes de instalaciones físicas del Banco





El Banco trata la información estrictamente necesaria de los visitantes para controlar el acceso, proteger personas y activos, y atender emergencias, que incluye:

- * Identificación y contacto: nombre, tipo y número de documento, firma y teléfono de contacto.
- * Datos de seguridad y trazabilidad: fecha/hora de ingreso y salida, funcionario anfitrión, área de visita, registros de entrega, devolución de elementos de seguridad (si aplica).
- * Datos sensibles (solo si son indispensables): imagen (CCTV) para seguridad y, excepcionalmente, datos de salud cuando se trate de la atención de una emergencia o de cumplimiento de SG-SST (p. ej., registro de accidente o primeros auxilios).

El Banco no solicitará información socioeconómica o profesional salvo que sea indispensable por protocolos de seguridad o por exigencia legal aplicable (p. ej., contratistas en áreas críticas).

Finalidades del tratamiento:

- * Control de accesos y salidas a instalaciones (registro en portería, recepción).
- * Seguridad de personas y activos: monitoreo y prevención de incidentes, CCTV con señalización visible, y verificación de cumplimiento de protocolos internos de seguridad.
- * Gestión de emergencias y SG-SST: contacto en caso de contingencias, registro de incidentes/accidentes y atención de primeros auxilios (cuando corresponda).
- * Investigaciones internas y atención de autoridades: suministrar evidencias cuando exista requerimiento formal y procedente.
- * Trazabilidad: mantener constancia mínima de la visita (fecha/hora, anfitrión y área visitada).

Terceros necesarios y encargados:

Para cumplir las finalidades anteriores, el Banco podrá transmitir datos solo en lo indispensable a:

- * Autoridades judiciales, administrativas que lo requieran.
- * Aseguradoras, IPS, EPS, ARL (si hubo accidente o atención de emergencia),
- * Proveedores encargados que operan CCTV, control de accesos, BPO de vigilancia, archivo o nube, quienes actúan por cuenta del Banco bajo contratos de transmisión con obligaciones de confidencialidad, seguridad, devolución y supresión al cierre.

Tratamiento de datos sensibles:

- * CCTV, imagen: exclusivo para seguridad, con acceso restringido y uso limitado a investigación interna o atención de autoridad.
- * Salud: solo para emergencias o registros SG-SST; acceso restringido a personal autorizado; conservación mínima.

Conservación y uso post-visita:





- * CCTV: hasta seis (6) meses, salvo requerimiento de autoridad o investigación que exija término superior.
- * Registros aplicables de SG-SST (p. ej., reporte de accidente): 20 años desde el hecho, de conformidad con la normativa de SST.
- * Libro o sistema de visitas (datos no cubiertos por SG-SST): conservación por el plazo mínimo necesario para trazabilidad y seguridad (define internamente el término operativo; sugerencia: 1 año).
- * Vencidos los plazos, el Banco procederá a la supresión o anonimización; durante la conservación residual los datos no se usarán para fines distintos a los aquí descritos.

2.3.10. Visitantes del portal web.

La información que los visitantes suministren a través de los formularios en www.bancocontactar.com se limita a:

- * Identificación y contacto: nombre, tipo y número de documento (cuando sea necesario para el trámite), correo electrónico, teléfono y ciudad.
- * Datos de la solicitud: asunto, mensaje, categoría del trámite y archivos que el propio usuario adjunte.
- * Datos técnicos del canal: identificadores en línea y telemetría mínima para seguridad, autenticación y funcionamiento del sitio (p. ej., cookies necesarias).
- * El Banco no solicitará permisos intrusivos del dispositivo (p. ej., contactos o galería) para dar trámite a la solicitud.

Finalidades del tratamiento:

- * Atender y dar respuesta a solicitudes, quejas, reclamos, felicitaciones o peticiones de información remitidas por el visitante a través de los formularios del sitio.
- * Contactar al visitante para enviar comunicaciones relacionadas con su solicitud y, con consentimiento, remitir información comercial del Banco o de aliados (el visitante puede optar por no recibir en cualquier momento).
- * Formalizar registros cuando el visitante así lo solicite o sea necesario para continuar un proceso (p. ej., crear usuario, prospecto, postulante a vacante o cliente), siguiendo las reglas específicas de cada categoría de titular previstas en esta Política.
- * Seguridad del canal y prevención de fraude: verificación antifraude, bloqueo de actividad maliciosa y preservación de evidencias técnicas.
- * Cookies y tecnologías similares: Necesarias (funcionamiento del sitio); De seguridad, autenticación; De analítica, marketing solo con consentimiento, a través de aviso de cookies y panel de preferencias que el visitante puede gestionar en cualquier momento.

Geolocalización y notificaciones (opt-in): cuando el titular active la geolocalización en los canales digitales del Banco, se usará para: (i) indicarle puntos de atención cercanos, (ii) enviar notificaciones push informativas y comerciales con consentimiento y opt-out disponible, (iii) fortalecer prevención de fraude y seguridad del canal, y (iv) analítica para mejorar experiencia y ubicación de servicios, aplicando minimización y sin compartir ubicación con terceros salvo cuando sea necesario para la operación o exista consentimiento para fines comerciales.





Terceros necesarios y encargados:

- * Para las finalidades anteriores, el Banco podrá transmitir datos en lo estrictamente necesario a:
- * Proveedores, encargados de hosting, seguridad del sitio, plataformas de formularios, CRM, servicios de mensajería (email/SMS) y nube, quienes actúan por cuenta del Banco bajo contratos de transmisión con obligaciones de seguridad, confidencialidad, devolución y supresión al cierre;
- * Aliados comerciales únicamente si el visitante consintió recibir comunicaciones de dichos aliados;
- * Autoridades competentes, cuando exista requerimiento formal y procedente.
- * Si alguna plataforma se aloja en el exterior, el Banco aplicará las garantías para transferencias o transmisiones internacionales y, cuando corresponda, realizará los registros en el RNBD.

Conservación y uso post-interacción:

- * Los datos aportados en formularios se conservarán hasta por un (1) año desde la última interacción o manifestación de interés, o antes si el titular solicita supresión o revoca el consentimiento;
- * Cuando el visitante evoluciona a otra categoría (p. ej., prospecto, cliente o candidato), aplicarán los plazos y finalidades del numeral correspondiente de esta Política;
- * Los registros técnicos de seguridad podrán conservarse por el plazo mínimo necesario para soportar investigaciones o defensa ante incidentes del canal.
- * Vencidos los plazos, el Banco procederá a la supresión o anonimización; durante la conservación residual los datos no se usarán para fines distintos a los aquí descritos.

2.3.11. Menores de edad – Productos de ahorro.

Corresponde a niños, niñas y adolescentes (NNA) que se vinculan como titulares de productos de ahorro del Banco, en los cuales actúa un representante legal en los términos de la ley.

El Banco trata los datos estrictamente necesarios del menor y de su representante legal para la apertura, administración y operación del producto de ahorro, que incluyen:

- * Datos de identificación del menor: nombres y apellidos, tipo y número de documento, fecha y lugar de nacimiento, nacionalidad.
- * Datos de contacto del menor: cuando aplique (p. ej., dirección).
- * Datos del representante legal: nombres, identificación, parentesco, datos de contacto y firma.
- * Información financiera del producto: número de producto, movimientos, saldos, rendimientos, reglas del producto.
- * Datos técnicos y de seguridad: registros de acceso, autenticación y trazabilidad de transacciones.





- * Datos sensibles (excepcionalmente): biométricos, únicamente para autenticación o seguridad, cuando se ofrezcan y con alternativa no biométrica.

Finalidades del tratamiento:

Los datos personales del menor serán tratados exclusivamente para las siguientes finalidades:

- * Vinculación y administración del producto de ahorro, incluyendo apertura, mantenimiento y cancelación del producto.
- * Identificación y verificación de identidad del menor y de su representante legal.
- * Gestión operativa del producto, incluyendo registro de movimientos, administración de saldos y rendimientos, y atención de solicitudes relacionadas con el producto.
- * Cumplimiento de obligaciones legales y regulatorias, incluyendo reportes a autoridades administrativas, judiciales y de supervisión financiera.
- * Prevención de fraude, suplantación y operaciones irregulares, mediante mecanismos de autenticación y control proporcionales.
- * Atención de peticiones, quejas o reclamos relacionados con el producto.
- * Defensa judicial y administrativa del Banco frente a eventuales controversias.
- * Trazabilidad, auditoría y control interno, en cumplimiento de los deberes propios del sector financiero.
- * No se realizará marketing directo al menor. Cualquier comunicación comercial se dirigirá únicamente al representante legal, cuando exista autorización expresa.

Autorización y garantías especiales:

- * El tratamiento de los datos del menor requerirá autorización previa, expresa e informada del representante legal.
- * Cuando por su edad y madurez resulte razonable, el Banco informará al menor sobre el tratamiento de sus datos.
- * El Banco garantizará en todo momento el interés superior del menor, la confidencialidad reforzada y el acceso restringido a su información.
- * El menor podrá ejercer sus derechos a través de su representante legal.

Terceros necesarios y encargados:

Los datos podrán ser transmitidos únicamente a:

- * Autoridades judiciales, administrativas y de supervisión financiera, cuando sea procedente.
- * Proveedores tecnológicos y de servicios financieros que actúen como encargados, bajo contratos de transmisión con obligaciones de seguridad y confidencialidad.
- * Sistemas de pago, compensación o recaudo, cuando sea necesario para la operación del producto.

Conservación:





- * La información del menor se conservará durante la vigencia del producto de ahorro y posteriormente por diez (10) años, exclusivamente para fines legales, regulatorios, de auditoría y defensa.
- * Vencidos estos plazos, la información será suprimida o anonimizada según corresponda.

2.3.12. Otros titulares.

Este numeral aplica a las siguientes personas naturales cuyos datos personales puede tratar el Banco en el curso de su operación:

- * Cotitulares de productos y apoderados, autorizados (p. ej., cuentas compartidas, poderes especiales, tarjetas adicionales).
- * Garantes, deudores solidarios o avalistas que respalden obligaciones de clientes del Banco.
- * Referencias personales o comerciales reportadas por el titular para verificación puntual.
- * Contrapartes transaccionales (p. ej., ordenantes o beneficiarios de pagos, transferencias) vinculadas a operaciones que cursan a través del Banco.

Categorías de datos tratados:

- * Identificación y contacto: nombre, tipo y número de documento, firma (cuando aplique), nacionalidad, teléfono(s), correo(s) y dirección(es).
- * Datos operativos y de relación: calidad en la que actúa (cotitular, apoderado, autorizado, garante, referencia, ordenante, beneficiario), número de producto u operación asociada, reglas de operación autorizadas.
- * Información económico-financiera (solo cuando corresponda): para garantes, deudores solidarios, avalistas, datos proporcionales de riesgo necesarios para evaluación, seguimiento del respaldo (p. ej., ingresos, actividad económica, referencias y soportes exigidos por la ley o por el proceso de originación, administración).
- * Datos técnicos y de seguridad (mínimos): registros de acceso, autenticación y trazabilidad técnica y transaccional.
- * Datos sensibles (solo si son indispensables): biometría (autenticación, ingresos), imagen (CCTV) y voz, imagen en grabaciones de atención o reuniones exclusivamente para seguridad, calidad y evidencia. El Banco no solicitará permisos intrusivos del dispositivo (p. ej., lista de contactos o galería) para verificación, cobranza, originación u otros fines.

Finalidades del tratamiento:

a) Cotitulares, apoderados y autorizados.

- * Vinculación, acreditación y administración de la calidad y facultades (apertura o vinculación al producto, verificación de poderes, mandatos, altas, bajas, parametrizaciones).





- * Identificación, verificación y autenticación (incluida biometría con alternativas no biométricas), control de suplantación y prevención de fraude; trazabilidad de acciones y accesos.
- * Operación del producto y canales conforme las facultades conferidas; comunicaciones operativas (p. ej., alertas, confirmaciones y notificaciones de seguridad).
- * Cumplimiento regulatorio y atención de autoridades; defensa judicial, administrativa y auditoría.

b) Garantes, Deudores solidarios, Avalistas.

- * Evaluación y formalización del respaldo: verificación de identidad y análisis proporcional de riesgo (capacidad, colaterales, referencias, listas cuando aplique), constitución de garantías y documentación del soporte.
- * Administración y seguimiento del respaldo durante la vigencia de la obligación; comunicaciones relativas a su rol (p. ej., notificaciones de mora, requerimientos de pago).
- * Cobranza y recuperación en caso de incumplimiento, bajo prácticas no intrusivas (sin acceso a contactos, galería del dispositivo ni contacto a referencias con fines de cobranza).
- * Cumplimiento regulatorio (incluye, cuando aplique, verificación proporcional para LA/FT por la naturaleza del respaldo) y atención de autoridades; defensa y auditoría.

c) Referencias personales o comerciales.

- * Verificación puntual de la información suministrada por el titular exclusivamente para confirmar datos de contacto o aspectos básicos (vinculación, antigüedad, relación comercial) sin generación de perfiles comerciales ni usos distintos.
- * Trazabilidad mínima de la gestión de verificación y atención de autoridades si fuese requerido.

d) Contrapartes transaccionales (ordenantes, beneficiarios de pagos, transferencias.

- * Cursar y operar la transacción (pago, transferencia, recaudo, devolución) y mantener trazabilidad (soporte de la orden, cuenta de cargo, abono, fecha, monto, referencia).
- * Prevención de fraude y control de operaciones irregulares; controles de listas y señales mínimas cuando sean exigidos por normativa o por la naturaleza de la operación.
- * Cumplimiento de obligaciones legales y de supervisión (p. ej., cámaras/ACH, sistemas de pago, reportes cuando aplique); atención de autoridades; defensa y auditoría.

Terceros necesarios y encargados:

Para las finalidades anteriores, el Banco podrá transmitir (encargar) o transferir datos solo en lo indispensable a:

- * Sistemas de pago, compensación e interoperabilidad (p. ej., ACH, redes de pago) y entidades financieras participantes en la operación;





- * Burós u operadores de información (únicamente para garantes, avalistas y dentro del marco de la Ley 1266 de 2008, si aplica al proceso de evaluación, seguimiento del respaldo);
- * Autoridades administrativas, judiciales y de supervisión (p. ej., SFC, UIAF, SIC) cuando proceda; revisoría fiscal y auditores;
- * Proveedores encargados que soportan la operación del Banco (p. ej., BPO, nube, plataformas de onboarding, validación de identidad, prevención de fraude, mensajería y gestión documental), quienes actúan por cuenta del Banco mediante contratos de transmisión con obligaciones de seguridad, confidencialidad, subencargo autorizado, devolución y supresión al cierre.

Si alguna plataforma o almacenamiento se ubica en el exterior, el Banco aplicará las reglas de transferencias o transmisiones internacionales y, cuando corresponda, realizará los registros ante el RNBD.

Tratamiento de datos sensibles:

- * Biometría: solo para autenticación, ingreso, constancia de consentimiento; carácter facultativo con alternativas no biométricas; no se usa con fines comerciales.
- * Imagen (CCTV): uso exclusivo de seguridad, con señalización visible, acceso restringido y plazo de conservación limitado.
- * Voz, imagen en grabaciones de atención, reuniones: uso limitado a trazabilidad, calidad y evidencia; acceso restringido y conservación mínima.

Conservación y uso post-relación, operación:

- * Cotitulares, apoderados, autorizados: durante la vigencia del producto y por diez (10) años adicionales exclusivamente para cumplimiento legal (regulatorio), defensa y auditoría.
- * Garantes, deudores solidarios, avalistas: durante la vigencia de la obligación garantizada y por diez (10) años adicionales para fines de cumplimiento, defensa y auditoría; si existe proceso judicial, administrativo, por el tiempo que dure y el que la ley exija.
- * Referencias personales, comerciales: solo por el plazo mínimo necesario para la verificación puntual y para soportar la decisión de originación.
- * Contrapartes transaccionales: por el plazo mínimo necesario para trazabilidad y cumplimiento de obligaciones contables, tributarias, financieras y de prevención de fraude, sin exceder los términos legales aplicables a la documentación de la operación.
- * Durante cualquier conservación residual, los datos no se usarán para marketing ni para fines distintos a los aquí descritos; vencidos los plazos, se procederá a la supresión o anonimización irreversible.

2.3.13. Canales digitales - electrónicos

Este numeral aplica al tratamiento de datos personales realizado a través de los canales digitales del Banco (incluye aplicaciones móviles, portal transaccional, sitio web, webviews,





APIs, asistentes virtuales y demás canales electrónicos), tanto para clientes como para usuarios que interactúen con dichos canales.

En estos canales las categorías de datos tratados corresponden a:

- * Identificación y contacto según el perfil del titular (cliente, usuario).
- * Credenciales y seguridad: usuario, huellas técnicas de inicio de sesión, registros de acceso y eventos de ciberseguridad (logs).
- * Datos técnicos de canal (mínimos): dirección IP, dispositivo, navegador, identificadores de sesión, errores, trazas de rendimiento; telemetría y/o grabación de sesión (si se usa) exclusivamente para seguridad, soporte y mejora de experiencia (UX).
- * Geolocalización (solo si el titular la activa): ubicación aproximada o precisa para funciones informadas (p. ej., puntos de atención cercanos), seguridad antifraude y, con consentimiento, notificaciones push.
- * Cookies y tecnologías similares: necesarias para el funcionamiento; analítica, marketing solo con consentimiento a través del Panel de Preferencias.
- * Datos sensibles (solo si son indispensables): biometría del dispositivo para autenticación (p. ej., huella/rostro) o imagen, voz en videollamadas de onboarding.

Finalidades del tratamiento:

- * Autenticación y operación segura del canal (login, MFA, firma, autorización de transacciones, recuperación de acceso).
- * Prestación del servicio: consulta de productos, transacciones, solicitudes y PQRS; entrega de constancias y evidencias.
- * Ciberseguridad y prevención de fraude: detección de patrones anómalos, protección de la cuenta y del canal, preservación de evidencias.
- * Mejora continua de la experiencia (usabilidad, accesibilidad, estabilidad): uso proporcional de telemetría o grabación de sesión, anonimización cuando sea viable.
- * Comunicaciones operativas (alertas de seguridad, confirmaciones, cambios de condiciones) y, con consentimiento, comunicaciones comerciales del Banco (y de aliados solo si el titular lo autoriza).
- * Geolocalización y notificaciones push (opt-in): puntos de atención cercanos, seguridad, autenticación y comunicaciones informativas; marketing geolocalizado solo con consentimiento y opt-out disponible.
- * Cumplimiento legal (regulatorio), atención de autoridades y auditorías; defensa y archivo.

Permisos y configuración del dispositivo.

- * El Banco no accederá a contactos, fotos, galería ni a información del dispositivo no necesaria para las finalidades.
- * Permisos que podrán solicitarse, solo para la función indicada y con opt-in del usuario:
 - Cámara y micrófono: onboarding por video, lectura de QR o soporte remoto.





- **Biometría para autenticación reforzada en canales digitales:** Para proteger la identidad del cliente y prevenir suplantación, fraude en canales digitales, el Banco podrá requerir datos biométricos (p. ej., huella, rostro, voz) exclusivamente para autenticación y autorización de operaciones de alto riesgo, cuando (i) exista una evaluación de riesgo que lo justifique y (ii) el Banco haya determinado que no existe un mecanismo menos intrusivo con seguridad equivalente. El uso de biometría será objeto de autorización previa, expresa e informada del titular, tendrá finalidad exclusiva de seguridad (no se usará para marketing), se conservará por el tiempo mínimo necesario y se tratará con medidas reforzadas de seguridad. Si el titular no autoriza el tratamiento de su dato biométrico, podrá acceder al producto o servicio por canales no digitales que no requieran dicho tratamiento, de acuerdo con la disponibilidad operativa y los horarios del Banco. Esta previsión se adopta en cumplimiento de la Ley 1581 de 2012 (dato sensible, autorización explícita y principio de libertad) y de las instrucciones de la SFC sobre mecanismos fuertes de autenticación.
 - **Ubicación:** funciones de cercanía, seguridad y, con consentimiento, notificaciones contextualizadas.
 - **Notificaciones:** alertas de seguridad y comunicaciones.
- * El usuario podrá revocar permisos en la configuración del dispositivo o del perfil de la App; la negativa no afectará funciones no vinculadas a esos permisos.

Terceros y SDKs (transmisiones, transferencias).

- * Los proveedores (encargados) que soportan el canal (hosting, nube, Content Delivery Network, antifraude, analítica, mensajería push, grabación de sesión, soporte de apps) actúan por cuenta del Banco bajo contratos de transmisión con obligaciones de seguridad, confidencialidad y no acceden a los datos.
- * La analítica (marketing) solo se habilita con consentimiento a través del Panel de Preferencias; el titular puede gestionar sus opciones en cualquier momento.
- * Si existieren flujos internacionales, el Banco aplicará las garantías exigidas y, cuando corresponda, realizará los registros en el RNBD.
- * Seguridad y autenticación.
- * El Banco podrá emplear Autenticación Multifactor, biometría opcional y controles anti-suplantación; registra eventos SOC y logs necesarios, con acceso restringido.

Menores de edad (NNA).

- * En el uso de canales digitales por NNA, el Tratamiento se supedita al interés superior del menor y a la autorización del representante legal; no se realiza marketing ni contacto directo al menor.

Conservación.

- * Registros técnicos (accesos, transacciones, telemetría relevante para seguridad): por el plazo mínimo necesario para ciberseguridad, soporte, auditoría y defensa, en armonía con los términos especiales del producto, servicio y de la ley.





- * Cookies analítica: según la Política de Cookies y el Panel de Preferencias.
- * Vencidos los plazos regulatorios, se aplicará supresión o anonimización; la conservación residual no habilita usos distintos a los aquí descritos.

2.4 Tratamiento de datos sensibles (régimen operativo)

El Banco Contactor en su calidad de Responsable del tratamiento, podrá tratar datos personales sensibles únicamente cuando dicho tratamiento resulte estrictamente necesario, se encuentre legalmente permitido y respete los principios de proporcionalidad, finalidad, seguridad y confidencialidad previstos en la Ley 1581 de 2012.

Los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación, tales como los datos biométricos, datos de salud, imagen y voz, los cuales se someten a un régimen reforzado de protección.

El suministro de datos sensibles es facultativo, razón por la cual el Banco no condiciona el acceso a productos, servicios o relaciones jurídicas a su entrega, cuando existan alternativas razonables.

2.4.1 Datos biométricos:

El Banco podrá tratar datos biométricos (como huella dactilar, rasgos faciales u otros equivalentes) exclusivamente para las siguientes finalidades:

- * Autenticación y verificación de identidad, tanto en canales presenciales como no presenciales.
- * Control de acceso a instalaciones físicas o sistemas de información.
- * Prevención de fraude y suplantación.
- * Acreditación del consentimiento cuando sea necesario dejar constancia verificable del mismo.

El tratamiento de datos biométricos es requerido para autenticación reforzada en canales digitales, para proteger la identidad del cliente y prevenir suplantación, fraude en canales digitales, no se utiliza para fines comerciales, publicitarios ni de perfilamiento. se conserva únicamente por el tiempo mínimo necesario para la finalidad que le dio origen.

2.4.2 Datos relacionados con la salud:

Los datos de salud serán tratados únicamente para:

- * Cumplir la normativa vigente en materia de Seguridad y Salud en el Trabajo (SG-SST), incluyendo exámenes de ingreso, periódicos y de retiro.
- * Gestionar incidentes, accidentes laborales, determinación de origen y pérdida de capacidad laboral (PCL).
- * Atender requerimientos de EPS, ARL, IPS y autoridades competentes.
- * Atención de emergencias médicas dentro de las instalaciones del Banco.





El acceso a la información de salud es restringido al personal autorizado, y su conservación se limita a los plazos legales obligatorios.

2.4.3 Imagen y voz (videovigilancia, llamadas, reuniones y eventos)

a) **Videovigilancia (CCTV):** La imagen captada a través de cámaras de seguridad será tratada con la finalidad de: garantizar la seguridad de personas, bienes e instalaciones, apoyar investigaciones internas, atender requerimientos de autoridades competentes.

Las imágenes de CCTV se conservan por un plazo máximo de seis (6) meses, salvo que deban preservarse por orden de autoridad o investigación en curso, y cuentan con señalización visible en las instalaciones.

b) **Grabación de llamadas, reuniones virtuales y eventos:** La voz e imagen captada en llamadas, reuniones virtuales o eventos institucionales será tratada con las finalidades de: control de calidad, trazabilidad, constancia y evidencia, cumplimiento normativo.

La difusión externa de imagen o voz solo se realizará con autorización previa, expresa y revocable del titular, y nunca con fines distintos a los informados.

2.4.4 Factores de vulnerabilidad y seguridad

El Banco podrá tratar información asociada a factores de vulnerabilidad o riesgo únicamente para:

- * Realizar verificaciones mínimas y proporcionales necesarias para la gestión de la seguridad.
- * Adelantar investigaciones internas frente a incidentes o incumplimientos.
- * Preservar la seguridad de personas, activos e instalaciones.

2.4.5 Tratamiento por terceros y encargados.

El tratamiento de datos sensibles podrá ser realizado por terceros en calidad de Encargados, tales como: operadores de videovigilancia, proveedores de medicina laboral y ocupacional, servicios tecnológicos de nube, autenticación o antifraude.

Estos terceros actuarán exclusivamente por cuenta del Banco, mediante acuerdos de transmisión que incorporen obligaciones de confidencialidad, seguridad, limitación de finalidad, subencargo autorizado y supresión.

En caso de transferencias o transmisiones internacionales, el Banco aplicará las garantías exigidas por el Título V de la Circular Única y realizará, cuando corresponda, los registros ante el RNBD.

2.5 Obligaciones de los Encargados del tratamiento

- a) Tratar datos solo conforme a instrucciones y finalidades del Banco; no usarlos para fines propios.





- b) Implementar medidas de seguridad (técnicas, organizativas, jurídicas);
- c) Confidencialidad del personal; continuidad y gestión de vulnerabilidades.
- d) Notificar y co-gestionar incidentes de seguridad y suministrar información para reportar a la autoridad en ≤ 15 días hábiles
- e) No subcontratar sin autorización del Banco y sin trasladar obligaciones equivalentes; mantener registro de subencargados.
- f) Permitir auditorías y aportar evidencias; cooperar con autoridades a través del Banco.
- g) Asistir al Banco en derechos de los titulares, consultas y reclamos. Devolver y/o suprimir datos al cierre del encargo y no conservar copias salvo obligación legal; destrucción segura.
- h) Suscribir acuerdo de transmisión el que podrá ser incorporado en el contrato de servicios (objeto, alcance, medidas, subencargos, confidencialidad, colaboración, devolución, supresión, localización, flujos internacionales y RNBD).

Cuando el Banco actúe como Encargado

- i) Tratará los datos únicamente según instrucciones del Responsable y para las finalidades pactadas.
- j) Adoptará medidas de seguridad, confidencialidad y continuidad; llevará registro de actividades del encargo en lo pertinente.
- k) Cooperará en la atención de consultas, reclamos y requerimientos de autoridades.
- l) Notificará y co-gestionará incidentes de seguridad y aportará insumos para el reporte en ≤ 15 días hábiles.
- m) No subcontratará sin autorización y sin trasladar obligaciones.
- n) Devolverá, suprimirá los datos al finalizar el encargo (con certificación de destrucción segura).
- o) En flujos internacionales, aplicará garantías regulatorias y realizará los registros RNBD que el Responsable disponga.

CAPÍTULO TERCERO - DERECHOS DE LOS TITULARES

El Banco Contactor en su calidad de Responsable del tratamiento de datos personales, garantiza a todos los titulares (incluidos clientes, prospectos, usuarios, colaboradores, beneficiarios, proveedores (terceros), miembros de junta directiva, accionistas, visitantes, NNA y cualquier otro titular previsto en este Manual) el ejercicio gratuito, expedito y no discriminatorio de los siguientes derechos:

- a) Conocer, acceder y obtener copia de sus datos personales que reposen en las bases o sistemas del Banco.
- b) Actualizar y rectificar sus datos frente a información parcial, inexacta, incompleta, fraccionada o que induzca a error.
- c) Ser informado, previa solicitud, sobre el uso que el Banco ha dado a sus datos personales.
- d) Solicitar prueba de la autorización otorgada para el tratamiento, cuando el tratamiento requiera consentimiento y este haya sido el fundamento de legitimación.





- e) Revocar la autorización y/o solicitar la supresión del dato cuando: (i) no se respeten los principios, derechos y garantías constitucionales y legales; o (ii) haya desaparecido la finalidad o no exista deber legal o contractual de conservación.
- f) Oponerse a finalidades accesorias (p. ej., marketing o difusión externa de imagen, voz) sin afectar las finalidades necesarias (ejecución contractual, cumplimiento legal, seguridad).
- g) Presentar consultas y reclamos según el procedimiento y los plazos legales; recibir respuesta oportuna y de fondo dentro de los términos establecidos.
- h) Elevar quejas ante la Superintendencia de Industria y Comercio (SIC) por presuntas infracciones, previo agotamiento del trámite de consulta o reclamo ante el Banco.
- i) Acceder, en forma gratuita, al menos una vez al mes, a sus datos personales y a las respuestas de consulta o reclamo, sin costos de envío o reproducción en medios electrónicos estándar.
- j) Ejercicio por apoderados, causahabientes o representantes: los cónyuges o compañeros permanentes, los herederos, los padres de NNA y los apoderados debidamente acreditados pueden ejercer los derechos del titular con prueba idónea de su legitimación.
- k) Protección reforzada para datos sensibles y para Niños, Niñas y Adolescentes (NNA), con trato proporcional y mínimo conforme al interés superior del menor.

El Banco habilita, como mínimo, los canales gratuitos para el ejercicio de derechos que se señalan en el capítulo siguiente.

CAPÍTULO CUARTO - PROCEDIMIENTOS PARA EL EFECTIVO EJERCICIO DE DERECHOS

4.1. Aspectos generales.

4.1.1 Área designada: Banco Contactor ha designado al Oficial de Protección de Datos Personales como el responsable de recibir, gestionar, tramitar y responder las solicitudes, consultas y reclamos que presenten los titulares de datos personales relacionadas con el tratamiento de su información, de conformidad con la Ley 1581 de 2012 y el Decreto 1074 de 2015.

El Oficial de Protección de Datos actuará en coordinación con las áreas internas competentes y con los Encargados del tratamiento cuando sea necesario, garantizando la oportunidad, gratuidad, trazabilidad y calidad de las respuestas.

4.1.2 Mecanismos de atención habilitados.

Los titulares podrán ejercer sus derechos a través de los siguientes mecanismos gratuitos de atención:

- * Página web: <https://www.bancocontactar.com>
- * Línea telefónica: 323 254 0606
- * Correo electrónico: pqrs.banco@bancocontactar.com





- * Dirección física: Carrera 6 No. 22-90, Barrio El Ejido, Pasto – Nariño

El Banco podrá habilitar canales adicionales, los cuales serán informados en su Política de Tratamiento de Datos Personales publicada.

4.1.3 Ejercicio del derecho de consultas.

Los titulares, causahabientes, representantes legales o apoderados debidamente acreditados podrán consultar y acceder gratuitamente a la información personal que repose en las bases de datos del Banco y que esté vinculada con su identificación.

Requisitos de las consultas: La solicitud deberá presentarse por escrito e incluir, como mínimo:

- * Nombre completo y número de identificación del titular.
- * Descripción clara y específica de la información que se desea consultar.
- * Dirección física o electrónica para recibir la respuesta.
- * Documentos que acrediten la calidad de titular o la legitimidad del solicitante cuando se actúe en nombre de un tercero.

Trámite y plazos de respuesta de consultas:

- * El Banco dará respuesta a la consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de radicación de la solicitud.
- * Si no fuere posible atender la consulta dentro de dicho término, el Banco informará al solicitante antes del vencimiento, indicando los motivos de la demora y la nueva fecha de respuesta, la cual no podrá superar cinco (5) días hábiles adicionales.

Medio de respuesta a consultas: La respuesta será enviada por escrito al medio físico o electrónico indicado por el solicitante. Cuando se reporten varias direcciones de contacto, el Banco determinará el canal más idóneo para el envío de la respuesta.

4.1.4 Ejercicio del derecho de reclamos: Los titulares, causahabientes, representantes o apoderados debidamente acreditados podrán presentar reclamos cuando consideren que la información debe ser corregida, actualizada, suprimida, o cuando adviertan el incumplimiento de los deberes legales del Banco.

Requisitos de los reclamos: El reclamo deberá contener:

- Nombre completo y número de identificación del titular.
- Descripción clara de los hechos que dan lugar al reclamo y de los datos personales involucrados.
- Dirección física o electrónica para recibir la respuesta.
- Documentos que acrediten la calidad de titular o la legitimidad del solicitante.

Trámite y plazos de respuesta de reclamos:





Reclamo incompleto: Si el reclamo no reúne los requisitos señalados, el Banco requerirá al solicitante dentro de los cinco (5) días hábiles siguientes a su recepción para que lo complete. Si el solicitante no presenta la información requerida dentro de los dos (2) meses siguientes, se entenderá que ha desistido del reclamo, sin perjuicio de que pueda presentar uno nuevo.

Reclamo completo: Una vez recibido el reclamo completo, el Banco incorporará en la base de datos una leyenda que indique “reclamo en trámite” y el motivo del mismo, dentro de un plazo máximo de dos (2) días hábiles. El Banco resolverá el reclamo en un término máximo de quince (15) días hábiles, contados a partir del día siguiente a la fecha de recibo completo. Cuando no fuere posible atender el reclamo dentro de dicho plazo, se informará al solicitante los motivos de la demora y la nueva fecha de respuesta, la cual no podrá exceder ocho (8) días hábiles adicionales.

Medio de respuesta a reclamos: La respuesta será enviada por escrito al medio físico o electrónico suministrado por el solicitante. De existir múltiples direcciones, el Banco seleccionará el medio que garantice una comunicación más efectiva.

Requisito de procedibilidad ante la SIC: Antes de presentar una queja ante la Superintendencia de Industria y Comercio, el titular debe haber agotado previamente el trámite de consulta o reclamo ante el Banco. El agotamiento de este trámite constituye requisito de procedibilidad para que la autoridad nacional de protección de datos pueda conocer de la queja correspondiente.

CAPÍTULO QUINTO - FINANZAS ABIERTAS

5.1. Ámbito y activación.

El presente capítulo establece reglas generales para el tratamiento de datos personales en el marco de finanzas abiertas. Solo aplicará si el Banco informa previamente su participación a los consumidores financieros y publica en sus canales oficiales la activación de este modelo, de conformidad con la regulación de la Superintendencia Financiera de Colombia (SFC).

5.2. Principios y marco aplicable.

En finanzas abiertas el Banco observará, además de la Ley 1581 de 2012, Ley 1266 de 2008 (en lo pertinente) y esta Política, las instrucciones de la SFC para open finance (consentimiento, autenticación, seguridad, estandarización, revelación pública y no discriminación).

5.3. Consentimiento y autenticación del consumidor financiero.

Antes de cualquier circulación de datos, el Banco verificará la existencia de autorización





previa, expresa e informada del consumidor financiero con el contenido mínimo exigido por la SFC (identificación del tercero receptor, datos específicos, tratamiento, finalidad, y tiempo de la finalidad). El otorgamiento, modificación o revocatoria de dichas autorizaciones requerirá autenticación fuerte del consumidor, conforme a la regulación. No se condicionarán productos, servicios no relacionados con finanzas abiertas a otorgar esta autorización.

5.4. Terceros receptores de datos (reglas generales).

Si el Banco decide vincular terceros receptores de datos, adoptará políticas y procedimientos de vinculación y monitoreo aprobados por la Junta Directiva y publicados en la web, que contemplen, como mínimo: (i) verificación de RNBD o de políticas y procedimientos; (ii) procedimientos de consultas y reclamos; (iii) gestión de riesgos de seguridad y ciberseguridad, cifrado en reposo y tránsito con estándares internacionalmente reconocidos, monitoreo y gestión de vulnerabilidades; (iv) notificación temprana de incidentes; (v) verificaciones periódicas proporcionadas al riesgo y evidencia disponible para la SFC. El Banco no incurrirá en tratos discriminatorios frente a terceros que cumplan requisitos.

5.5. Estándares tecnológicos y de seguridad.

Los intercambios de información en finanzas abiertas deberán ajustarse a los estándares y protocolos exigidos por la SFC, adoptando los sustitutos que correspondan cuando los estándares sean actualizados por el organismo competente.

5.6. Derechos del consumidor financiero y canales.

El Banco garantizará al consumidor financiero canales accesibles y permanentes para consultar, actualizar o revocar sus autorizaciones de finanzas abiertas cuando proceda, sin perjuicio de los derechos de acceso, rectificación, actualización, supresión y reclamo previstos en esta Política y en la ley.

5.7. Revelación pública y educación financiera.

Al activarse este mecanismo de finanzas abiertas, el Banco publicará en su sitio web, en sección visible, la información y procedimientos requeridos por la SFC (consulta, actualización, revocatoria de autorizaciones, contactos de terceros receptores, canales de atención, supresión cuando aplique) y adelantará programas de educación financiera sobre derechos y responsabilidades del tratamiento de datos en este esquema.

CÁPITULO SEXTO - ASPECTOS FINALES

6.1. Medidas permanentes.





El Banco verificará de manera permanente y sistemática que en sus procesos, protocolos, procedimientos y políticas internas se garantice el derecho fundamental de hábeas data, aplicando controles de legalidad, seguridad, confidencialidad y responsabilidad demostrada.

6.2 Duración general

Los datos se conservarán por la vigencia de la relación y por el término adicional necesario para cumplimientos legales (regulatorios), archivo, auditoría y defensa, o por el plazo especial que prevea esta Política para determinadas categorías; vencidos los términos, se aplicará supresión o anonimización.

6.3. Cookies

Banco Contactor definirá una Política para el uso de las Cookies en su sitio web corporativo y sus aplicaciones móviles (Apps), en donde se establecen los términos de uso de estos archivos y los derechos de los Titulares en relación con la recolección de datos y el uso que se da a esta información personal.

6.4. Publicación, versiones y control de cambios.

La presente Política estará disponible en www.bancocontactar.com y en los canales físicos de atención. Toda actualización material será informada por los canales habituales del Banco, indicando la fecha de entrada en vigor y el resumen de cambios.

El Banco conservará histórico de versiones y el acta de aprobación por la instancia competente (Junta Directiva), con el fin de demostrar cumplimiento y trazabilidad.

6.5. Canales accesibles e inclusión.

El Banco procurará que la información sobre el Tratamiento de Datos Personales y los canales de ejercicio de derechos resulten accesibles para personas con discapacidad o barreras digitales, garantizando ajustes razonables cuando corresponda (p. ej., formatos alternativos, asistencia en oficina, línea telefónica).

6.6. Integración normativa y prevalencia.

En caso de conflicto entre la presente Política y normas imperativas, prevalecerán estas últimas. En lo no previsto, se aplicarán supletivamente la Ley 1581 de 2012, el Decreto 1074 de 2015, la Circular Única de la SIC, la Ley 1266 de 2008 y demás disposiciones aplicables.





6.7. Cambios y vigencia de la Política.

La presente Política de Tratamiento de Datos Personales rige por tiempo indefinido a partir del 21 de enero del año 2026, fecha en la cual fue aprobada su actualización por la Junta Directiva del Banco Contactor S.A.

Cualquier modificación sustancial será informada a los titulares a través de los canales dispuestos por el Banco y publicada en su sitio web.

