Banco Agrario de Colombia

Crecer juntos es posible

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Jefatura de Cumplimiento

Unidad de Protección de Datos

2025

Indice

Selecciona la pregunta para ir directo a la respuesta:

¿Para qué sirve esta Política?

El Banco Agrario de Colombia S.A., identificado con NIT 800.037.800-8, es una entidad financiera comprometida con el desarrollo rural y la inclusión social. En calidad de responsable del tratamiento de datos personales, emitimos esta política con dos objetivos principales:

Proteger tus derechos: Queremos que, como titular de los datos, tengas claridad sobre qué datos recolectamos, cómo los usamos, por qué los necesitamos y cómo puedes ejercer tus derechos (como conocer, actualizar o suprimir tu información).

Promover la responsabilidad en el manejo de los datos: Establece los lineamientos generales que orientan a nuestra organización para garantizar un tratamiento seguro, transparente y conforme con la ley. Con ello, damos cumplimiento al principio de responsabilidad demostrada, que implica que la entidad puede evidenciar las medidas adoptadas para proteger los datos personales y prevenir su uso indebido o no autorizado.

Esta política se aplica a todas las bases de datos físicas y digitales, manuales o automatizadas, que contengan información personal de empleados, clientes, proveedores, usuarios o contratistas.

Es de **cumplimiento obligatorio** para todos los colaboradores, contratistas, proveedores, responsables y aliados que, en el desarrollo de sus funciones o actividades, tengan acceso, manejen o realicen cualquier tipo de tratamiento sobre datos personales en nombre de la organización.

Nos regimos por lo establecido en la Constitución Política de Colombia (artículos 15 y 20), la Ley 1581 de 2012 (Protección de Datos Personales), la Ley 1266 de 2008 (Hábeas Data financiero), el Decreto 1074 de 2015 , la Ley 2300 de 2023 y demás normas complementarias.

En el tratamiento de los datos personales aplicamos los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, que orientan todas las actuaciones de la organización y garantizan el manejo responsable de la información personal.

¿Cómo puedes ejercer tus derechos (consultas y reclamos)?

Si quieres **conocer, actualizar, corregir, eliminar tus datos o revocar tu autorización**, puedes hacerlo de forma fácil y sin costo.

¿Cómo hacerlo? Solo debes enviarnos una solicitud a través de cualquiera de estos canales:

Dirección: Carrera 8 No. 15-42 Piso 9, Bogotá D.C

Líneas Telefónicas: Bogotá 6015948500 - 6013821400

Resto del País: 018000915000.

Página web: www.bancoagrario.gov.co

Correo: servicio.cliente@bancoagrario.gov.co
proteccion.datos@bancoagrario.gov.co

¿Qué debes incluir en tu solicitud?

- Tu nombre completo y tipo de documento.
- El derecho que quieres ejercer.
- Un medio para darte respuesta (correo electrónico o dirección física).

Importante: Ten en cuenta que las solicitudes relacionadas con el ejercicio de tus derechos se atenderán dentro de los plazos establecidos en la ley.

- Para consultas, el plazo máximo de respuesta es de diez (10) días hábiles, contados a partir de la fecha de recibo.
- Para reclamos o solicitudes de corrección, actualización o supresión, el plazo máximo es de quince (15) días hábiles, prorrogables por una sola vez hasta por ocho (8) días hábiles.

Si después de recibir nuestra respuesta consideras que tu solicitud no fue atendida de manera adecuada o crees que se han vulnerado tus derechos, puedes acudir de forma **subsidiaria ante la Superintendencia de Industria y Comercio (SIC)**, que es la autoridad encargada de velar por la protección de los datos personales en Colombia. Puedes hacerlo a través de los canales dispuestos en www.sic.gov.co.

¿Qué datos personales recolectamos?

Recolectamos solo los datos necesarios para cumplir con nuestras funciones, prestar nuestros servicios y cumplir la ley. Estos datos pueden variar dependiendo de tu relación con nosotros (cliente, proveedor, empleado, contratista, usuario, etc.).

A continuación, te contamos qué tipos de datos recolectamos:

Datos de identificación

Incluyen nombre, tipo y número de documento, fecha y lugar de nacimiento, firma (física o electrónica), nacionalidad, estado civil, entre otros.

Datos de contacto y ubicación

Dirección de correspondencia, número de teléfono, correo electrónico, lugar de residencia o trabajo, datos de geolocalización y georeferenciación.

Datos financieros o patrimoniales

Información sobre tus ingresos, egresos, historial crediticio, productos financieros que tengas, bienes muebles o inmuebles, entre otros datos necesarios para procesos contractuales o legales.

Datos sensibles

Solo recolectamos este tipo de datos cuando es estrictamente necesario y con tu autorización expresa. Por ejemplo: datos de salud, orientación sexual, datos biométricos (como huella, voz, rostro, iris), origen étnico, convicciones religiosas, políticas, socioeconómicos, etc.

Datos biométricos

Como tu voz, huella digital, imagen fotográfica o facial, utilizados, por ejemplo, para verificar tu identidad en procesos de autenticación o seguridad.

Datos laborales y académicos

Tu formación académica, experiencia laboral, historia de empleo, referencias, y otra información requerida en procesos de selección o gestión del talento humano.

Datos digitales

Incluye tu dirección IP, logs de conexión, historial de navegación en nuestras plataformas, usuarios, perfiles, actividad en apps o portales, entre otros.

Datos derivados de tecnologías emergentes

Como parte de la transformación digital y el uso de nuevas tecnologías, también recolectamos y tratamos:

- **Datos generados por sistemas de inteligencia artificial:** inferencias automatizadas, modelos predictivos, análisis de comportamiento y preferencias.
- **Datos derivados de análisis de Big Data:** segmentaciones, agrupamientos, correlaciones estadísticas y patrones de comportamiento.
- **Datos recolectados por interacción multicanal:** información obtenida a través de dispositivos IoT, asistentes virtuales, redes sociales, chatbots, y otros canales digitales.
- **Datos relacionados con blockchain (si aplica):** identificadores únicos, claves públicas, hashes de transacciones, registros en contratos inteligentes.

Importante: No recolectamos datos innecesarios ni los utilizamos para finalidades distintas a las que te informamos. Además, cuando recolectamos datos sensibles, siempre lo haremos cumpliendo con la Ley y solicitando tu consentimiento expreso.

¿Para qué usamos tus datos?

Usamos tus datos personales con finalidades específicas que encontrarás desarrolladas en nuestro **aviso de privacidad**, de acuerdo con el tipo de relación que tengas con nosotros.

- Si eres cliente o consumidor financiero

- Si eres cliente potencial o usuario
- Si eres colaborador, excolaborador o candidato en proceso de selección
- Si eres practicante o aprendiz SENA
- Si eres proveedor, oferente o contratista

En general, tratamos tus datos para:

- **Gestionar la relación contractual o precontractual, de los productos que tengas con el Banco (por ejemplo: créditos, cuenta de ahorros o tarjeta de crédito),** incluyendo validación de identidad, procesamiento de solicitudes, ejecución de servicios, cumplimiento de obligaciones y atención de requerimientos legales o administrativos.
- **Desarrollar procesos de selección, contratación, formación, evaluación y bienestar**, cuando se trate de colaboradores, practicantes o aprendices.
- **Realizar análisis, estudios y segmentación** para conocer tus preferencias, hábitos y necesidades, y así ofrecerte productos o servicios ajustados a tu perfil o generar estrategias de fidelización.
- **Ejecutar campañas, promociones, encuestas o actividades comerciales**, directamente o a través de terceros aliados.
- **Prevenir el fraude, el lavado de activos y la financiación del terrorismo**, mediante validaciones, cruces con listas de control y cumplimiento de normativa aplicable.
- **Actualizar y verificar tu información** a través de fuentes públicas y privadas, nacionales o internacionales, incluidas redes sociales, operadores de información y bases de datos autorizadas.
- **Hacer uso de tecnologías como Big Data, Inteligencia Artificial (IA), blockchain o IoT**, para mejorar procesos operativos, analíticos y de servicio al cliente.
- **Atender trámites administrativos, judiciales o contractuales**, incluidas visitas domiciliarias, controles de acceso, reportes a autoridades o defensa legal.
- **Cumplir obligaciones tributarias, contables, laborales o contractuales**, así como requerimientos de entes de supervisión o control.

Asimismo, te informamos que algunas de estas actividades podrán incluir el uso de tecnologías emergentes, tales como:

- **Inteligencia artificial (IA)** para el análisis automatizado de datos, toma de decisiones, perfilamiento, detección de anomalías o comportamientos inusuales, entre otros;

- **Big Data** para la identificación de patrones, segmentaciones y comportamientos con fines estadísticos, predictivos o de mejora continua;
- **Tecnología blockchain** para garantizar la trazabilidad, integridad, autenticación de transacciones y procesos, cuando aplique.

El uso de estas tecnologías se realiza bajo criterios de necesidad, proporcionalidad y respeto a los derechos de los titulares de los datos, en cumplimiento de los principios y deberes establecidos por la Ley 1581 de 2012, Ley 1266 de 2008 y demás normas aplicables.

En caso de que se realicen procesos de análisis automatizado o perfilamiento que puedan generar efectos jurídicos o significativos sobre las personas, garantizamos que tales decisiones no serán completamente automatizadas, sino que contarán con revisión e intervención humana.

Importante: Siempre te informaremos a través de nuestro **aviso de privacidad** la finalidad específica antes de recolectar tus datos. Si en algún caso deseamos usarlos para una nueva finalidad, te pediremos tu autorización previa cuando sea necesario, conforme a la Ley 1581 de 2012 y la Ley 1266 de 2008.

¿Qué tipo de datos tratamos?

Tratamos diferentes tipos de datos personales, dependiendo de la relación que tengas con nosotros y del servicio o actividad en la que participes. Siempre recolectamos solo los datos estrictamente necesarios, de manera **legal, legítima y proporcional**.

Estos son los principales tipos de datos que tratamos:

A. Datos personales de identificación y contacto

Incluyen tu nombre, tipo y número de documento, lugar y fecha de nacimiento, firma (física o digital), nacionalidad, sexo, estado civil, dirección, correo electrónico y número de teléfono.

B. Datos financieros, patrimoniales y comerciales

Información sobre ingresos, egresos, historial crediticio, cuentas bancarias, bienes o activos, productos contratados, comportamiento de pago, y otra información asociada a tu actividad económica o financiera.

C. Datos sensibles

Solo los tratamos si hay una justificación legal, una finalidad legítima y tu **autorización expresa**. Esto puede incluir:

- Datos biométricos: huella, imagen, rostro, iris, voz, firma, entre otros, siempre que sea necesario para verificar tu identidad con sistemas tecnológicos.
- Información de personas en condición de víctimas.
- Información sobre tu identidad de género, orientación sexual o expresión de género.
- Pertenencia a comunidades especiales o minorías protegidas: indígenas, afrodescendientes, raizales, palenqueras, entre otras.
- Historia clínica y datos de salud.
- Datos de georreferenciación y/o geolocalización.

D. Datos laborales y académicos

Incluyen tu hoja de vida, experiencia profesional, estudios realizados, referencias laborales, evaluaciones de desempeño, historial de empleo, afiliaciones al sistema de seguridad social, y demás relacionados con procesos de selección o gestión del talento humano.

E. Datos digitales y tecnológicos

Recolectamos ciertos datos derivados de tu interacción con nuestras plataformas digitales (sitios web, aplicaciones móviles, canales transaccionales, etc.), incluyendo:

- Dirección IP, logs de acceso, navegación en nuestros portales o aplicaciones.
- Interacción con correos, mensajes o notificaciones.
- Información recolectada mediante cookies, sistemas biométricos o de autenticación digital.

Adicionalmente, utilizamos **cookies y tecnologías similares** (como etiquetas de seguimiento, píxeles, SDK y herramientas de analítica) con las siguientes finalidades:

- Mejorar tu experiencia de navegación, mantener sesiones activas, recordar preferencias o configuraciones personalizadas.
- Realizar análisis de comportamiento, segmentación y personalización de contenidos o servicios.

- Medir el rendimiento de campañas publicitarias y ofrecer anuncios ajustados a tus intereses.
- Optimizar la funcionalidad de nuestras plataformas digitales y detectar posibles errores técnicos o de seguridad.

F. Datos públicos o provenientes de terceros autorizados

Información proveniente de bases de datos legítimas, públicas o privadas, como: centrales de riesgo, operadores de información del sistema de seguridad social (PILA), listas restrictivas, o entidades públicas nacionales o extranjeras.

Importante: No recolectamos datos innecesarios ni los usamos para fines distintos a los que te hemos informado. Siempre puedes consultar, actualizar, rectificar o suprimir tu información cuando lo consideres necesario.

¿Compartimos tus datos con terceros?

Sí. En algunos casos compartimos tus datos personales con terceros, pero solo cuando es necesario, está permitido por la ley, o tú nos has autorizado. Siempre lo hacemos respetando los principios de seguridad, confidencialidad, finalidad y legalidad.

La mayoría de estos terceros actúan como Encargados del Tratamiento, lo que significa que manejan tus datos personales por cuenta nuestra y siguiendo nuestras instrucciones. En otros casos, la información se comparte con autoridades o entidades que actúan como responsables independientes, en cumplimiento de obligaciones legales o contractuales, o con personas que tú hayas autorizado expresamente.

Compartimos tus datos en los siguientes casos:

A. Aliados y proveedores de servicios

- Empresas que nos prestan servicios de tecnología, seguridad, logística, mensajería, archivo, atención al cliente, cobranza, mercadeo, formación, o análisis de datos.
- Plataformas que usamos para análisis de información, campañas, atención digital o validación de identidad.

B. Autoridades y organismos de control

- Entidades judiciales, administrativas o tributarias cuando lo exige la ley.
- Superintendencias o entes de control en el ejercicio de sus funciones legales.

- Autoridades de investigación o policía judicial (cuando existe orden legal).

C. Aliados del sistema financiero o asegurador

- Centrales de riesgo crediticio o financiero, operadores del sistema PILA, entidades del sistema pensional y de seguridad social.
- Aseguradoras, fiducias, bancos o cooperativas, cuando el producto o servicio así lo exige.

D. Terceros autorizados por ti

- Personas naturales o jurídicas a las que tú expresamente autorices para consultar tu información.
- Abogados, apoderados o familiares que acrediten un interés legítimo o una representación válida.

E. Receptores en esquemas de datos abiertos

- Entidades públicas o privadas que participen en programas de interoperabilidad o datos abiertos, conforme a la ley, siempre y cuando cuenten con las medidas adecuadas de seguridad y confidencialidad.

Además, el Banco puede compartir información con Terceros Receptores de Datos (TRD) cuando la gestión de productos o servicios lo requiera. A continuación, se explica quiénes son y cómo se verifica su cumplimiento.

¿Quiénes son los Terceros Receptores de Datos o TRD?

Son personas jurídicas encargadas de manejar datos personales y financieros de los titulares de la información.

Verificación periódica: Durante toda la vigencia del contrato, el Banco realizará una verificación anual de estos requisitos. La frecuencia puede ajustarse según el perfil de riesgo del TRD y la naturaleza de la relación contractual. Cada verificación debe ser documentada, garantizando la transparencia y el cumplimiento normativo.

¿Qué requisitos deben cumplir los TRD para vincularse con el Banco y cómo se verifica su cumplimiento?

Los TRD deben presentar la política de protección de datos y el programa de tratamiento. Además, deben entregar al Banco los procedimientos para el ejercicio del habeas data,

atención de PQR, gestión de riesgos, revocatoria de consentimiento y manejo de incidentes de seguridad.

Estos requisitos se verifican **anualmente** y durante toda la relación contractual, conforme a la **Guía de Responsabilidad Demostrada de la SIC** y la **Circular Básica Jurídica**, dejando constancia documental de cada verificación.

Importante: El Banco Agrario de Colombia, en su calidad de **responsable del Tratamiento**, cumple con los deberes establecidos en el artículo 17 de la Ley 1581 de 2012, garantizando el ejercicio efectivo de los derechos de los titulares y la seguridad de la información.

De igual forma, los **Encargados del Tratamiento** que gestionen datos personales por cuenta del Banco deberán observar los deberes previstos en el artículo 18 de la misma ley, asegurando el cumplimiento de las condiciones de seguridad, confidencialidad y atención oportuna de los requerimientos de los titulares y de la Superintendencia de Industria y Comercio.

¿Tus datos se transfieren a otros países?

Sí. En algunos casos tus datos personales pueden ser transmitidos o transferidos a otros países, pero esto solo ocurre cuando es estrictamente necesario para prestar nuestros servicios, cumplir una obligación legal o desarrollar una actividad autorizada. Siempre aplicamos medidas que garanticen un nivel adecuado de protección, conforme a lo exigido por la normativa colombiana.

¿Cuál es la diferencia entre transmisión y transferencia internacional?

- **Transmisión internacional:** Ocurre cuando un tercero en otro país trata tus datos por encargo nuestro (por ejemplo, un proveedor tecnológico que presta servicios desde el exterior). Seguimos siendo los responsables del tratamiento.
- **Transferencia internacional:** Ocurre cuando compartimos tus datos con un tercero en otro país que los tratará como responsable (por ejemplo, una matriz o empresa aliada que necesita los datos para fines propios).

¿Cuándo hacemos transmisiones o transferencias internacionales?

- Cuando usamos servicios en la nube ubicados en servidores fuera del país.
- Cuando trabajamos con plataformas de análisis, atención, mensajería o marketing digital que operan desde el exterior.

- Cuando participamos en programas de interoperabilidad, datos abiertos o intercambio internacional de información financiera o tributaria.

- Cuando participamos en esquemas de **Finanzas Abiertas (Open Finance)**, en los que se permite el intercambio estandarizado de información financiera con otros actores, nacionales o internacionales, siempre que hayas otorgado tu autorización expresa conforme a la regulación vigente.

¿Qué garantías aplicamos?

- Verificamos que el país receptor ofrezca un nivel adecuado de protección
- Celebramos contratos de transmisión o transferencia con cláusulas específicas de seguridad, confidencialidad y cumplimiento de la ley
- Cuando exigimos a nuestros proveedores internacionales el cumplimiento de estándares técnicos, organizacionales y contractuales que garanticen el buen manejo de tu información.

¿Cómo protegemos tus datos?

Contamos con medidas técnicas, humanas y administrativas para proteger tus datos personales contra accesos no autorizados, pérdidas, filtraciones, alteraciones o usos indebidos. Estas medidas se ajustan al tipo de dato, al riesgo del tratamiento y a los estándares del sector financiero.

A. Medidas técnicas:

- Uso de firewalls, antivirus, cifrado de información y protocolos seguros de comunicación (como HTTPS).

- Sistemas de autenticación multifactor y control de accesos diferenciados.

- Monitoreo continuo de redes, alertas tempranas y gestión de vulnerabilidades.

B. Medidas organizacionales y humanas:

- Entrenamiento y sensibilización continua al personal sobre buenas prácticas de seguridad y privacidad.

- Acceso limitado a la información personal según el rol o función.

- Cláusulas de confidencialidad y protocolos para el manejo responsable de la información.

C. Medidas administrativas:

- Políticas internas de tratamiento de datos, gestión de incidentes y conservación de la información.
- Auditorías internas y externas para verificar el cumplimiento de estas políticas.
- Evaluaciones de impacto o análisis de riesgos en proyectos que involucren tratamiento de datos personales sensibles.

Adicionalmente, cuando implementamos nuevas tecnologías, servicios, plataformas o procesos que puedan implicar tratamiento masivo de datos personales, uso de datos sensibles o adopción de tecnologías emergentes (como inteligencia artificial o analítica avanzada), realizamos Evaluaciones de Impacto en Protección de Datos (EIPD).

Estas evaluaciones nos permiten anticipar riesgos, adoptar medidas preventivas, y garantizar que el tratamiento se haga conforme al principio de responsabilidad demostrada, conforme a los lineamientos de la Superintendencia de Industria y Comercio y estándares internacionales de privacidad.

Importante: Mantenemos actualizadas nuestras medidas de seguridad y realizamos revisiones periódicas para mitigar riesgos y responder adecuadamente ante cualquier incidente que pueda poner en riesgo tu información.

¿Qué pasa si ocurre un incidente de seguridad?

En caso de que ocurra un incidente que comprometa tus datos personales (por ejemplo, acceso no autorizado, pérdida, fuga o alteración) activamos de inmediato nuestro protocolo de respuesta.

A. Detección y contención inmediata:

- Identificamos el tipo de incidente y aislamos la causa para evitar que se extienda.
- Activamos nuestro equipo de respuesta y notificamos a las áreas responsables.

B. Evaluación del impacto:

- Analizamos los posibles efectos sobre tus derechos y el nivel de exposición de los datos comprometidos.
- Clasificamos el incidente según su criticidad.

C. Notificación a las autoridades y a los titulares:

- Si el incidente representa un riesgo relevante para tus derechos, informamos a la Superintendencia de Industria y Comercio dentro de los términos establecidos.
- Si es necesario, también te notificaremos directamente para que tomes medidas de protección.

D. Remediación y seguimiento:

- Tomamos medidas correctivas inmediatas para mitigar los daños y prevenir que vuelva a ocurrir.
- Documentamos todo el proceso y realizamos ajustes en nuestros controles de seguridad.

Importante: Tomamos muy en serio la seguridad de tus datos. Cada incidente es tratado con prioridad, y mantenemos un registro interno detallado para asegurar la trazabilidad, seguimiento y mejora continua de nuestro control.

¿Qué derechos tienes como titular de los datos?

Como titular de datos personales, tienes una serie de derechos que puedes ejercer en cualquier momento. Estos derechos están protegidos por la Constitución, la Ley 1581 de 2012 y demás normas que regulan el tratamiento de tu información en Colombia.

A. Conocer, actualizar y corregir tus datos:

Puedes solicitar en cualquier momento información sobre los datos personales que tenemos sobre ti, conocer el uso que les damos y pedir que los actualicemos, completemos o corrijamos si están incompletos, inexactos o desactualizados.

B. Solicitar prueba de tu autorización:

Tienes derecho a pedirnos copia de la autorización que otorgaste para el tratamiento de tus datos, salvo en los casos en que la ley no exige dicha autorización.

C. Ser informado sobre el uso de tus datos:

Puedes pedirnos que te informemos cómo hemos tratado tus datos personales y con qué finalidad.

D. Presentar reclamos o quejas ante la Superintendencia de Industria y Comercio (SIC) o la Superintendencia Financiera de Colombia (SFC):

Si consideras que hemos vulnerado tus derechos o incumplido las normas de protección de datos, puedes presentar una queja ante la SIC, autoridad encargada de velar por la protección de los datos personales en Colombia.

E. Revocar la autorización o solicitar la eliminación de tus datos:

Puedes pedirnos que eliminemos tus datos o revocar la autorización otorgada cuando consideres que el tratamiento no respeta los principios, derechos o garantías legales, o cuando haya cesado la finalidad para la cual fueron recolectados, salvo que exista un deber legal o contractual que nos obligue a conservarlos.

F. Acceder de forma gratuita a tus datos:

Puedes consultar gratuitamente tus datos personales que hayan sido objeto de tratamiento, de acuerdo con los procedimientos y plazos establecidos por la ley.

Te notificaremos cualquier cambio sustancial en esta política y en la forma como tratamos tu información. Para ello, utilizaremos mecanismos como:

- Publicación en nuestra página web.
- Envío de correo electrónico a la dirección registrada.
- Avisos a través de nuestras aplicaciones o canales digitales.
- Otros medios que resulten eficaces según la naturaleza del cambio y el canal de relación contigo.

Importante: No estás obligado a autorizar el tratamiento de tus datos sensibles o de menores de edad. Siempre puedes ejercer tus derechos a través de los canales que hemos habilitado (ver Pregunta 11).

¿Cuánto tiempo conservamos tus datos?

Conservamos tus datos personales solo por el tiempo necesario para cumplir con la finalidad para la cual fueron recolectados, o mientras exista una obligación legal, contractual o institucional que lo justifique.

¿De qué depende el tiempo de conservación?

Depende de factores como:

- La naturaleza de la relación contigo (cliente, proveedor, colaborador, usuario, etc.).

- El tipo de datos tratados (financieros, laborales, sensibles, etc.).
- Las normas legales y reglamentarias que nos obligan a conservar cierta información.
- Los plazos de prescripción de obligaciones legales, contractuales o judiciales.
- Las políticas internas de archivo, auditoría o cumplimiento.

¿Qué pasa cuando ya no es necesario conservarlos?

- Eliminamos, suprimimos o anonimizamos los datos personales, según el caso.
- Si los datos forman parte de registros que deben conservarse por ley (como información financiera o tributaria), los bloqueamos para que no sean usados con otras finalidades.

Importante: Aunque solicites la supresión de tus datos, en algunos casos debemos conservarlos por más tiempo debido a mandatos legales o contractuales. Te informaremos cuando esto ocurra.

¿Tratamos datos de niños, niñas y adolescentes?

Sí, pero con condiciones especiales. El tratamiento de datos personales de niños, niñas y adolescentes (NNA) solo está permitido cuando se cumplan estrictamente los siguientes requisitos:

A. Finalidades del tratamiento de datos de menores: Se podrán tratar datos de menores únicamente para fines legítimos y claros, como:

- Vinculación a productos o servicios del Banco dirigidos a menores.
- Servicios de bienestar o programas institucionales para hijos de colaboradores.
- Participación en actividades de formación, aprendizaje o prácticas laborales (como aprendices SENA).

B. Autorización reforzada: En todos los casos en que tratemos datos de menores o datos sensibles, aplicamos una autorización **previa, expresa y reforzada**, otorgada por su **representante legal**, e informando al menor cuando sea posible, de acuerdo con su nivel de madurez. Esto significa que:

• Informamos de manera clara la finalidad y el carácter opcional del tratamiento.

• Aclaramos que no existe obligación de suministrar datos sensibles ni de menores.

• Garantizamos que el tratamiento se realiza bajo el principio del **interés superior del menor**, asegurando su protección integral y respeto a su dignidad.

Importante: Nunca tratamos datos de NIÑOS, NIÑAS Y ADOLESCENTES para fines distintos a los autorizados, ni los compartimos con terceros sin el cumplimiento estricto de las condiciones legales.

¿Qué debes saber sobre el esquema de Open Finance y datos abiertos?

En línea con el marco normativo colombiano, el Banco participa en iniciativas de inclusión financiera que promueven el uso de datos abiertos y el modelo de Finanzas Abiertas (Open Finance), regulado por normas como el Decreto 1297 de 2022, la Ley 2294 de 2023 (artículos 89 y 94) y la Circular Externa 04 de 2024 de la Superintendencia Financiera de Colombia.

¿Qué es Open Finance?

Es una práctica que permite al consumidor financiero autorizar al Banco para compartir sus datos con otras entidades vigiladas o terceros autorizados, a través de un sistema estandarizado, con el fin de acceder a mejores productos y servicios financieros. Esta práctica busca fomentar la competencia, la innovación y el acceso inclusivo a servicios financieros.

¿Qué datos pueden circular?

Los datos personales y financieros que hayas autorizado a compartir pueden ser utilizados por el Banco o solicitados por otras entidades financieras, siempre respetando tu consentimiento previo, informado y explícito.

¿Quiénes pueden acceder a los datos?

Los terceros receptores de datos (TRD) son entidades que pueden recibir y tratar tus datos con autorización. Para ello, deben cumplir requisitos mínimos como:

- Acreditar su política y programa de tratamiento de datos.
- Contar con canales para que puedas ejercer tus derechos (consultas, reclamos, supresión, revocatoria, etc.)
- Tener mecanismos de seguridad de la información y gestión de riesgos asociados al tratamiento de datos personales.

- Permitir la revocatoria del consentimiento y la supresión de datos personales.
- Implementar procedimientos para gestión de incidentes de seguridad de la información.

¿Cada cuánto se verifica esto?

El Banco realiza una verificación anual y periódica del cumplimiento de los requisitos por parte de los TRD, de acuerdo con su perfil de riesgo y la relación contractual vigente. Esta verificación garantiza la protección de tus datos y el cumplimiento normativo.

En todo momento, el Banco vela por el cumplimiento de la Ley 1581 de 2012, Ley 1266 de 2008, Ley 1712 de 2014, y demás normas que protegen tu información. Aunque los datos abiertos promueven la disponibilidad y el acceso, tu autorización sigue siendo un requisito indispensable para cualquier tratamiento.

¿Cómo tratamos los datos recolectados a través de redes sociales y canales digitales?

El Banco también trata datos personales que recolecta a través de sus canales digitales, incluyendo redes sociales (como Facebook, Instagram, LinkedIn, X, YouTube, entre otras), formularios web, chatbots, aplicaciones móviles y otros entornos digitales oficiales.

Estos datos pueden incluir:

- Información de identificación y contacto que tú mismo suministras voluntariamente.

- Datos de interacción, como clics, comentarios, “me gusta”, respuestas a encuestas, formularios o descargas de contenido.

- Datos técnicos, como tu dirección IP, tipo de dispositivo, sistema operativo, navegador, ubicación general, hora de conexión, entre otros.

Usamos esta información para:

- Atender tus solicitudes, responder mensajes, comentarios o reclamos.

- Analizar tu experiencia de navegación y mejorar la usabilidad de nuestras plataformas.
- Ofrecer contenido personalizado, enviar comunicaciones de interés o promociones cuando lo hayas autorizado.
- Realizar análisis de comportamiento y medir la efectividad de nuestras campañas.

El tratamiento de estos datos se realiza conforme a esta política y a los términos de uso de cada plataforma. Recuerda que la información que compartes en redes sociales también está sujeta a las políticas de privacidad de dichas plataformas.

¿Cuáles son nuestros mecanismos de autenticación y trazabilidad?

Para proteger tus datos personales, contamos con mecanismos robustos de autenticación, control de acceso y trazabilidad, aplicables tanto a nuestros usuarios como al personal autorizado con acceso a bases de datos.

Entre estas medidas se incluyen:

- Autenticación multifactor (MFA): Algunos servicios digitales requieren verificación en dos o más pasos (por ejemplo, contraseña + código SMS o verificación biométrica).
- Biometría: En algunos procesos se utiliza el reconocimiento facial, huella digital o firma electrónica biométrica, con el fin de validar tu identidad y prevenir suplantaciones.
- Trazabilidad y auditoría: Todas las actividades de acceso, modificación o consulta de bases de datos personales son registradas mediante logs de auditoría. Estos registros permiten detectar accesos no autorizados y garantizar la rendición de cuentas.
- Controles de acceso basados en perfiles: Solo el personal autorizado puede acceder a los datos personales, conforme al principio de mínimo privilegio.

Estas medidas se complementan con nuestras políticas internas de seguridad de la información, gestión de incidentes y control de usuarios, conforme a los lineamientos de la Guía de Responsabilidad Demostrada y la normativa vigente en protección de datos.

¿Qué hace el Oficial de Protección de Datos Personales (OPD) y qué funciones tiene?

El Oficial de Protección de Datos (OPD) es la persona encargada de velar porque se cumplan las normas sobre protección de datos personales dentro de nuestra organización. También es el punto de contacto para resolver tus dudas, recibir tus solicitudes o reclamos, y garantizar tus derechos como titular de datos.

El OPD actúa con independencia, confidencialidad y enfoque preventivo, para que el tratamiento de tu información sea seguro, transparente y conforme a la ley.

¿Dónde encuentro las definiciones, términos legales y anexos de esta política?

Si quieres comprender mejor los conceptos usados en esta política o conocer el marco normativo que la sustenta, hemos preparado una sección complementaria con:

Glosario legal: Incluye las definiciones más importantes relacionadas con la protección de datos personales.

Puedes acceder a esta información al final del documento o solicitarla directamente a través de nuestros canales de atención.

Estos recursos están diseñados para ayudarte a entender mejor tus derechos, nuestras obligaciones y cómo protegemos tu información.

¿Desde cuándo aplica esta política y por cuánto tiempo?

Esta política de protección de datos personales rige a partir del 1 de enero de 2026 y permanecerá vigente mientras el Banco continúe realizando actividades de tratamiento de datos personales, o hasta que sea modificada, actualizada o reemplazada por una nueva versión.

Cualquier cambio sustancial en su contenido será informado a los titulares de los datos a través de los canales oficiales del Banco Agrario de Colombia. Esto incluye, por ejemplo, cambios en las finalidades del tratamiento, en los derechos de los titulares o en los canales habilitados para ejercerlos.

La vigencia de las bases de datos dependerá de la finalidad para la cual fueron recolectados los datos, respetando los términos legales aplicables, los plazos contractuales o el ejercicio legítimo de derechos del Banco o de los titulares.

Cuando realicemos cambios sustanciales en esta política, te lo haremos saber por medio de los canales que usamos habitualmente para comunicarnos contigo. Estos pueden incluir:

- Nuestra página web institucional.
- Correo electrónico registrado.
- Notificaciones en nuestras plataformas digitales o apps.
- Cartas físicas, mensajes de texto u otros medios disponibles.

La notificación incluirá un resumen de los cambios más relevantes, la fecha de entrada en vigor, y las instrucciones para ejercer tus derechos si no estás de acuerdo con los nuevos términos.

Anexo Técnico: Glosario y Marco Normativo de Protección de Datos Personales

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de sus datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Información que por su naturaleza puede estar contenida en registros públicos, documentos públicos o boletines oficiales, como el estado civil de las personas, su profesión u oficio y su calidad de comerciante o servidor público.

Dato privado: Es la información que por su naturaleza íntima o reservada solo interesa al titular, como la historia clínica, hábitos de vida o información financiera.

Dato sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación, como datos sobre salud, orientación sexual, convicciones religiosas, origen étnico, entre otros.

Encargado del tratamiento: Persona natural o jurídica que realiza el tratamiento de datos por cuenta del responsable.

Incidente de seguridad: Evento que compromete la confidencialidad, integridad o disponibilidad de los datos personales.

Oficial de Protección de Datos (OPD): Persona designada para supervisar y coordinar el cumplimiento de las políticas y normas de protección de datos en la organización.

Responsable del tratamiento: Persona natural o jurídica que decide sobre la base de datos y/o el tratamiento de los datos.

Tratamiento: Cualquier operación sobre datos personales, como su recolección, almacenamiento, uso, circulación o supresión.

Transferencia internacional: Envío de datos personales a otro país donde el receptor actúa como responsable del tratamiento.

Transmisión internacional: Envío de datos personales a otro país para que un encargado realice el tratamiento por cuenta del responsable.

Titular: Persona natural cuyos datos son objeto de tratamiento.

Autenticación multifactor: Proceso de verificación de identidad que combina dos o más factores, como contraseña, huella digital o código enviado al teléfono móvil.

Big Data: Procesamiento masivo y automatizado de grandes volúmenes de datos estructurados y no estructurados para detectar patrones, correlaciones o tendencias útiles.

Blockchain: Tecnología de registro distribuido que permite almacenar información de forma segura, transparente e inalterable mediante bloques encadenados entre sí. Se usa, entre otros, para trazabilidad, registros seguros y contratos inteligentes.

Cookies: Archivos que se almacenan en el navegador del usuario cuando visita un sitio web. Permiten recopilar datos de navegación, preferencias o comportamiento para mejorar la experiencia del usuario o personalizar contenidos.

Datos biométricos: Datos personales relacionados con las características físicas, fisiológicas o de comportamiento de una persona que permiten su identificación (por ejemplo, huella digital, reconocimiento facial, voz, iris, etc.).

Datos de interacción multicanal: Información recolectada a través de diversos puntos de contacto digitales con el usuario, como chatbots, apps móviles, redes sociales, call centers, o formularios web.

Datos inferidos: Información generada a partir del análisis de datos personales recolectados, mediante procesos estadísticos o tecnologías de inteligencia artificial. Pueden incluir perfiles de riesgo, preferencias, comportamientos, entre otros.

Finanzas Abiertas (Open Finance): Esquema regulado en Colombia mediante el Decreto 1297 de 2022 y la Circular Externa 004 de 2024, que permite el intercambio de datos financieros del consumidor entre entidades vigiladas por la Superintendencia Financiera, con previa autorización del titular.

IA (Inteligencia Artificial): Conjunto de tecnologías que permiten a sistemas informáticos realizar tareas propias de la inteligencia humana, como análisis, predicción, clasificación, segmentación o toma de decisiones automatizada.

Interoperabilidad: Capacidad de distintos sistemas o plataformas para intercambiar información de forma efectiva, segura y estandarizada.

IoT (Internet de las Cosas): Red de objetos físicos conectados a internet que pueden recopilar, enviar o recibir datos. Por ejemplo, sensores, dispositivos móviles, wearables, entre otros.

Perfilamiento algorítmico: Proceso automatizado de categorización de personas con base en modelos estadísticos o de aprendizaje automático, utilizado para segmentar, predecir comportamientos o tomar decisiones.

Píxel de seguimiento: Fragmento de código invisible insertado en páginas web o correos electrónicos que permite rastrear la actividad del usuario.

Trazabilidad digital: Registro de los eventos, acciones o accesos realizados sobre datos personales en los sistemas de información de la organización.

Terceros receptores de datos (TRD): Entidades externas que, previa autorización del titular y verificación de requisitos legales, pueden recibir datos personales en el marco del esquema de Open Finance.

2. Marco Normativo Aplicable en Colombia

- Constitución Política de Colombia: Artículos 15 y 20.
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1266 de 2008: Régimen de Habeas Data Financiero.
- Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, capítulos 25 a 27.
- Ley 2300 de 2023 – Ley de Desconexión de Canales Digitales.
- Ley 2294 de 2023 – Plan Nacional de Desarrollo (Art. 89 y 94 sobre Open Finance).
- Circular Única de la Superintendencia de Industria y Comercio: Particularmente el Título V.
- Guías oficiales de la SIC:

    I. Guía para la implementación del principio de responsabilidad demostrada (accountability).
    II. Guía de gestión de incidentes de seguridad de la información.
    III. Guía para el registro de bases de datos.

Nota: Este anexo es parte integral de la política de tratamiento de datos personales y se actualiza conforme a cambios normativos, operativos o tecnológicos que afecten la forma en que se protegen los datos personales en la organización.