LOS RETIROS

REFORESTADORA Y MANUFACTURERA

MANUAL DE
POLÍTICAS PARA EL TRATAMIENTO DE DATOS PERSONALES

2026 – Versión 03

CONTENIDO

1. INTRODUCCIÓN

REFORESTADORA Y MANUFACTURERA LOS RETIROS S.A.S. (en adelante, la "Compañía") adopta el presente Manual de Políticas para el Tratamiento de Datos Personales con el propósito de proteger el derecho fundamental de habeas data, asegurar el tratamiento legítimo de la información y establecer reglas comprensibles, verificables y operativas para todos los procesos que involucren datos personales.

El Manual regula el ciclo de vida de los datos, desde su recolección hasta su archivo, anonimización, devolución o eliminación, e integra reglas para las relaciones laborales, societarias, comerciales, contractuales, tecnológicas y de cumplimiento, así como para las transferencias y transmisiones nacionales e internacionales.
La Compañía aplicará el principio de responsabilidad demostrada, por lo cual conservará evidencias de las autorizaciones, evaluaciones, contratos, medidas de seguridad, capacitaciones, incidentes, reportes regulatorios y demás actuaciones que acrediten el cumplimiento de este Manual.

2. MARCO NORMATIVO

- Artículo 15 de la Constitución Política de Colombia y demás disposiciones constitucionales aplicables.
- Ley Estatutaria 1581 de 2012.
- Decreto 1377 de 2013, en las disposiciones compiladas y vigentes.
- Decreto Único Reglamentario 1074 de 2015, particularmente el régimen general de protección de datos personales y el Registro Nacional de Bases de Datos.
- Decreto 090 de 2018, en cuanto a los sujetos obligados al RNBD.
- Decreto 255 de 2022, sobre Normas Corporativas Vinculantes, cuando resulte aplicable.
- Circular Única de la Superintendencia de Industria y Comercio, Título V, en su versión vigente.
- Circular Externa No. 002 del 7 de octubre de 2025, en los procesos de transferencia de tecnología que involucren datos personales o tecnologías destinadas a su Tratamiento.
- Circular Externa No. 003 del 19 de diciembre de 2025, publicada en enero de 2026, y sus cláusulas contractuales modelo para transferencias y transmisiones internacionales.
- Estándares de Protección de Datos Personales aprobados por la Red Iberoamericana de Protección de Datos.
- Ley 1273 de 2009 y demás disposiciones sobre protección de la información y delitos informáticos.
- Código de Comercio, normas laborales, tributarias, societarias, contables y de conservación documental que resulten aplicables.

Las referencias normativas se entenderán hechas a las normas que las modifiquen, adicionen, sustituyan o compilen. El Área de Cumplimiento revisará al menos una vez al año la vigencia del marco regulatorio y documentará los ajustes que deban incorporarse al Manual.

3. RESPONSABLE DEL TRATAMIENTO, UBICACIÓN Y CONTACTO

El Responsable del Tratamiento es REFORESTADORA Y MANUFACTURERA LOS RETIROS S.A.S. sociedad constituida conforme a la legislación colombiana, con domicilio en Medellín, Antioquia.

Dato	Información
Dirección	Calle 5A No. 39-131, torre 4, piso 3, Centro de Trabajo Corfin, Medellín, Antioquia.
Teléfono	(+57 604) 448 60 67
Correo de habeas data y notificaciones	notificacionesjudiciales@valoresind.com
Horario de atención	Lunes a viernes de 8:00 a. m. a 5:30 p. m.

El Área de Cumplimiento será la dependencia encargada de tramitar las consultas, reclamos, peticiones, solicitudes de supresión y revocatoria, sin perjuicio del apoyo que deban prestar Tecnología, Recursos Humanos, Secretaría General y los propietarios de las bases de datos.

Para efectos de la recepción y gestión de consultas, reclamos, peticiones, solicitudes de supresión, revocatoria de autorización y demás requerimientos relacionados con el tratamiento de datos personales, el canal de contacto será el correo electrónico **notificacionesjudiciales@valoresind.com**. Este correo es de propiedad y dominio de **Valores Industriales S.A.**, sociedad encargada de centralizar y gestionar estos asuntos en apoyo de Reforestadora y Manufacturera los Retiros S.A.S. en calidad de Responsable del Tratamiento. La designación de este canal no implica la transferencia de las responsabilidades que, conforme a la normativa aplicable, corresponden a Reforestadora y Manufactuerar los Retiros S.A.S.

4. OBJETO, ALCANCE Y DESTINATARIOS

Este Manual se aplica a todas las bases de datos, archivos, libros, expedientes, aplicaciones, plataformas, servicios en la nube y repositorios que contengan datos personales y sean administrados por la Compañía o por terceros por cuenta de esta.
También aplica cuando la Compañía actúe como Encargado de otro Responsable, cuando permita accesos remotos, cuando utilice proveedores tecnológicos, cuando comparta información con sociedades vinculadas o aliados y cuando se efectúen flujos nacionales o internacionales.

- Representantes legales, administradores y miembros de órganos sociales.
- Empleados, practicantes, aprendices, temporales, aspirantes y exempleados.
- Clientes, proveedores, contratistas, consultores, aliados y sus personas de contacto.
- Accionistas, beneficiarios, apoderados, representantes y demás vinculados societarios.
- Responsables, Encargados y Subencargados que traten datos por cuenta o en relación con la Compañía.
- Visitantes, peticionarios, usuarios del sitio web y cualquier persona cuyos datos sean tratados.

5. DEFINICIONES.

Autorización: Consentimiento previo, expreso e informado del Titular para realizar el Tratamiento, salvo las excepciones legales.
Aviso de privacidad: Comunicación mediante la cual el Responsable informa la existencia de la Política, la forma de acceder a ella y las finalidades principales.
Base de datos automatizada: Conjunto organizado de datos administrado mediante aplicaciones, sistemas, servidores, computadores, hojas de cálculo, plataformas o servicios tecnológicos.
Base de datos manual o física: Conjunto organizado de datos contenido en libros, carpetas, formularios, expedientes u otros soportes no automatizados.
Base de datos mixta: Base que combina soportes físicos y digitales.
Causahabiente: Persona que sucede al Titular en sus derechos por causa de su fallecimiento.
Cesión o comunicación: Revelación o puesta a disposición de datos a una persona diferente del Titular y de quien estaba legitimado para recibirlos.
Corresponsable: Persona que, conjuntamente con otro Responsable, determina las finalidades y medios esenciales del Tratamiento.
Custodio o propietario interno: Área o persona responsable de la gestión operativa, calidad, actualización, acceso y seguridad de una base de datos.
Dato personal: Información vinculada o que pueda asociarse a una persona natural determinada o determinable.
Dato público: Dato que no es semiprivado, privado o sensible y que puede estar contenido en registros o documentos públicos.
Dato semiprivado: Dato que no tiene naturaleza íntima, reservada ni pública y cuyo conocimiento puede interesar al Titular y a determinado sector o grupo.
Dato privado: Dato que por su naturaleza íntima o reservada solo es relevante para el Titular.
Dato sensible: Dato que afecta la intimidad del Titular o cuyo uso indebido puede generar discriminación.
Decisión individual automatizada: Decisión basada exclusivamente en Tratamiento automatizado que produzca efectos jurídicos o afecte significativamente al Titular.
Encargado: Persona natural o jurídica que trata datos por cuenta y siguiendo instrucciones del Responsable.

Exportador de datos: Responsable o Encargado ubicado en Colombia que envía o permite el acceso a datos hacia otro país.
Fuentes de acceso público: Bases o fuentes cuya consulta puede realizar cualquier persona, sin que ello convierta todos los datos contenidos en datos públicos.
Importador de datos: Receptor ubicado en el exterior que recibe o accede a datos personales.
Incidente de seguridad: Evento confirmado o sospechoso que afecta o puede afectar la confidencialidad, integridad, disponibilidad, autenticidad o reserva de datos.
Medidas de seguridad: Controles humanos, administrativos, físicos, jurídicos, técnicos y organizacionales destinados a proteger los datos.
Procedimiento de disociación: Tratamiento destinado a impedir que la información se asocie con una persona identificada o identificable.
Receptor: Persona que recibe, consulta o accede a datos personales.
Responsable: Persona que decide sobre la base de datos o determina las finalidades y medios esenciales del Tratamiento.
Seudonimización: Sustitución de identificadores directos por códigos separados, sin eliminar totalmente la posibilidad de reidentificación.
Subencargado: Tercero vinculado por un Encargado para ejecutar parte del Tratamiento por cuenta del Responsable.
Tercero beneficiario: Titular que puede ejercer los derechos reconocidos a su favor en cláusulas contractuales, aunque no haya firmado el contrato.
Titular: Persona natural cuyos datos personales son objeto de Tratamiento.
Transferencia internacional: Envío o acceso desde Colombia hacia un receptor exterior que actúa como Responsable.
Transmisión internacional: Tratamiento realizado por un Encargado exterior por cuenta de un Responsable ubicado en Colombia.
Transferencia o transmisión ulterior: Flujo posterior efectuado por el receptor inicial a otro tercero, Subencargado o país.
Tratamiento: Cualquier operación sobre datos, como recolección, registro, almacenamiento, consulta, uso, circulación, actualización, análisis, transferencia, transmisión, bloqueo, supresión o eliminación.
Violación de seguridad: Incidente que compromete efectivamente datos personales y genera o puede generar riesgos para su administración o para los derechos de los Titulares.

6. PRINCIPIOS RECTORES

Legalidad: El Tratamiento se realizará conforme a la Constitución, la ley y las instrucciones de la SIC.
Finalidad: Los datos serán recolectados para propósitos legítimos, específicos, informados y compatibles.
Libertad: Salvo excepción legal, se requerirá autorización previa, expresa e informada.
Veracidad o calidad: La información será completa, exacta, actualizada, comprobable y comprensible.
Transparencia: El Titular podrá conocer la existencia, fuente, finalidad y uso de sus datos.
Acceso y circulación restringida: Solo accederán personas autorizadas y para fines permitidos.
Seguridad: Se aplicarán controles proporcionales a la naturaleza, volumen, contexto y riesgo.
Confidencialidad: El deber de reserva subsiste incluso después de terminada la relación con la Compañía.
Necesidad y minimización: Solo se recolectarán datos adecuados, pertinentes y estrictamente necesarios.
Temporalidad: Los datos no se conservarán por más tiempo del necesario, salvo deber legal o contractual.
Responsabilidad demostrada: La Compañía documentará sus medidas y podrá acreditar su efectividad.
Privacidad desde el diseño y por defecto: Los proyectos y sistemas incorporarán controles de privacidad desde su concepción y limitarán por defecto el acceso y la recolección.
Proporcionalidad: La intensidad del Tratamiento y de las medidas de seguridad guardará relación con el riesgo para los Titulares.

7. CATEGORÍAS DE DATOS PERSONALES OBJETO DE TRATAMIENTO

Las bases podrán contener las categorías descritas a continuación de acuerdo con la finalidad aplicable. Su inclusión no significa que todas las bases contengan todos los datos ni autoriza su recolección indiscriminada.

7.1. Datos generales

- Datos de personas mayores de edad.
- Datos de menores de edad únicamente cuando sean necesarios y se cumplan las garantías reforzadas.

7.2. Datos de identificación

- Nombres, apellidos, documento, fecha y lugar de expedición, estado civil, fecha y lugar de nacimiento, nacionalidad, edad y sexo cuando resulte necesario.
- Firma manuscrita o electrónica; datos de familiares, beneficiarios, representantes, apoderados o terceros relacionados.
- Fotografías, videos, voz y datos biométricos cuando exista necesidad, autorización y fundamento jurídico.

7.3. Datos de ubicación

- Direcciones comerciales, laborales o residenciales; teléfonos; correos; ciudad, departamento y país.

7.4. Datos sensibles

- Salud, diagnósticos, tratamientos, biométricos, afiliación sindical, convicciones religiosas o políticas, origen racial o étnico, orientación o identidad sexual, discapacidad y condiciones de vulnerabilidad.

7.5. Datos socioeconómicos

- Información financiera, crediticia, tributaria, patrimonial, ingresos, egresos, activos, pasivos, inversiones y actividad económica.
- Historia laboral, cargo, fechas de ingreso y retiro, experiencia, formación académica y afiliaciones al Sistema Integral de Seguridad Social.

7.6. Datos tecnológicos y de seguridad

- Usuarios, direcciones IP, perfiles, registros de acceso, eventos de seguridad, identificadores de dispositivos y datos de autenticación. Las contraseñas no se incorporarán en documentos generales y deberán almacenarse con medidas de protección adecuadas.

7.7. Datos de cumplimiento

- Resultados de debida diligencia, consultas en listas, antecedentes judiciales, fiscales, disciplinarios o administrativos, alertas y soportes de análisis, dentro de los límites legales.

7.8. Datos de navegación y cookies

- Identificadores, preferencias, páginas consultadas, duración de sesión, dispositivo y demás datos obtenidos mediante cookies o tecnologías similares, cuando el sitio web las utilice.

Toda la información será tratada bajo reserva y con acceso limitado. Los datos sensibles, biométricos, de menores, financieros, laborales, societarios y de cumplimiento tendrán controles reforzados.

8. BASES DE DATOS Y REGLAS ESPECÍFICAS DE GESTIÓN

La Compañía mantendrá un inventario central que permita conocer la base, su finalidad, forma de Tratamiento, ubicación, custodio, encargados, los cuales se encuentran en herramienta tecnologica usada por la empresa. Como mínimo se reconocen las siguientes bases:

8.1. Empleados

Elemento	Descripción
Titulares	Empleados, exempleados, aprendices, practicantes, beneficiarios, familiares y contactos de emergencia.
Finalidades	Selección, contratación, nómina, prestaciones, seguridad social, seguridad y salud en el trabajo, bienestar, formación, disciplina, certificaciones, acceso físico y lógico, emergencias y cumplimiento legal.
Categorías de datos	Identificación, contacto, laborales, académicos, financieros, salud, seguridad social, beneficiarios, accesos y cumplimiento.

Forma de Tratamiento	Mixta. Historias laborales físicas y repositorios corporativos autorizados.
Área responsable	Recursos Humanos
Conservación	Durante la relación y por los términos laborales, tributarios, contables y de archivo.
Controles específicos	Acceso restringido; acuerdos de confidencialidad; no compartir por redes sociales; no fotografiar expedientes sin autorización; verificaciones por canales formales; eliminación segura de documentos no requeridos; no reutilizar hojas de vida para fines distintos.

8.2. Clientes

Elemento	Descripción
Titulares	Clientes, potenciales clientes, representantes y contactos.
Finalidades	Gestión precontractual, contratación, facturación, servicio, comunicaciones, calidad, cobro, cumplimiento, seguridad y administración de riesgos. El mercadeo se realizará cuando exista autorización o fundamento legal.
Categorías de datos	Identificación, contacto, contractuales, financieros, tributarios, debida diligencia y comunicaciones.
Forma de Tratamiento	Automatizada o mixta.
Área responsable	Área comercial y Contabilidad
Conservación	Durante la relación y por los términos legales y contractuales.
Controles específicos	Reserva de comunicaciones; consulta de listas por áreas autorizadas; transmisión a aliados o proveedores únicamente bajo contrato; control de acceso y trazabilidad.

8.3. Proveedores

Elemento	Descripción
Titulares	Proveedores, contratistas, representantes, beneficiarios finales, empleados y contactos.
Finalidades	Selección, evaluación, vinculación, contratación, pagos, impuestos, calidad, seguridad, cumplimiento, prevención de riesgos y administración de la relación.
Categorías de datos	Identificación, contacto, financieros, tributarios, contractuales, antecedentes y debida diligencia.
Forma de Tratamiento	Automatizada o mixta.
Área responsable	Compras o Administrativa, área contratante, Contabilidad
Conservación	Durante la relación y términos legales y contractuales.
Controles específicos	Consultas en listas por personal autorizado; cláusulas de privacidad; verificación de Encargados y Subencargados; devolución o eliminación al terminar.

8.4. Accionistas

Elemento	Descripción
Titulares	Accionistas actuales y anteriores, beneficiarios, herederos, apoderados, representantes y contactos.
Finalidades	Administrar el libro de registro, títulos, asambleas, comunicaciones, dividendos, sucesiones, derechos políticos y económicos, obligaciones tributarias, contables, comerciales y de cumplimiento.
Categorías de datos	Identificación, contacto, societarios, patrimoniales, bancarios, tributarios, sucesorales y cumplimiento.
Forma de Tratamiento	Mixta: libro de registro, archivos societarios y repositorios autorizados.
Área responsable	Secretaría General y Área Jurídica
Conservación	Durante la existencia de la sociedad y los términos societarios, contables y tributarios.
Controles específicos	Reserva de pagos y participaciones; acceso limitado; entrega a autoridades y depositarios solo con fundamento; actualización de accionistas y sucesores.

9. FINALIDADES GENERALES Y ESPECÍFICAS DEL TRATAMIENTO

- Ejecutar las actividades propias del objeto social y las relaciones contractuales, societarias, laborales, comerciales y administrativas.
- Ofrecer productos, servicios o beneficios por medios físicos o electrónicos, cuando exista autorización o fundamento legal.
- Enviar información a entidades públicas o privadas cuando exista solicitud legítima, obligación legal o autorización.
- Consultar fuentes públicas y listas de control para debida diligencia, prevención del fraude, LA/FT/FPADM, corrupción y otros riesgos, dentro de los límites aplicables.
- Soportar auditorías internas y externas, revisiones de control, investigaciones y procesos judiciales o extrajudiciales.
- Verificar referencias laborales, comerciales, societarias y contractuales.
- Gestionar cuentas, pagos, dividendos, facturas, obligaciones tributarias y contables.
- Administrar seguridad física y lógica, accesos, herramientas corporativas, continuidad y soporte.
- Generar reportes estadísticos y de gestión procurando anonimizar cuando no sea necesaria la identificación.
- Transmitir datos a Encargados y transferirlos a Responsables cuando exista fundamento y se adopten salvaguardas.
- Conservar evidencia de las actividades y atender solicitudes de Titulares y autoridades.

La Compañía no venderá, licenciará, divulgará ni utilizará datos para finalidades incompatibles. Cualquier uso nuevo sustancial será informado y, cuando corresponda, requerirá una nueva autorización.
Los datos podrán ser conocidos por el personal autorizado y por órganos como la Asamblea General de Accionistas, Junta Directiva, Revisoría Fiscal, Representante Legal, gerencias y áreas jurídica, cumplimiento, contable, financiera, tecnológica y de control, únicamente en la medida necesaria para sus funciones.

10. AUTORIZACIÓN, EXCEPCIONES Y PRUEBA DEL CONSENTIMIENTO

10.1. Regla general

Salvo excepción legal, la Compañía obtendrá autorización previa, expresa e informada y conservará prueba del mecanismo utilizado, la fecha, las finalidades y la versión del aviso o Política suministrada, mediante acuerdo contractual, NDA, o autorización del tratamiento incorporado en Formulario de Conocimiento de Contrapartes.

10.2. Formas de autorización

- Documento físico o electrónico.
- Grabación de voz o aceptación mediante mecanismo electrónico.
- Conducta inequívoca que permita concluir razonablemente que el Titular autorizó el Tratamiento. El silencio no será considerado autorización.
- Formulario de conocimiento de contrapartes, contrato, portal, formato laboral o registro de evento, siempre que la cláusula sea clara y verificable.

10.3. Casos en los que no se requiere autorización

- Información requerida por entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

La ausencia de autorización no exime del cumplimiento de los demás principios y deberes.

10.4. Autorización de contrapartes

La autorización incluida en el formulario de conocimiento deberá identificar al Responsable, finalidades, incluir debida diligencia, consultas en listas y fuentes, gestión contractual y cumplimiento, informar los derechos y canales, y mencionar las transmisiones, transferencias y Subencargados cuando puedan ocurrir.

Cuando la contraparte suministre datos de representantes, socios, accionistas, beneficiarios finales, empleados, apoderados o contactos, declarará que cuenta con legitimación para entregarlos o que informará a los Titulares. Esta declaración no traslada ni elimina las obligaciones de la Compañía.

10.5. Datos obtenidos de fuentes públicas

La consulta de una fuente accesible al público no habilita el uso indiscriminado de toda la información. La Compañía verificará que el dato sea público, pertinente y necesario, y documentará la finalidad y la fuente.

10.6. Revocatoria y supresión

El Titular podrá solicitar revocatoria o supresión cuando proceda. La solicitud podrá negarse total o parcialmente cuando exista deber legal o contractual de conservar la información, caso en el cual se limitará el Tratamiento a dichas finalidades.

11. TRATAMIENTO DE DATOS SENSIBLES

Por regla general, el Tratamiento de datos sensibles está prohibido. Solo se realizará cuando exista autorización explícita del Titular o una excepción del artículo 6 de la Ley 1581 de 2012 y siempre bajo controles reforzados.

- Informar que no está obligado a autorizar el Tratamiento.
- Identificar cuáles datos son sensibles y explicar de manera separada su finalidad.
- Limitar el acceso al personal estrictamente necesario.
- Aplicar acuerdos de confidencialidad reforzados, cifrado, segregación, trazabilidad y, cuando proceda, anonimización o seudonimización.
- No condicionar una actividad a la entrega de datos sensibles, salvo que sean indispensables o exista obligación legal.
- Realizar una evaluación de necesidad y riesgo antes de recolectar biométricos, salud u otras categorías especiales.

12. TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

La Compañía evitará tratar datos de menores salvo que resulte necesario, lícito y proporcional. Cuando proceda, el Tratamiento deberá responder al interés superior del menor, respetar sus derechos fundamentales y garantizar su derecho a ser escuchado de acuerdo con su madurez y autonomía.

- Obtener autorización previa, expresa e informada del representante legal, salvo excepción legal.
- Informar de forma comprensible las finalidades y riesgos.
- Recolectar únicamente los datos necesarios.
- Aplicar controles reforzados y evitar publicidad o perfilamiento que pueda afectar al menor.
- Documentar la evaluación de interés superior y el mecanismo utilizado para escuchar al menor.

13. AVISOS DE PRIVACIDAD Y POLÍTICA DE COOKIES

13.1. Emisión y actualización de avisos de privacidad

La Compañía emitirá avisos adaptados a los diferentes canales y grupos de Titulares: contrapartes, clientes, proveedores, empleados, aspirantes, accionistas, visitantes, videovigilancia, sitio web, eventos y plataformas.
La Compañía emitirá avisos adaptados a los diferentes canales y grupos de Titulares: contrapartes, clientes, proveedores, empleados, aspirantes, accionistas, visitantes, videovigilancia, sitio web, eventos y plataformas.
Identidad y contacto del Responsable.
Finalidades principales.
Derechos del Titular y canales para ejercerlos.
Carácter facultativo de las respuestas sobre datos sensibles o de menores.
Forma de acceder a la Política completa.
Referencia a transferencias o transmisiones, cuando corresponda.
Vigencia o criterios de conservación.

Avisos y tratamiento de datos mediante videovigilancia: La Compañía utilizará sistemas de videovigilancia exclusivamente para la protección de las personas, bienes, instalaciones y activos de información, así como para la prevención, detección e investigación de incidentes de seguridad.
Cuando aplique, en nuestras instalaciones físicas, las zonas monitoreadas contarán con avisos de privacidad visibles, ubicados en los accesos o lugares de fácil consulta, que incluyan un pictograma de cámara, la finalidad del tratamiento y el medio para acceder a esta Política.
Las grabaciones serán conservadas durante el tiempo estrictamente necesario para cumplir las finalidades descritas y, en todo caso, por un término máximo de **treinta (30) días calendario**, salvo que deban preservarse por la ocurrencia de un incidente, una investigación interna, una reclamación, un requerimiento de autoridad competente o una obligación legal.
El acceso a las grabaciones estará restringido al personal autorizado por la Compañía. Cuando un tercero administre, opere o tenga acceso al sistema, deberá actuar bajo instrucciones de la Compañía, guardar confidencialidad y aplicar medidas de seguridad que impidan el acceso, uso, divulgación o entrega no autorizada de las grabaciones.
La entrega o consulta de grabaciones por terceros solo procederá cuando exista autorización del Titular, requerimiento de autoridad competente, obligación legal o cuando sea necesaria para atender un incidente o una investigación legítima de la Compañía.

13.2. Política de Cookies

Las cookies y tecnologías similares pueden almacenar identificadores, preferencias, datos de navegación o información del dispositivo y, cuando permitan identificar o asociar a una persona, constituyen Tratamiento de datos personales.

13.2.1. Tipos de cookies

- Esenciales o técnicas: necesarias para el funcionamiento y seguridad del sitio.
- Funcionales: recuerdan preferencias y personalizan la navegación.
- Analíticas o de rendimiento: permiten medir visitas, interacción y desempeño.
- Publicidad o marketing: personalizan anuncios o campañas.
- De terceros: instaladas o gestionadas por proveedores externos.

13.2.2. Consentimiento y gestión

El sitio web deberá mostrar un banner que permita aceptar, rechazar o configurar las cookies no esenciales. El consentimiento podrá retirarse posteriormente. El bloqueo de ciertas cookies puede afectar algunas funciones, lo cual deberá informarse.

13.2.3. Terceros, transferencias y conservación

Antes de utilizar cookies de terceros se verificará su rol, país, finalidades, periodo de conservación y mecanismos internacionales. La información se conservará solo por el tiempo necesario y luego será eliminada o anonimizada.

14. DERECHOS DE LOS TITULARES

- Conocer, actualizar y rectificar sus datos.
- Solicitar prueba de la autorización, salvo excepción legal.
- Ser informado sobre el uso dado a sus datos y sobre receptores o Encargados relevantes.
- Acceder gratuitamente a sus datos en los términos legales.
- Revocar la autorización y solicitar supresión cuando proceda.
- Presentar consultas, reclamos, quejas ante la Compañía y la SIC.
- Oponerse a tratamientos incompatibles o contrarios a la ley.
- Ejercer los derechos reconocidos en contratos como tercero beneficiario.
- Solicitar información sobre decisiones automatizadas y la intervención humana cuando resulten aplicables.

Los derechos podrán ser ejercidos por el Titular, sus causahabientes, representante o apoderado debidamente acreditado, o por la persona a favor de quien se haya estipulado.

15. PROCEDIMIENTOS PARA CONSULTAS, RECLAMOS, REVOCATORIA Y SUPRESIÓN

15.1. Verificación de identidad

Antes de entregar información o ejecutar una modificación, la Compañía verificará razonablemente la identidad y legitimación del solicitante. No se exigirán requisitos desproporcionados.

15.2. Consultas

Las consultas serán atendidas dentro de diez (10) días hábiles contados desde su recibo. Si no es posible, se informarán los motivos y la fecha de respuesta, que no podrá superar cinco (5) días hábiles adicionales.
La consulta será gratuita al menos una vez por mes calendario y cada vez que existan modificaciones sustanciales que motiven nuevas consultas. Los costos adicionales solo podrán corresponder a reproducción, envío o certificación, en los casos permitidos.

15.3. Reclamos

El reclamo deberá identificar al Titular, describir los hechos, indicar una dirección o canal de respuesta y anexar los documentos pertinentes. Si está incompleto, se requerirá subsanación dentro de cinco (5) días hábiles. Si transcurren dos (2) meses sin respuesta, se entenderá desistido.
Si quien recibe el reclamo no es competente, lo trasladará dentro de dos (2) días hábiles. Recibido el reclamo completo, se incluirá la leyenda "reclamo en trámite" dentro de dos (2) días hábiles y se mantendrá hasta la decisión.
El reclamo será resuelto dentro de quince (15) días hábiles, prorrogables por ocho (8) días hábiles adicionales, previa información al Titular.

15.4. Agotamiento del trámite interno

Antes de acudir a la SIC por una reclamación individual, el Titular deberá agotar el trámite de consulta o reclamo ante la Compañía cuando así lo exija la ley.

15.5. Canales habilitados

- Correo: notificacionesjudiciales@valoresind.com.
- Dirección física: Calle 5A No. 39-131, torre 4, piso 3, Centro de Trabajo Corfin, Medellín.
- Teléfono: (+57 604) 448 60 67.

El Área de cumplimiento documentará las solicitudes y respuestas, y las áreas internas deberán suministrar la información requerida dentro de tres (3) días hábiles o en el plazo interno que se establezca según la complejidad.

16. DEBERES DE RESPONSABLES, ENCARGADOS Y SUBENCARGADOS

16.1. Deberes de la Compañía como Responsable

- Garantizar el pleno ejercicio de habeas data.
- Solicitar, conservar y demostrar la autorización cuando sea necesaria.
- Informar finalidades, derechos y flujos relevantes.
- Conservar la información bajo condiciones de seguridad.
- Suministrar a Encargados información veraz, completa, actualizada y autorizada.
- Actualizar, rectificar y comunicar novedades a los Encargados.
- Exigir a Encargados y Subencargados seguridad, privacidad y confidencialidad.
- Tramitar consultas y reclamos y registrar las leyendas legales.
- Informar al Encargado cuando una información se encuentre en discusión.
- Informar al Titular sobre el uso dado a sus datos.
- Reportar incidentes y cumplir instrucciones de la SIC.
- Adoptar procedimientos de respaldo, recuperación, auditoría e inventario.

16.2. Deberes de Encargados y Subencargados

- Tratar datos exclusivamente por instrucciones documentadas.
- Garantizar seguridad, confidencialidad y acceso restringido.
- Mantener actualizada la información comunicada por el Responsable dentro del plazo acordado.
- Asistir en consultas, reclamos, auditorías e incidentes.
- Registrar "reclamo en trámite" e "información en discusión judicial" cuando sea instruido.
- Abstenerse de circular datos controvertidos cuyo bloqueo haya sido ordenado.
- No vincular Subencargados sin autorización.
- Devolver, eliminar o anonimizar la información y sus copias al terminar.
- Cooperar con la SIC y conservar evidencia de cumplimiento.

16.3. Deberes de propietarios y custodios internos

- Mantener el inventario y reportar novedades al Área de Cumplimiento
- Definir perfiles de acceso y revisar periódicamente los usuarios autorizados.
- Garantizar exactitud, actualización, conservación y eliminación.
- Reportar inmediatamente incidentes, reclamos y cambios de finalidad, datos, Encargados o ubicación.
- No crear bases paralelas o copias no autorizadas.

17. PROHIBICIONES Y REGLAS INTERNAS DE USO

- Acceder, usar, compartir, almacenar o tratar datos sin necesidad funcional, autorización interna o fundamento jurídico.
- Tratar datos sensibles sin autorización expresa o excepción legal.
- Compartir información por redes sociales, correos personales, mensajería no autorizada, dispositivos personales o nubes no aprobadas.
- Tomar fotografías o copias de historias laborales, libros societarios, expedientes o soportes reservados sin autorización.
- Reutilizar hojas de vida o datos para finalidades diferentes de las informadas.
- Ceder, comunicar o circular datos sin autorización o sin contrato y registro interno.
- Usar datos para discriminación, acoso, perfilamiento ilegítimo o decisiones contrarias a los derechos fundamentales.
- Cargar datos personales, sensibles, confidenciales o reservados en herramientas de inteligencia artificial generativa no autorizadas por la Compañía.
- Desactivar, eludir o alterar controles de seguridad.
- Realizar conductas que puedan configurar delitos informáticos o violaciones de confidencialidad.

El incumplimiento podrá constituir falta laboral, incumplimiento contractual o causa de terminación, sin perjuicio de las acciones legales y de repetición por perjuicios, multas o sanciones atribuibles a la conducta del infractor.

18. FORMA DE TRATAMIENTO, ALMACENAMIENTO Y UBICACIÓN

Cada base será clasificada como manual/física, automatizada o mixta. El inventario central deberá contener, como mínimo:

- Nombre y estado de la base: activa, inactiva o suprimida.
- Fecha de creación o vinculación.
- Área responsable, custodio y usuarios autorizados.
- Titulares, finalidad y categorías de datos.
- Ubicación física y lógica, sistema, plataforma y país de alojamiento.
- Encargados, Subencargados y contratos.
- Medidas de seguridad, copias de respaldo y recuperación.
- Periodo y fundamento de conservación.
- Transferencias y transmisiones.

- Procedimiento y evidencia de archivo, bloqueo, devolución o eliminación.

La información podrá almacenarse en repositorios corporativos autorizados, incluidos Microsoft 365 y OneDrive cuando resulte aplicable. El uso de estos servicios deberá ser evaluado como posible transmisión internacional o acceso transfronterizo y deberá contar con configuración, perfiles y contratos adecuados.

19. POLÍTICA DE CONTRATACIÓN CON CONTRAPARTES

Antes de permitir acceso, el área contratante, Cumplimiento y Tecnología verificarán el rol, necesidad, idoneidad, seguridad, y ubicación del tercero.

- Objeto, duración, naturaleza, finalidad, datos y Titulares.
- Instrucciones documentadas y deber de confidencialidad.
- Medidas administrativas, físicas y técnicas.
- Ubicación de servidores, accesos remotos y notificación de cambios.
- Subencargados y flujos ulteriores.
- Atención de derechos y cooperación con la SIC.
- Notificación, gestión y documentación de incidentes.
- Auditoría, evidencias y planes de mejora.
- Retención, devolución, eliminación y certificación.
- Continuidad, respaldo y recuperación.
- Responsabilidad, indemnidad y consecuencias por incumplimiento.
- Terceros beneficiarios cuando se utilicen las cláusulas modelo.

En formularios y contratos se incluirán cláusulas de autorización o información que describan de manera concreta las finalidades y los terceros que requieren acceso. No se utilizarán autorizaciones abiertas o indeterminadas.

20. TRANSFERENCIAS Y TRANSMISIONES NACIONALES E INTERNACIONALES

20.1. Diferenciación de roles

Existe transferencia cuando el receptor actúa como Responsable y transmisión cuando trata por cuenta e instrucciones de la Compañía. La denominación comercial del contrato no sustituye el análisis jurídico.

20.2. Evaluación previa

1. El área solicitante informa el flujo antes de contratar o habilitar acceso.
2. Cumplimiento clasifica la operación y verifica autorización, excepción o mecanismo aplicable.
3. Tecnología identifica países, centros de datos, respaldos, accesos y Subencargados.
4. Se describen Titulares, datos, finalidades, duración, frecuencia y riesgos.
5. Se verifica el nivel adecuado del país o las excepciones del artículo 26 de la Ley 1581.
6. Cuando corresponda, se tramita declaración de conformidad ante la SIC.
7. Se aprueba el flujo por Cumplimiento.
8. Se archiva con evidencia.

20.3. Excepciones a la prohibición de transferencia a países no adecuados

- Autorización expresa e inequívoca del Titular.
- Intercambio de datos médicos necesario por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles conforme a la legislación aplicable.
- Transferencias acordadas en tratados internacionales.
- Transferencias necesarias para ejecutar un contrato entre el Titular y el Responsable o para medidas precontractuales solicitadas por el Titular.

- Transferencias legalmente exigidas para salvaguardar interés público o para reconocimiento, ejercicio o defensa de un derecho judicial.

La aplicación de una excepción deberá documentarse. Las cláusulas contractuales modelo son facultativas y complementarias; no eliminan la verificación del artículo 26 ni levantan por sí solas la prohibición.

20.4. Cláusulas contractuales modelo

La Compañía podrá utilizar o adaptar los modelos Responsable-Responsable y Responsable-Encargado de la Circular Externa No. 003 de 2025. Cualquier modificación deberá mantener o aumentar las garantías colombianas.

20.5. Subencargados y flujos ulteriores

- Autorización previa, específica o general bajo condiciones definidas.
- Información sobre identidad, país, servicio y funciones del Subencargado.
- Obligaciones equivalentes y responsabilidad del Encargado principal.
- Derecho de objeción razonada de la Compañía.
- Prohibición de flujos ulteriores sin fundamento, contrato equivalente y registro.

20.6. Terceros beneficiarios

“Las Partes reconocen que los titulares de los datos personales son terceros beneficiarios del presente contrato y podrán ejercer directamente los derechos que de este se deriven, sin perjuicio de las competencias de la Superintendencia de Industria y Comercio”.

21. MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN

Las medidas se seleccionarán con base en el riesgo para los Titulares, la naturaleza de los datos, el estado de la técnica, el contexto y las consecuencias de una vulneración. Podrán clasificarse internamente como básicas, medias o reforzadas.

- Contraseñas robustas, autenticación multifactor y gestión segura de restablecimientos.
- Perfiles por rol, mínimo privilegio y revisión periódica de accesos.
- Cifrado de dispositivos, comunicaciones, archivos y respaldos cuando sea pertinente.
- Registro de actividades, trazabilidad y monitoreo de eventos.
- Antivirus, protección de correo, firewall, filtrado web y actualización de sistemas.
- Copias de seguridad, redundancia, recuperación y pruebas de restauración.
- Bloqueo de sesión, protección física de equipos y archivo restringido.
- Acuerdos de confidencialidad, cláusulas contractuales y capacitación.
- Procedimientos de alta, modificación y retiro de usuarios.
- Gestión de vulnerabilidades, parches y evaluación de proveedores.
- Advertencia de confidencialidad en correos corporativos.
- Eliminación segura de soportes, documentos y equipos.
- Controles específicos para trabajo remoto, dispositivos móviles y acceso de terceros.

Los controles concretos de Microsoft 365, OneDrive, firewall, antivirus y demás herramientas serán verificados y documentados por Tecnología; su mención en este Manual no sustituye la evidencia técnica ni la actualización de configuraciones.

22. GESTIÓN DE INCIDENTES DE SEGURIDAD

22.1. Alcance

Se considera incidente cualquier evento confirmado o sospechoso relacionado con acceso no autorizado, pérdida, robo, alteración, destrucción, divulgación, envío equivocado, malware, phishing, troyanos, credenciales comprometidas, fallas de proveedores o exposición accidental.

22.2. Reporte interno

Todo colaborador, proveedor o tercero que identifique, conozca o sospeche de un incidente de seguridad de la información deberá reportarlo de manera inmediata al correo electrónico admin@valoresind.com.

El reporte deberá incluir, en lo posible, la fecha y hora de identificación, la descripción de la novedad, los sistemas, equipos o información posiblemente afectados y los soportes disponibles.

El área de Tecnología de la Información será responsable de registrar, clasificar, investigar y gestionar cada incidente, así como de documentar las acciones de contención, corrección y cierre. De manera mensual, remitirá un informe consolidado al área de Cumplimiento, con las novedades identificadas, su estado y las acciones implementadas.

Cuando el incidente comprometa o pueda comprometer datos personales (incluyendo pérdida, robo, acceso no autorizado, alteración o divulgación de información), el área de TI deberá informarlo de forma inmediata al area de cumplimiento, con el fin de evaluar las medidas adicionales y, de ser procedente, el reporte ante la Superintendencia de Industria y Comercio.

22.3. Roles

Rol	Responsabilidad
Reportante	Informar, preservar evidencias y no alterar el evento.
Tecnología	Contener, investigar, erradicar, recuperar y documentar.
Cumplimiento	Evaluar obligaciones, derechos, autoridades y comunicaciones.
Propietario de la base	Identificar datos, Titulares, procesos y consecuencias.
Proveedor/Encargado	Notificar, colaborar y aportar actualizaciones.
Representante Legal o instancia competente	Adoptar decisiones estratégicas y aprobar comunicaciones críticas.

22.4. Clasificación

Nivel	Criterios	Gestión
Alto	Exposición masiva o de datos sensibles/biométricos; fraude; alto número de Titulares; acceso persistente; interrupción crítica; riesgo grave para derechos.	Escalamiento inmediato a Tecnología, Cumplimiento y alta dirección; evaluación prioritaria de reporte y comunicación.
Medio	Afectación relevante pero limitada, acceso contenido, sistema secundario o incidente de proveedor delimitado.	Análisis conjunto, seguimiento y decisión documentada.
Bajo	Amenaza bloqueada, archivo neutralizado o evento sin compromiso confirmado de datos.	Registro, análisis de tendencias y fortalecimiento de controles.

La clasificación interna no elimina la obligación legal de reportar cuando exista violación de códigos de seguridad y riesgo en la administración de la información.

22.5. Plazos contractuales y regulatorios

- En un acuerdo internacional basado en las cláusulas modelo, las Partes podrán pactar notificación a la otra Parte, autoridad y Titulares sin dilación y en máximo cinco (5) días, según el modelo aplicable.
- En el modelo Responsable-Encargado, el Importador/Encargado deberá notificar al Exportador/Responsable dentro de setenta y dos (72) horas desde el conocimiento, sin perjuicio de plazos más estrictos.
- El reporte colombiano ante la SIC se efectuará dentro de quince (15) días hábiles desde que el incidente sea detectado y puesto en conocimiento de la persona o área encargada.
- Los plazos contractuales más breves no sustituyen ni amplían el plazo legal colombiano.

22.6. Contenido del registro

- ID, fechas de detección, conocimiento, contención y cierre.
- Reportante, sociedad, base, sistemas, datos y Titulares afectados.
- Naturaleza, causa, vulnerabilidades, responsable y consecuencias.
- Número aproximado de Titulares y registros.
- Medidas inmediatas, correctivas y preventivas.
- Clasificación, riesgo, decisión de reporte y comunicación.
- Evidencias, radicados, cierre y lecciones aprendidas.

23. REPORTES, NOVEDADES Y OBLIGACIONES ANTE LA SIC

El Área de Cumplimiento administrará los reportes regulatorios con apoyo de Tecnología y de los propietarios de las bases. Antes de cada reporte verificará la versión vigente de la Circular Única.

Obligación	Plazo o frecuencia	Responsables
Inscripción de nuevas bases	Dentro del plazo vigente aplicable y antes de exceder el término legal.	Cumplimiento y propietario.
Actualización anual RNBD	Entre el 2 de enero y el 31 de marzo, para sujetos obligados.	Cumplimiento y propietarios.
Cambios sustanciales	Dentro de los primeros diez (10) días hábiles del mes siguiente o del mes en que se produzcan, conforme a la instrucción vigente.	Cumplimiento, Tecnología y propietario.
Reclamos de Titulares	Primer semestre (20 de febrero) – Segundo semestre (25 de agosto)	Cumplimiento.
Incidentes de seguridad	Dentro de quince (15) días hábiles desde la detección y conocimiento del área competente.	Cumplimiento y Tecnología.
Transferencias/transmisiones	Actualizar cuando cambien países, Encargados, finalidades, datos o medidas.	Cumplimiento y Tecnología.
Cierre o supresión	Actualizar el RNBD y conservar evidencia.	Cumplimiento y propietario.
Requerimientos de la SIC	Dentro del plazo fijado por la autoridad.	Cumplimiento y áreas involucradas.

Son cambios sustanciales, entre otros, los relacionados con finalidad, Encargados, canales de atención, tipos de datos, medidas de seguridad, Política y transferencias o transmisiones internacionales.

24. ENTREGA DE DATOS A AUTORIDADES Y TERCEROS LEGITIMADOS

Ante una solicitud de autoridad, la Compañía verificará competencia, fundamento, finalidad, pertinencia, proporcionalidad y alcance. La entrega será documentada y se advertirá el deber de reserva y seguridad al receptor.

- Verificar identidad, cargo y entidad solicitante.
- Conservar la orden, requerimiento o soporte jurídico.
- Entregar únicamente la información necesaria.
- Usar un canal seguro y registrar fecha, medio, receptor y documentos.
- Aplicar controles de integridad y autenticidad.
- Informar al Titular cuando sea jurídicamente posible y no exista reserva.

Las solicitudes de terceros particulares solo serán atendidas con autorización, legitimación, contrato o mandato legal suficiente.

25. CONSERVACIÓN, ARCHIVO, BLOQUEO Y ELIMINACIÓN SEGURA

Los datos se conservarán durante la vigencia de la finalidad y por los términos legales, contractuales, contables, tributarios, laborales, societarios o de defensa jurídica. Cada propietario definirá una tabla de retención con apoyo de Cumplimiento y Archivo.

- Cuando finalice la finalidad y no exista deber de conservación, los datos serán eliminados, devueltos o anonimizados.
- Durante un reclamo, investigación, litigio o deber de conservación, podrán bloquearse y limitarse a dichas finalidades.
- La eliminación comprenderá copias activas, soportes y respaldos en la medida técnica y legalmente posible.
- Los terceros deberán certificar devolución o eliminación.
- La destrucción física será segura y la eliminación lógica impedirá una recuperación razonable.

26. DIVULGACIÓN, CAPACITACIÓN, AUDITORÍA Y MEJORA CONTINUA

- Inducción a empleados y contratistas con acceso a datos.
- Capacitación periódica sobre autorización, incidentes, phishing, confidencialidad y herramientas autorizadas.
- Divulgación de cambios relevantes del Manual.
- Auditoría periódica de bases, permisos, contratos, RNBD, incidentes y proveedores.
- Pruebas de recuperación y simulacros de incidentes.
- Planes de acción con responsables y fechas.
- Revisión anual de la Política y cuando exista cambio normativo o tecnológico.

27. TRATAMIENTO DE DATOS PERSONALES REGULADOS POR LA LEY 1266 DE 2008 (HABEAS DATA FINANCIERO)

Sin perjuicio de las disposiciones contenidas en la Ley 1581 de 2012 y sus normas reglamentarias, cuando el tratamiento de datos personales corresponda a información financiera, crediticia, comercial, de servicios o aquella proveniente de terceros países de la misma naturaleza, será aplicable el régimen especial previsto en la **Ley 1266 de 2008**, modificada por la **Ley 2157 de 2021**, así como las demás normas que la adicionen, modifiquen o sustituyan.

En consecuencia, cuando la sociedad, en desarrollo de su objeto social o de sus relaciones comerciales, laborales o contractuales, actúe como fuente, operador o usuario de información financiera, o realice consultas, reportes, actualización, circulación o tratamiento de información ante operadores de bancos de datos o centrales de información crediticia legalmente constituidos, dicho tratamiento se sujetará a las disposiciones especiales establecidas en la Ley 1266 de 2008 y a los principios, derechos, deberes y procedimientos allí previstos.

En los eventos en que resulte aplicable el régimen de Habeas Data Financiero, las disposiciones de la Ley 1266 de 2008 prevalecerán respecto del tratamiento de esta clase de información, sin perjuicio de la aplicación complementaria de la Ley 1581 de 2012 en aquellos aspectos no regulados expresamente por la normativa especial.

28. MODIFICACIÓN, PUBLICACIÓN Y VIGENCIA

Los cambios sustanciales relativos a la identidad del Responsable, finalidades, derechos o condiciones del Tratamiento serán comunicados antes o a más tardar al momento de su implementación. Cuando se modifique una finalidad que requiera consentimiento, se obtendrá una nueva autorización.
La última versión estará disponible en el sitio web o en los canales corporativos definidos. El presente Manual entrará en vigor en la fecha de su aprobación y reemplazará la versión 02 del 15 de febrero de 2025.

Versión anterior	Fecha anterior	Nueva versión	Fecha	Descripción
02	15/02/2025	03	30 de agosto de 2026	Actualización integral: normativa 2025-2026, bases y finalidades, datos sensibles y menores, prohibiciones, cookies, transferencias, contratación, seguridad, incidentes, RNBD y anexos.