Tabla de contenido

1. Declaración de adopción, implementación y ejecución

1.1. Declaración de la Alta Dirección

Asesorías Vega Martínez S.A.S. (en adelante, la "Empresa" o "AVM S.A.S.") adopta, implementa y ejecuta la presente Política de Tratamiento de Datos Personales. Esta Política no constituye una declaración de intención ni un documento meramente informativo: es una norma interna de obligatorio cumplimiento, vinculante para la Empresa y para todas las personas que intervienen en el Tratamiento de datos personales, cuya observancia es objeto de verificación, medición y auditoría en los términos previstos en el numeral 18.

La Alta Dirección de la Empresa declara expresamente que:

1. Aprueba la presente Política y ordena su implementación y ejecución a partir de la fecha de entrada en vigencia señalada en el numeral 24.
2. Asigna los recursos humanos, técnicos, tecnológicos y financieros necesarios para su cumplimiento, en proporción al tamaño de la Empresa y a la naturaleza de los datos que trata.
3. Designa un Responsable de Protección de Datos Personales, con las funciones y la autoridad descritas en el numeral 7.
4. Asume el principio de responsabilidad demostrada (*accountability*) previsto en el artículo 26 del Decreto 1377 de 2013, en el sentido de adoptar medidas apropiadas, efectivas y verificables, y de conservar la evidencia documental que permita demostrar su cumplimiento ante los Titulares, ante sus clientes corporativos y ante la Superintendencia de Industria y Comercio.
5. Somete el cumplimiento de esta Política a un programa permanente de auditoría y de mejora continua.

1.2. Alcance del compromiso de ejecución

El incumplimiento de la presente Política por parte de trabajadores constituye falta disciplinaria y será sancionado conforme al Reglamento Interno de Trabajo y a la ley laboral. Tratándose de contratistas, proveedores y Encargados del Tratamiento, el incumplimiento constituye causal de incumplimiento contractual y podrá dar lugar a la terminación del vínculo y a las acciones legales que correspondan.

1.3. Plan de implementación

La Empresa ejecutará el siguiente plan de implementación, cuyos soportes se conservarán como evidencia del cumplimiento:

#	Actividad	Responsable	Plazo (contado desde la aprobación)	Evidencia
1	Publicación de la Política en el sitio web y comunicación a los Titulares	Responsable de Protección de Datos	15 días calendario	Captura del sitio web; constancia de comunicación
2	Socialización interna de la Política y firma de acuerdos de confidencialidad	Responsable de Protección de Datos	30 días calendario	Acta de socialización y listado de asistencia
3	Actualización del inventario de bases de datos (numeral 8.6)	Responsable de Protección de Datos	30 días calendario	Inventario firmado

#	Actividad	Responsable	Plazo (contado desde la aprobación)	Evidencia
4	Actualización de formatos de autorización y avisos de privacidad	Administración	45 días calendario	Formatos vigentes
5	Verificación y suscripción de contratos de transmisión con Encargados	Administración	60 días calendario	Contratos suscritos
6	Primera capacitación anual en protección de datos	Responsable de Protección de Datos	60 días calendario	Acta y listado de asistencia
7	Verificación del estado de obligación frente al RNBD y registro o constancia de no obligación	Responsable de Protección de Datos	60 días calendario	Certificación de activos y, si aplica, constancia de registro
8	Implementación de la matriz de riesgos y del plan de mitigación (numeral 15)	Responsable de Protección de Datos	90 días calendario	Matriz diligenciada y plan de acción
9	Primera auditoría de cumplimiento (numeral 18)	Auditor designado	90 días calendario	Informe de auditoría

1.4. Recursos y evidencias

La Empresa conservará, en expediente físico o electrónico bajo custodia del Responsable de Protección de Datos, la evidencia de cada una de las actividades anteriores, así como los registros de capacitaciones, autorizaciones, atención de consultas y reclamos, incidentes de seguridad, auditorías y planes de acción. Esta evidencia estará disponible para los procesos de verificación de los clientes corporativos de la Empresa y de las autoridades competentes.

2. Objeto

La presente Política de Tratamiento de Datos Personales (en adelante, la "Política") tiene por objeto desarrollar, implementar y garantizar el cumplimiento del derecho constitucional de hábeas data de los Titulares de la información, de conformidad con lo dispuesto en la Ley Estatutaria 1581 de 2012, el Decreto 1377 de 2013 —compilado en el Decreto Único Reglamentario 1074 de 2015— y las demás normas que los modifiquen, adicionen o reglamenten.

A través de esta Política, AVM S.A.S. establece las condiciones, finalidades, procedimientos, medidas de seguridad y controles bajo los cuales recolecta, almacena, usa, circula, transmite, transfiere y suprime los datos personales de sus clientes, Titulares vinculados a los servicios que presta, trabajadores, aspirantes, proveedores, aliados y demás terceros.

En particular, y dado el objeto social de la Empresa, esta Política regula el Tratamiento de datos personales que la Empresa realiza con fines de contactabilidad, socialización y notificación, tanto en nombre propio como por cuenta de sus clientes corporativos cuando actúa en calidad de Encargada del Tratamiento, según se desarrolla en el numeral 9.1.

Esta Política es de obligatorio cumplimiento para todos los colaboradores, contratistas, proveedores y terceros que, en ejercicio de sus funciones y con ocasión de la relación con la Empresa, intervengan en cualquier operación que implique el Tratamiento de datos personales, con independencia del medio o canal utilizado, físico o electrónico.

3. Ámbito de aplicación

La presente Política aplica a todas las bases de datos y archivos, físicos o electrónicos, que contengan datos personales y que sean objeto de Tratamiento por parte de la Empresa, incluidas las bases de datos de clientes y Titulares vinculados a los servicios prestados, trabajadores y aspirantes, proveedores y terceros, así como los datos recogidos a través de formularios web, correo electrónico, WhatsApp, llamadas telefónicas, formatos físicos y cualquier otro canal de atención o contacto.

De conformidad con el artículo 2° de la Ley 1581 de 2012, la Política resulta aplicable al Tratamiento de datos personales efectuado en territorio colombiano. Quedan excluidos de su ámbito los datos tratados en un contexto exclusivamente personal o doméstico, así como las categorías expresamente exceptuadas por la ley.

4. Marco normativo

La Empresa da cumplimiento al siguiente marco normativo, sin perjuicio de las normas que lo modifiquen o complementen:

1. Constitución Política de Colombia, artículo 15.
2. Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
3. Decreto Reglamentario 1377 de 2013, compilado en el Decreto Único Reglamentario 1074 de 2015 (Capítulo 25 del Título 2 de la Parte 2 del Libro 2).
4. Decreto 886 de 2014 y Decreto 090 de 2018, relativos al Registro Nacional de Bases de Datos (RNBD).
5. Decreto 255 de 2022, sobre normas corporativas vinculantes para la certificación de buenas prácticas en protección de datos personales y su transferencia a terceros países entre sociedades de un mismo grupo empresarial.

6. Título V de la Circular Única de la Superintendencia de Industria y Comercio, en particular: el Capítulo II sobre el RNBD y el reporte de novedades e incidentes de seguridad, y el Capítulo III sobre transferencias internacionales de datos personales, incorporado mediante la Circular Externa 005 de 2017.
7. Demás guías, circulares y conceptos expedidos por la Superintendencia de Industria y Comercio (SIC), autoridad nacional de protección de datos personales.

5. Definiciones

Para efectos de la presente Política, y en concordancia con el artículo 3° de la Ley 1581 de 2012 y sus normas reglamentarias, se entiende por:

Autorización: consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de sus datos personales.

Aviso de Privacidad: comunicación verbal o escrita generada por el Responsable, dirigida al Titular, mediante la cual se le informa el Tratamiento al que serán sometidos sus datos personales, las finalidades y los derechos que le asisten.

Base de Datos: conjunto organizado de datos personales que sea objeto de Tratamiento.

Contactabilidad: capacidad que tiene una empresa para comunicarse de forma efectiva con sus clientes o prospectos. Es el conjunto de actividades de Tratamiento orientadas a establecer, mantener y documentar comunicación para avanzar con diversos procesos con el Titular a través de los canales autorizados, con el fin de gestionar la relación contractual, coordinar la prestación del servicio, socializar información, notificar decisiones o resultados y atender sus solicitudes.

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

Dato privado: dato personal que, por su naturaleza, solo tiene relevancia para el Titular y las personas autorizadas por él.

Dato público: dato calificado como tal según los mandatos de la ley o la Constitución, así como aquellos que no sean semiprivados, privados o sensibles, por ejemplo el estado civil, la condición de comerciante o el estado de insolvencia.

Dato semiprivado: dato que no tiene naturaleza íntima, reservada ni pública, y cuyo conocimiento o divulgación puede interesar no solo a su Titular sino a un sector de personas o a la sociedad en general.

Dato sensible: aquel que afecta la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como los que revelan el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos u organizaciones sociales, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Encargado del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Incidente de seguridad: violación de los códigos de seguridad, o pérdida, robo o acceso no autorizado a la información de una base de datos administrada por el Responsable o por su Encargado.

Responsable del Tratamiento: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y el Tratamiento de los datos.

Titular: persona natural cuyos datos personales sean objeto de Tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Transferencia: comunicación de datos personales a un destinatario, ubicado dentro o fuera del territorio colombiano, que actúa como Responsable del Tratamiento.

Transmisión: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio colombiano, cuando tenga por objeto la realización de un Tratamiento por el Encargado, por cuenta del Responsable.

6. Principios rectores del Tratamiento

En el desarrollo, interpretación y aplicación de esta Política, la Empresa aplicará de manera armónica e integral los principios consagrados en el artículo 4° de la Ley 1581 de 2012:

Legalidad: el Tratamiento es una actividad reglada que se sujeta a la Constitución, la ley y las demás disposiciones que las desarrollan.

Finalidad: el Tratamiento obedece a una finalidad legítima, determinada, explícita e informada al Titular, y se desarrolla dentro del objeto social de la Empresa.

Libertad: el Tratamiento solo se ejerce con el consentimiento previo, expreso e informado del Titular, salvo mandato legal o judicial que releve el consentimiento.

Veracidad o calidad: la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Transparencia: el Titular tiene derecho a obtener de la Empresa, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Acceso y circulación restringida: el Tratamiento se sujeta a los límites derivados de la naturaleza de los datos y de la ley. Los datos no públicos no estarán disponibles en internet u otros medios de divulgación masiva, salvo que el acceso sea técnicamente controlable.

Seguridad: la información se maneja con las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros y evitar su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Confidencialidad: todas las personas que intervengan en el Tratamiento están obligadas a garantizar la reserva de la información, aun después de finalizada su relación con la Empresa.

7. Roles y responsabilidades

7.1. Representante Legal

Aprueba la Política y sus actualizaciones, asigna los recursos para su implementación, conoce los informes de auditoría y los planes de acción, y responde ante las autoridades por el cumplimiento del régimen de protección de datos personales.

7.2. Responsable de Protección de Datos Personales

La Empresa designa como Responsable de Protección de Datos Personales a Jhon Edison Sánchez Coordinador del departamento de TI, quien podrá ser contactado al correo electrónico asevega@avmsas.com y al celular (+57) 300-6518983. Sus funciones son:

1. Liderar la implementación, ejecución y actualización de la presente Política.
2. Atender y tramitar las consultas y reclamos de los Titulares dentro de los términos legales.
3. Mantener y actualizar el inventario de bases de datos.
4. Gestionar los incidentes de seguridad conforme al protocolo del numeral 16, y efectuar los reportes ante la SIC dentro de los términos del numeral 16.6.
5. Coordinar el programa de capacitación y conservar sus registros.
6. Apoyar la ejecución de las auditorías y hacer seguimiento a los planes de acción.
7. Verificar que los Encargados del Tratamiento cuenten con contrato de transmisión vigente.
8. Custodiar la evidencia documental del cumplimiento de esta Política.

7.3. Colaboradores, contratistas y proveedores

Cumplen la Política en el ejercicio de sus funciones, tratan únicamente los datos a los que estén autorizados, guardan reserva sobre la información, reportan de manera inmediata cualquier incidente de seguridad y participan en las capacitaciones programadas.

7.4. Auditor designado

Ejecuta el programa de auditoría del numeral 18. Podrá ser un colaborador designado por la Gerencia que no participe directamente en las actividades auditadas, o un tercero independiente. En ningún caso el Responsable de Protección de Datos auditará su propia gestión.

8. Categorías de información tratada

La Empresa trata únicamente los datos personales necesarios para el desarrollo de su objeto social y el cumplimiento de sus obligaciones legales, contractuales y laborales.

8.1. Datos de clientes y de Titulares vinculados a los servicios prestados

Nombres y apellidos; número de identificación; datos de contacto (teléfono fijo, celular, correo electrónico, dirección física, coordenadas de ubicación del bien objeto del servicio); calidad en que actúa el Titular frente al bien o servicio; y demás información necesaria para la prestación de los servicios comprendidos en el objeto social de la Empresa.

Parte de la información anterior —por ejemplo los datos catastrales, geográficos y de linderos de los inmuebles, o los datos de identificación y ubicación de maquinaria y equipo— puede permitir identificar a personas naturales, razón por la cual se tratará como dato personal bajo las condiciones de la presente Política.

8.2. Datos de trabajadores y aspirantes

Hoja de vida; documento de identidad; datos de contacto; información académica y de experiencia laboral; referencias personales y laborales; datos bancarios; información salarial y prestacional; afiliaciones al sistema de seguridad social (EPS, ARL y fondo de pensiones); certificados médicos e incapacidades; exámenes de ingreso y periódicos; antecedentes disciplinarios y judiciales cuando la ley lo permita; fotografía; e información de beneficiarios y familiares para efectos de seguridad social y seguros.

8.3. Datos de proveedores y terceros

Nombres y apellidos; documento de identidad; datos de contacto; datos bancarios; certificaciones y registros de habilitación; e información financiera básica necesaria para la gestión de pagos y la formalización de vínculos comerciales.

8.4. Datos de navegación web

Dirección IP, tipo de dispositivo y navegador, páginas visitadas, tiempo de permanencia y datos de origen del tráfico, recolectados a través de cookies y tecnologías similares en los términos del numeral 22.

8.5. Datos sensibles

De conformidad con el artículo 6° de la Ley 1581 de 2012, la Empresa no tratará datos sensibles, salvo que: (i) el Titular haya otorgado su autorización explícita e informada; (ii) el Tratamiento sea necesario para salvaguardar el interés vital del Titular, quien se encuentre física o jurídicamente incapacitado; (iii) se trate de datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso

judicial; o (iv) el Tratamiento tenga una finalidad histórica, estadística o científica con supresión de identidad, o exista otra excepción legal.

En el ámbito laboral, la Empresa podrá tratar información relativa a la salud de sus trabajadores (certificados médicos, incapacidades, afiliaciones a seguridad social) cuando ello sea necesario para el cumplimiento de sus obligaciones legales, contractuales y prestacionales. En estos casos se obtendrá autorización explícita del trabajador conforme al anexo de autorización para datos sensibles del contrato de trabajo, y se adoptarán medidas reforzadas de seguridad y confidencialidad.

8.6. Inventario de bases de datos y estado frente al RNBD

La Empresa mantiene un inventario actualizado de sus bases de datos que identifica, para cada una: denominación, finalidad, categorías de Titulares y de datos, canal de recolección, ubicación y medio de almacenamiento, responsable interno, Encargados con acceso, medidas de seguridad aplicadas y período de conservación. El inventario se revisa como mínimo una vez al año y cada vez que se cree, modifique o suprima una base de datos.

De conformidad con el Decreto 090 de 2018, están obligadas a inscribir sus bases de datos en el Registro Nacional de Bases de Datos las sociedades con activos totales superiores a 100.000 UVT y las personas jurídicas de naturaleza pública. La Empresa declara que, con corte al cierre del ejercicio 2025, sus activos totales no superan el umbral de 100.000 UVT y, en consecuencia, no se encuentra obligada a inscribir sus bases de datos en el RNBD. El deber de reportar incidentes de seguridad ante la SIC aplica con independencia de que exista o no obligación de registro, conforme al numeral 16.6.

9. Finalidades del Tratamiento

Los datos personales tratados por la Empresa tendrán las finalidades que se indican a continuación, según la categoría del Titular. Ninguna finalidad distinta de las aquí previstas será desarrollada sin informarlo previamente al Titular y, cuando corresponda, sin obtener una nueva autorización.

9.1. Finalidad de contactabilidad, socialización y notificación

La Empresa declara que una parte esencial del objeto del Tratamiento es la contactabilidad de los Titulares. En desarrollo de esta finalidad, la Empresa trata los datos de contacto (teléfono fijo, teléfono celular, correo electrónico, WhatsApp, dirección física y demás canales suministrados por el Titular) para:

1. **Contactar** al Titular para verificar y confirmar la información necesaria para la prestación del servicio.
2. **Coordinar, confirmar y reprogramar** las visitas de inspección o los desplazamientos técnicos a los bienes objeto del servicio, así como informar la fecha, hora e identidad del personal que realizará la visita.
3. **Socializar** con el Titular el alcance, las condiciones, el estado de avance y los resultados del servicio contratado, así como los requisitos y documentos que deba aportar.

4. **Notificar** la entrega de informes, comunicaciones, requerimientos de información, decisiones y respuestas a solicitudes.
5. **Notificar y gestionar** asuntos de facturación, cobro y cartera relacionados con los servicios prestados.
6. **Verificar la identidad** del Titular y la legitimidad de quien solicita el servicio o ejerce derechos sobre los datos.
7. **Atender** consultas, reclamos, peticiones y solicitudes de ejercicio de derechos, y comunicar su respuesta.
8. **Comunicar** cambios en la presente Política, en los canales de atención o en las condiciones del servicio.
9. **Realizar** encuestas de satisfacción y actividades de mejora de la calidad del servicio.

Contactabilidad por cuenta de clientes corporativos. Cuando la Empresa actúe como Encargada del Tratamiento por cuenta de un Responsable —en particular entidades financieras, fiduciarias, aseguradoras o despachos judiciales que le transmitan datos de sus clientes—, la contactabilidad se ejercerá exclusivamente para las finalidades instruidas por el Responsable y dentro de los límites del contrato de transmisión de datos suscrito. En estos casos, la Empresa contactará al Titular únicamente para coordinar y ejecutar el servicio encomendado, se identificará indicando por cuenta de quién actúa, y no utilizará los datos así recibidos para finalidades propias, comerciales o de cualquier otra naturaleza.

Reglas de contacto. Las gestiones de contacto se realizarán en horario hábil, salvo que el Titular autorice expresamente otro horario; se limitarán a un número razonable de intentos por canal; respetarán la solicitud del Titular de ser contactado por un canal determinado o de no ser contactado para finalidades no contractuales; y quedarán registradas con fecha, hora, canal, responsable de la gestión y resultado, como soporte de la trazabilidad del Tratamiento.

Distinción entre contacto operativo y contacto comercial. El contacto necesario para la ejecución del contrato, la prestación del servicio y el cumplimiento de obligaciones legales no requiere autorización adicional a la otorgada al momento de la vinculación. El envío de comunicaciones comerciales, publicidad u ofertas de nuevos servicios requiere autorización previa, expresa e independiente del Titular, recogida mediante casilla o marcación separada, revocable en cualquier momento y sin que su revocatoria afecte la prestación del servicio contratado.

9.2. Finalidades frente a clientes y solicitantes de servicios

1. Atender solicitudes de información, cotizaciones y solicitudes de servicios profesionales.
2. Celebrar, ejecutar y dar seguimiento a los contratos de prestación de servicios.
3. Verificar la identidad y la legitimidad de la persona que solicita el servicio y su relación con el bien o asunto objeto de este.
4. Facturar y gestionar el cobro de los servicios prestados.
5. Cumplir obligaciones tributarias, contables, registrales y legales, así como los requerimientos de autoridades judiciales, administrativas o de control.

6. Conservar el historial de servicios con fines de calidad, estadística, archivo y defensa de los derechos de la Empresa o de los Titulares.
7. Desarrollar las actividades de contactabilidad, socialización y notificación descritas en el numeral 9.1.
8. Enviar comunicaciones comerciales, publicidad y ofertas de nuevos servicios, únicamente cuando medie la autorización previa, expresa e independiente prevista en el numeral 9.1.

9.3. Finalidades frente a trabajadores y aspirantes

1. Gestionar procesos de selección y vinculación laboral.
2. Celebrar, ejecutar y terminar los contratos de trabajo y demás actos derivados de la relación laboral.
3. Gestionar la nómina, liquidaciones, prestaciones sociales, aportes al sistema de seguridad social, cajas de compensación y demás obligaciones laborales y parafiscales.
4. Administrar permisos, vacaciones, incapacidades y ausentismo.
5. Cumplir con el Sistema de Gestión de Seguridad y Salud en el Trabajo y las obligaciones ante la ARL.
6. Ejercer control interno, disciplina y evaluación de desempeño dentro de los límites legales.
7. Garantizar la seguridad de las personas, bienes e instalaciones, incluida la videovigilancia previo aviso informativo, y la continuidad del negocio.
8. Cumplir requerimientos de autoridades administrativas, fiscales, laborales o judiciales.
9. Conservar la información para la gestión documental y la defensa de los derechos de las partes en procesos judiciales o administrativos.

9.4. Finalidades frente a proveedores y terceros

1. Gestionar la vinculación, evaluación, contratación y pago de proveedores y colaboradores externos.
2. Cumplir obligaciones tributarias, contables y legales.
3. Mantener comunicación relacionada con los vínculos comerciales.

9.5. Finalidades generales y de archivo

La Empresa conservará los datos personales únicamente por el tiempo necesario para cumplir las finalidades autorizadas, así como durante los términos de prescripción o conservación exigidos por la ley, los contratos y las obligaciones con autoridades de control. Vencidos dichos términos, los datos serán suprimidos, destruidos de forma segura o anonimizados.

10. Autorización del Titular

De conformidad con el artículo 9° de la Ley 1581 de 2012, el Tratamiento de datos personales requiere la autorización previa, expresa e informada del Titular, la cual deberá obtenerse por cualquier medio que pueda ser objeto de consulta posterior.

La Empresa solicitará la autorización a través de los siguientes mecanismos, entre otros: (i) casillas de verificación en los formularios de su sitio web y canales digitales; (ii) declaraciones de autorización contenidas en contratos, cotizaciones u órdenes de servicio; (iii) formatos físicos de autorización firmados; (iv) mensajes de datos —correo electrónico, WhatsApp u otro canal que deje constancia del envío y la aceptación—; y (v) cláusulas de los contratos de trabajo y sus anexos. En todos los casos se conservará prueba del otorgamiento de la autorización.

10.1. Contenido de la autorización

Al solicitar la autorización, la Empresa informará al Titular de manera clara y expresa, en cumplimiento del artículo 12 de la Ley 1581 de 2012 y del artículo 12 del Decreto 1377 de 2013:

1. El Tratamiento al cual serán sometidos sus datos personales y su finalidad, incluida expresamente la finalidad de contactabilidad prevista en el numeral 9.1.
2. El carácter facultativo de la respuesta a las preguntas que versen sobre datos sensibles o sobre datos de niñas, niños y adolescentes.
3. Los derechos que le asisten como Titular: conocer, actualizar, rectificar, suprimir, revocar la autorización y acceder gratuitamente a sus datos.
4. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.
5. Los mecanismos habilitados para conocer la Política y ejercer sus derechos, así como el canal donde podrá consultar su versión vigente.

10.2. Casos en los que no se requiere autorización

De conformidad con el artículo 10 de la Ley 1581 de 2012, no se requerirá autorización cuando se trate de: (i) información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; (ii) datos de naturaleza pública; (iii) casos de urgencia médica o sanitaria; (iv) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos; y (v) datos relacionados con el Registro Civil de las Personas. Quien acceda a los datos sin autorización deberá, en todo caso, cumplir las disposiciones de la Ley 1581 de 2012.

11. Derechos de los Titulares

De conformidad con el artículo 8° de la Ley 1581 de 2012, el Titular tendrá los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales frente a la Empresa, incluso frente a datos parciales, inexactos, incompletos, fraccionados o que induzcan a error.

2. Solicitar prueba de la autorización otorgada, salvo cuando la ley la exceptúe como requisito para el Tratamiento.
3. Ser informado por la Empresa, previa solicitud, respecto del uso que le ha dado a sus datos personales.
4. Presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la Ley 1581 de 2012 y demás normas que la modifiquen o complementen.
5. Revocar la autorización o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de Tratamiento.

La revocatoria de la autorización o la solicitud de supresión no implicará la eliminación total de la información cuando la Empresa tenga un deber legal o contractual de conservarla. En tal caso, la Empresa conservará la información únicamente en la medida necesaria para cumplir dicho deber y procederá a la supresión o bloqueo del dato cuando ese deber desaparezca, conforme a los artículos 15 de la Ley 1581 de 2012 y 21 del Decreto 1377 de 2013.

12. Protocolo de atención al Titular: alcance, canales y procedimiento

12.1. Alcance

Este protocolo aplica a toda petición, consulta, reclamo, solicitud de actualización, rectificación o supresión, y a toda revocatoria de autorización presentada por un Titular, sus causahabientes o sus representantes, con independencia del canal por el que se reciba y de si la Empresa actúa como Responsable o como Encargada del Tratamiento.

12.2. Canales de atención

Canal	Dato de contacto	Disponibilidad
Correo electrónico	asevega@avmsas.com	Permanente
Dirección física	Calle 26 Norte # 4N–23, segundo piso, oficina AVM, Cali, Valle del Cauca	Horario de atención de la Empresa
Teléfono y WhatsApp	(+57) 300 651 8983	Horario de atención de la Empresa
Sitio web	www.avmsas.com, sección de protección de datos	Permanente

Toda solicitud recibida por un canal distinto de los anteriores será redirigida internamente al Responsable de Protección de Datos dentro del día hábil siguiente a su recepción, y el término legal se contará desde la recepción inicial.

12.3. Contenido de la solicitud

La solicitud deberá contener la identificación del Titular (nombres, apellidos y documento de identidad), la descripción clara y precisa de la petición, los hechos que la motivan, los datos de contacto para recibir la respuesta y, cuando corresponda, los documentos que se quieran hacer valer. Cuando actúe un tercero en representación del Titular, deberá acreditar su condición mediante poder o documento de representación.

12.4. Trámite de consultas (artículo 14, Ley 1581 de 2012)

Las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo. Cuando no fuere posible atenderlas dentro de dicho término, la Empresa informará al interesado los motivos de la demora y la fecha en que se atenderá, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

12.5. Trámite de reclamos (artículo 15, Ley 1581 de 2012)

1. Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a su recepción para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.
2. Recibido el reclamo completo, la Empresa incluirá en la base de datos la leyenda “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles, la cual se mantendrá hasta que el reclamo sea decidido.
3. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.
4. La respuesta se comunicará al peticionario por el medio señalado en su solicitud y se conservará prueba de su envío y de la actuación surtida.

12.6. Registro y trazabilidad

Toda solicitud se registrará en la bitácora de atención a Titulares, que contendrá como mínimo: número consecutivo, fecha y hora de recepción, canal, identificación del solicitante, tipo de solicitud, término legal aplicable, fecha de respuesta, sentido de la respuesta y soporte de su envío. Esta bitácora es insumo de las auditorías previstas en el numeral 18 y, cuando la Empresa se encuentre obligada, del reporte semestral de reclamos ante el RNBD.

12.7. Requisito de procedibilidad ante la SIC

De conformidad con el artículo 16 de la Ley 1581 de 2012, el Titular solo podrá elevar queja ante la Superintendencia de Industria y Comercio una vez haya agotado el trámite de consulta o reclamo ante la Empresa. La Empresa informará a los Titulares sobre este requisito y les facilitará, cuando corresponda, las constancias de las respuestas emitidas.

12.8. Medio de información y gratuidad

La información solicitada será suministrada por cualquier medio, incluidos los electrónicos, en formato de fácil lectura y sin barreras técnicas, de conformidad con el artículo 11 de la Ley 1581 de 2012. El acceso a los datos personales por parte del Titular es gratuito.

13. Deberes del Responsable y del Encargado del Tratamiento

13.1. Deberes de la Empresa como Responsable del Tratamiento

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
2. Solicitar y conservar copia de la autorización otorgada por el Titular.
3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información suministrada a los Encargados sea veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar la información y comunicar oportunamente a los Encargados las novedades respecto de los datos suministrados.
7. Rectificar la información cuando sea incorrecta y comunicarlo al Encargado.
8. Suministrar a los Encargados únicamente datos cuyo Tratamiento esté previamente autorizado.
9. Exigir al Encargado el respeto a las condiciones de seguridad y privacidad de la información del Titular.
10. Tramitar las consultas y reclamos en los términos señalados en la ley.
11. Adoptar un manual interno de políticas y procedimientos para el adecuado cumplimiento de la Ley 1581 de 2012.
12. Informar al Encargado cuando determinada información se encuentre en discusión por parte del Titular.
13. Informar, a solicitud del Titular, sobre el uso dado a sus datos.
14. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares, en los términos del numeral 16.6.
15. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

13.2. Deberes de la Empresa cuando actúe como Encargada

Cuando la Empresa actúe como Encargada del Tratamiento por cuenta de un tercero —por ejemplo, al prestar servicios propios de su objeto social a bancos, fiduciarias, aseguradoras o despachos judiciales que le transmitan datos de sus clientes— cumplirá los deberes del artículo 18 de la Ley 1581 de 2012, entre ellos: garantizar al Titular el pleno y efectivo ejercicio de sus derechos; conservar la información bajo las condiciones de seguridad necesarias; realizar oportunamente las actualizaciones, rectificaciones o supresiones; registrar la leyenda "reclamo en trámite" en la forma prevista en la ley; tramitar consultas y reclamos; adoptar el manual interno de políticas y procedimientos; y abstenerse de circular información que esté en discusión.

Adicionalmente, en su condición de Encargada, la Empresa se obliga a: (i) tratar los datos únicamente conforme a las instrucciones documentadas del Responsable; (ii) no utilizar los datos para finalidades propias; (iii) suprimir o devolver los datos al terminar el encargo, salvo obligación legal de conservación; (iv) informar al Responsable, dentro de las veinticuatro (24) horas siguientes a su detección, cualquier incidente de seguridad que afecte los datos recibidos; y (v) permitir y facilitar las auditorías que el Responsable decida practicar sobre el cumplimiento del encargo. Toda actuación como Encargada se regirá por el contrato de transmisión suscrito con el correspondiente Responsable.

14. Medidas de seguridad de la información

La Empresa adopta medidas técnicas, humanas y administrativas razonables y proporcionales a su tamaño y a la naturaleza de los datos que trata, para proteger los datos personales contra adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

14.1. Medidas administrativas y de personal

- Designación del Responsable de Protección de Datos Personales y de la persona encargada de atender consultas y reclamos.
- Cláusulas de confidencialidad y manejo de información en contratos de trabajo y de prestación de servicios, con vigencia posterior a la terminación del vínculo.
- Capacitación periódica sobre protección de datos y deber de confidencialidad, conforme al numeral 17.
- Política de escritorio y archivo limpio.
- Acceso a los datos personales únicamente por el personal autorizado y según sus funciones, bajo el principio de mínimo privilegio.
- Revocatoria de accesos y devolución de activos de información al terminar la relación laboral o contractual.

14.2. Medidas físicas

- Archivos físicos bajo llave o en áreas de acceso restringido, con control de préstamo y consulta.

- Documentación de los servicios custodiada en archivadores cerrados; destrucción segura, confidencial y documentada de documentos obsoletos.
- Oficinas y áreas de almacenamiento con acceso controlado.
- Equipos portátiles y celulares corporativos asegurados con contraseña y cifrado.

14.3. Medidas técnicas

- Equipos, correos y sistemas con contraseñas robustas y acceso por usuario, con cambio periódico de credenciales.
- Doble factor de autenticación en los servicios que lo permitan, en especial correo electrónico y almacenamiento en la nube.
- Antivirus, firewall y actualizaciones de seguridad en equipos corporativos.
- Respaldo periódico y cifrado de las bases de datos, almacenado en ubicación separada, con pruebas de restauración.
- Restricción de acceso a carpetas y archivos digitales por nivel de autorización.
- Transmisión de información sensible únicamente por canales seguros y cifrados.
- Uso de herramientas de nube y correo de proveedores reconocidos, previa verificación de sus condiciones de seguridad.

15. Gestión de riesgos y plan de mitigación

15.1. Metodología

La Empresa identifica, analiza, valora y trata los riesgos asociados al Tratamiento de datos personales, en desarrollo del principio de responsabilidad demostrada. Cada riesgo se valora en función de su probabilidad de ocurrencia y del impacto sobre los derechos de los Titulares, y se le asigna un nivel (bajo, medio o alto) que determina la prioridad de las medidas de mitigación. La matriz se revisa como mínimo una vez al año, y cada vez que se materialice un incidente, se modifique un proceso, se incorpore una nueva herramienta tecnológica o se cree una nueva base de datos.

15.2. Matriz de riesgos y medidas de mitigación

#	Riesgo identificado	Nivel	Medidas de mitigación	Responsable
1	Acceso no autorizado a bases de datos digitales	Alto	Autenticación por usuario, doble factor, perfiles de acceso por función, revisión trimestral de accesos activos	Responsable de Protección de Datos
2	Pérdida o destrucción de información	Alto	Copias de respaldo periódicas y cifradas en ubicación separada; pruebas de restauración semestrales	Responsable de Protección de Datos

#	Riesgo identificado	Nivel	Medidas de mitigación	Responsable
3	Pérdida o hurto de equipos portátiles o celulares corporativos	Medio	Cifrado de disco, bloqueo por contraseña, borrado remoto, inventario de equipos y reporte inmediato	Administración
4	Envío de información a destinatario equivocado (correo o WhatsApp)	Alto	Verificación del destinatario antes del envío, uso de copia oculta en envíos masivos, protección de archivos con contraseña, capacitación específica	Todos los colaboradores
5	Tratamiento sin autorización válida del Titular	Alto	Formatos estandarizados de autorización, verificación de autorización previa al ingreso del dato, muestreo en auditoría	Administración
6	Uso de datos para finalidades no autorizadas, en particular contacto comercial sin autorización independiente	Alto	Marcación separada de la autorización comercial, segmentación de la base para envíos comerciales, revisión previa de campañas	Responsable de Protección de Datos
7	Datos desactualizados, inexactos o duplicados	Medio	Validación de datos en cada contacto, depuración anual del inventario, canal permanente de actualización para el Titular	Administración
8	Incumplimiento de los términos legales de respuesta a consultas y reclamos	Alto	Bitácora con control de términos, alertas de vencimiento, designación de un encargado responsable durante la ausencia del responsable principal de la protección de datos personales	Responsable de Protección de Datos
9	Fuga de información por colaboradores o contratistas	Alto	Acuerdos de confidencialidad, principio de mínimo privilegio, revocatoria de accesos al retiro, capacitación y régimen disciplinario	Representante Legal
10	Encargados del Tratamiento sin contrato de transmisión vigente	Medio	Inventario de Encargados, verificación previa a la entrega de datos, cláusulas de protección de datos en todos los contratos	Administración
11	Conservación de datos más allá del término necesario	Medio	Tabla de retención documental, revisión anual y supresión o anonimización documentada	Responsable de Protección de Datos

#	Riesgo identificado	Nivel	Medidas de mitigación	Responsable
12	Suplantación de identidad en solicitudes de ejercicio de derechos	Medio	Verificación de identidad antes de entregar información, exigencia de poder cuando actúe un tercero	Responsable de Protección de Datos
13	Ataques de phishing, ransomware o suplantación de correo corporativo	Alto	Antivirus y filtros de correo, capacitación en reconocimiento de fraudes, doble verificación de instrucciones sensibles, copias de respaldo aisladas	Responsable de Protección de Datos
14	Recolección de datos excesivos o innecesarios para la finalidad	Medio	Revisión de formularios y formatos, aplicación del principio de minimización, validación en auditoría	Administración

15.3. Plan de acción y seguimiento

Los riesgos calificados como altos contarán con un plan de acción documentado que precise la actividad, el responsable, el plazo y el indicador de cumplimiento. El avance del plan se revisa en cada ciclo de auditoría y se reporta a la Alta Dirección. Los hallazgos de auditoría y los incidentes materializados se incorporan a la matriz como insumo de la mejora continua.

16. Protocolo de gestión de incidentes de seguridad

16.1. Alcance

Este protocolo aplica a todo incidente de seguridad que afecte datos personales tratados por la Empresa, tanto en calidad de Responsable como de Encargada, con independencia del medio en que se encuentren los datos y de si el incidente tiene origen interno o externo, accidental o intencional. Se consideran incidentes, entre otros: el acceso no autorizado a bases de datos o a cuentas de correo; la pérdida, hurto o extravío de equipos o documentos que contengan datos personales; el envío de información a destinatarios no autorizados; la publicación o divulgación indebida de datos; la infección por software malicioso; y la alteración o destrucción no autorizada de información.

16.2. Canales de reporte interno

Todo colaborador, contratista o proveedor que detecte o sospeche la ocurrencia de un incidente debe reportarlo de manera inmediata y a más tardar dentro de las veinticuatro (24) horas siguientes al Responsable de Protección de Datos, a través de cualquiera de los siguientes canales: correo electrónico asevega@avmsas.com, teléfono o WhatsApp (+57) 300 651 8983, o comunicación directa con la Administración. El reporte de buena fe de un incidente no dará lugar a sanción alguna para quien lo efectúe.

16.3. Fases del protocolo

Fase	Actividad	Plazo interno
1. Detección y registro	Recepción del reporte y apertura del registro del incidente en la bitácora	Inmediato
2. Contención	Adopción de medidas inmediatas para detener o limitar el incidente (cambio de credenciales, aislamiento de equipos, bloqueo de accesos)	Dentro de las 24 horas siguientes al reporte
3. Evaluación	Determinación del alcance, tipo y volumen de datos comprometidos, Titulares afectados y nivel de riesgo	Dentro de los 3 días hábiles siguientes
4. Notificación	Comunicación a los Titulares afectados, a los clientes corporativos que corresponda y a la SIC, según los numerales 16.4 a 16.6	Según los plazos allí previstos
5. Erradicación y recuperación	Eliminación de la causa, restauración de la información y verificación de la normalidad de la operación	Dentro de los 10 días hábiles siguientes
6. Cierre y lecciones aprendidas	Informe final, actualización de la matriz de riesgos y definición de acciones correctivas	Dentro de los 15 días hábiles siguientes

16.4. Notificación a los Titulares

Cuando el incidente represente un riesgo para los derechos de los Titulares afectados, la Empresa les informará de manera clara y en el menor tiempo posible, y en todo caso dentro de los **cinco (5) días hábiles** siguientes a la evaluación del incidente, indicando la naturaleza del incidente, los datos comprometidos, las posibles consecuencias, las medidas adoptadas y las recomendaciones que deban seguir.

16.5. Notificación a clientes corporativos

Cuando el incidente afecte datos recibidos en calidad de Encargada del Tratamiento, la Empresa informará al Responsable del Tratamiento correspondiente dentro de las veinticuatro (24) horas siguientes a su detección, sin perjuicio de los plazos más exigentes que establezca el contrato de transmisión, y le prestará toda la colaboración necesaria para la atención del incidente y para el reporte que dicho Responsable deba efectuar ante la autoridad.

16.6. Reporte ante la Superintendencia de Industria y Comercio: tiempos

De conformidad con el literal n) del artículo 17 y el literal k) del artículo 18 de la Ley 1581 de 2012, y con el Capítulo II del Título V de la Circular Única de la SIC, la Empresa reportará los incidentes de seguridad

ante la Superintendencia de Industria y Comercio dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona encargada de atenderlos.

El canal de reporte depende de la situación de la Empresa frente al RNBD:

- Si la Empresa se encuentra obligada a inscribir sus bases de datos, el reporte se efectúa como novedad en el Registro Nacional de Bases de Datos.
- Si la Empresa no se encuentra obligada a inscribirlas, o cuando actúa en calidad de Encargada del Tratamiento, el reporte se efectúa mediante el aplicativo dispuesto para tal fin en el micrositio de la Delegatura para la Protección de Datos Personales, en www.sic.gov.co.

El deber de reportar incidentes de seguridad ante la SIC existe con independencia de que la Empresa esté o no obligada a registrar sus bases de datos en el RNBD.

16.7. Otros reportes ante la SIC

Cuando la Empresa se encuentre obligada a inscribir sus bases de datos en el RNBD, observará adicionalmente los siguientes términos:

Obligación	Término
Inscripción de bases de datos creadas con posterioridad al registro inicial	Dentro de los dos (2) meses siguientes a su creación
Actualización anual de la información registrada	Dentro del plazo anual señalado por la SIC, que vence el 31 de marzo de cada año
Reporte de cambios sustanciales en la información registrada	Dentro de los primeros diez (10) días hábiles del mes siguiente a aquel en que se produzca el cambio
Reporte semestral de reclamos presentados por los Titulares	Dentro de los primeros quince (15) días hábiles de los meses de febrero y agosto de cada año
Reporte de incidentes de seguridad	Quince (15) días hábiles, conforme al numeral 16.6

Se consideran cambios sustanciales, entre otros, los relacionados con la finalidad de la base de datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de datos almacenados, las medidas de seguridad implementadas, la presente Política y las transferencias o transmisiones internacionales de datos.

Los requerimientos de información que formule la SIC serán atendidos dentro del término señalado en el respectivo oficio.

16.8. Registro de incidentes

La Empresa mantiene una bitácora de incidentes que documenta, para cada uno: fecha y hora de detección, forma de detección, descripción, datos y Titulares afectados, nivel de riesgo, medidas de

contención y corrección, notificaciones efectuadas con su soporte, fecha del reporte a la SIC y su constancia, y acciones de mejora derivadas. Esta bitácora se conserva como evidencia de la gestión diligente de la Empresa.

17. Programa de capacitación

17.1. Objeto

La Empresa mantiene un programa permanente de capacitación en protección de datos personales y deber de confidencialidad, dirigido a todos los colaboradores, contratistas y demás personas que intervengan en el Tratamiento de datos personales, con el fin de garantizar que conozcan, entiendan y apliquen la presente Política, la Ley 1581 de 2012, sus normas reglamentarias y las medidas de seguridad adoptadas.

17.2. Periodicidad

Las capacitaciones se realizarán como mínimo una (1) vez al año, y la edición anual se programará dentro del primer trimestre del calendario. Adicionalmente se adelantarán capacitaciones extraordinarias cuando se produzcan cambios normativos relevantes, se actualice la presente Política, se implementen nuevas herramientas tecnológicas o medidas de seguridad, ocurra un incidente de seguridad o lo requiera la Superintendencia de Industria y Comercio.

17.3. Capacitación de ingreso

Todo colaborador que se vincule a la Empresa y vaya a intervenir en el Tratamiento de datos personales —incluidos trabajadores, contratistas, aprendices y pasantes— recibirá una capacitación de inducción dentro de los quince (15) días calendario siguientes a su vinculación y, en todo caso, antes de asumir funciones que impliquen Tratamiento de datos. La inducción incluirá como mínimo: el contenido de esta Política y el marco normativo aplicable; los deberes de confidencialidad y reserva, que subsisten después de terminada la relación; las finalidades autorizadas y las reglas para obtener la autorización de los Titulares; las reglas de contactabilidad del numeral 9.1; las medidas de seguridad aplicables a su cargo; el procedimiento de atención de consultas y reclamos; el deber de reportar incidentes y sus canales; y las consecuencias del incumplimiento.

17.4. Registro

Cada capacitación quedará registrada en un acta o listado de asistencia, físico o electrónico, con fecha, duración, temas tratados y asistentes, con su firma o constancia de participación. Estos registros se conservan como soporte del cumplimiento y se ponen a disposición de las auditorías del numeral 18 y de las autoridades competentes.

18. Programa de auditoría y verificación del cumplimiento

18.1. Objeto

La Empresa mantiene un programa permanente de auditoría y verificación del cumplimiento de la presente Política, de la Ley 1581 de 2012 y de sus normas reglamentarias, con el fin de evaluar la efectividad de las medidas adoptadas, identificar brechas de cumplimiento y promover la mejora continua.

18.2. Periodicidad

Las auditorías se realizarán con periodicidad trimestral, de manera continua mientras la Política se encuentre vigente. La primera auditoría se realizará dentro de los noventa (90) días calendario siguientes a la aprobación de la presente versión. Se adelantarán auditorías extraordinarias ante cambios normativos relevantes, la ocurrencia de incidentes de seguridad, requerimientos de la SIC o solicitud de un cliente corporativo.

18.3. Alcance

Cada ciclo de auditoría evaluará, entre otros aspectos: (i) el cumplimiento de los principios rectores y de las finalidades del Tratamiento, incluida la finalidad de contactabilidad y la separación entre contacto operativo y comercial; (ii) la existencia, vigencia y contenido de las autorizaciones otorgadas por los Titulares; (iii) la atención oportuna y completa de consultas y reclamos, con verificación de términos en la bitácora; (iv) la implementación y efectividad de las medidas de seguridad técnicas, humanas y administrativas; (v) la gestión de los incidentes de seguridad y el cumplimiento de los tiempos de reporte; (vi) la vigencia del inventario de bases de datos y el estado frente al RNBD; (vii) la gestión y supervisión de los Encargados del Tratamiento y la vigencia de sus contratos de transmisión; (viii) la ejecución del programa de capacitación; y (ix) el avance del plan de mitigación de riesgos.

18.4. Ejecución

Las auditorías serán ejecutadas por el auditor designado conforme al numeral 7.4, con el apoyo del Responsable de Protección de Datos, en las siguientes etapas:

1. **Planificación:** definición del alcance, cronograma y lista de verificación.
2. **Ejecución:** revisión documental, verificación de procedimientos y medidas de seguridad, pruebas de recorrido y entrevistas con el personal.
3. **Informe de resultados:** observaciones, hallazgos clasificados por criticidad y recomendaciones.
4. **Plan de acción:** acciones correctivas y preventivas, con responsable, plazo e indicador.
5. **Seguimiento:** verificación de la implementación del plan de acción en el ciclo siguiente y cierre de hallazgos.

18.5. Programa anual de auditorías

Ciclo	Mes programado	Alcance principal
1	Tercer mes siguiente a la aprobación	Cumplimiento general de la Política y verificación del plan de implementación
2	Sexto mes	Medidas de seguridad y gestión de incidentes
3	Noveno mes	Atención a Titulares, autorizaciones y reglas de contactabilidad
4	Duodécimo mes	Inventario de bases de datos, RNBD, Encargados y transferencias
5	Decimoquinto mes	Revisión anual integral y evaluación del plan de mitigación de riesgos

El programa se actualiza anualmente y podrá ajustarse según las necesidades de la Empresa, dejando constancia del ajuste.

18.6. Reporte a la Alta Dirección

Los informes de auditoría y los planes de acción serán presentados a la Alta Dirección y se conservarán como soporte del cumplimiento. Los hallazgos relevantes se tendrán en cuenta para la actualización de la Política y de sus medidas de seguridad, y podrán ser puestos a disposición de los clientes corporativos que lo requieran en desarrollo de sus procesos de verificación de proveedores.

19. Transferencias y transmisiones a terceros

La Empresa comparte datos personales con terceros únicamente cuando sea necesario para el desarrollo de sus actividades y en los casos previstos por la ley. En particular:

- **Con Encargados del Tratamiento** —por ejemplo, contadores y asesores tributarios, firmas de abogados, proveedores de nómina, plataformas de correo y almacenamiento en la nube, operadores logísticos o elaboradores de informes técnicos— mediante contratos de transmisión que garanticen la protección de los datos y la confidencialidad, de conformidad con el artículo 25 del Decreto 1377 de 2013.
- **Con autoridades judiciales, administrativas o de control**, o con entidades públicas en ejercicio de sus funciones legales o por orden judicial, sin necesidad de autorización del Titular, conforme al artículo 10 de la Ley 1581 de 2012.
- **Con los Titulares**, sus causahabientes y representantes legales, y con terceros autorizados por el Titular o por la ley.

La Empresa no vende ni alquila bases de datos ni información personal a terceros.

19.1. Transferencias y transmisiones internacionales

De conformidad con el artículo 26 de la Ley 1581 de 2012, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección, salvo las excepciones legales. Mediante la Circular Externa 005 de 2017, incorporada al Capítulo III del Título V de la Circular Única, la SIC estableció el listado de países que garantizan un nivel adecuado de protección, dentro del cual se encuentran, entre otros, los Estados Unidos de América y los Estados miembros de la Unión Europea.

Cuando la Empresa transfiera o transmita datos personales al exterior verificará, previamente y dejando constancia documental: (i) si el país de destino se encuentra en el listado de nivel adecuado de protección; (ii) en caso contrario, si la operación se enmarca en alguna de las excepciones del artículo 26 de la Ley 1581 de 2012 o si requiere declaración de conformidad de la SIC; y (iii) la existencia del contrato de transmisión correspondiente cuando el destinatario actúe como Encargado. La adopción de normas corporativas vinculantes en los términos del Decreto 255 de 2022 constituye un mecanismo adicional y facultativo, aplicable a transferencias entre sociedades de un mismo grupo empresarial.

Transferencia vigente – Vega Martinez Appraisal Management Services LLC. En desarrollo del Acuerdo de Colaboración suscrito entre la Empresa y Vega Martinez Appraisal Management Services LLC – VM Appraisal, sociedad domiciliada en el Estado de Florida, Estados Unidos de América, la Empresa comunica a esta última información derivada de los avalúos de maquinaria y equipo elaborados desde el año 2015 hasta la fecha, con la finalidad de que sea utilizada en la construcción, entrenamiento y validación de un modelo de valoración asistido por inteligencia artificial. La información objeto de esta comunicación comprende las características técnicas de los bienes valorados, sus condiciones de operación y estado, las variables de mercado consideradas y los resultados de la valoración, y es sometida a un proceso previo de disociación mediante el cual se suprime todo dato que permita identificar o hacer identificable a una persona natural. En consecuencia, y de conformidad con el artículo 2° de la Ley 1581 de 2012, la información así comunicada no constituye dato personal y su Tratamiento no se encuentra sujeto al régimen de protección de datos personales. La Empresa conserva la documentación del procedimiento de disociación aplicado y verifica, antes de cada envío, que la información no contenga datos identificables. Sin perjuicio de lo anterior, la Empresa deja constancia de que los Estados Unidos de América se encuentran dentro del listado de países con nivel adecuado de protección de datos personales señalado por la Superintendencia de Industria y Comercio en la Circular Externa 005 de 2017, incorporada al Capítulo III del Título V de la Circular Única.

20. Conservación y supresión de la información

La información se conservará durante el tiempo necesario para el cumplimiento de las finalidades autorizadas y durante los términos de prescripción y de conservación documental exigidos por las normas colombianas, entre ellas la conservación de libros y papeles de comercio y las obligaciones laborales y tributarias. Vencidos dichos términos, la Empresa suprimirá, destruirá de manera segura o anonimizará los datos personales, dejando constancia documental del procedimiento aplicado.

21. Tratamiento de datos de niños, niñas y adolescentes

De conformidad con el artículo 7° de la Ley 1581 de 2012, la Empresa asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Queda proscrito el Tratamiento de sus datos personales, salvo aquellos de naturaleza pública o cuando el Tratamiento se realice con la autorización del representante legal o tutor, atendiendo el interés superior del menor y su opinión cuando sea posible.

En el giro ordinario de la Empresa solo se tratarán datos de menores cuando sean titulares o copropietarios de los bienes objeto de estudio, caso en el cual la autorización será otorgada por sus representantes legales. Los datos de hijos menores de los colaboradores se tratarán únicamente para efectos de seguridad social, beneficios y seguros, previa autorización otorgada por el respectivo representante legal.

22. Política de cookies y datos de navegación

El sitio web de la Empresa puede utilizar cookies y tecnologías similares con fines técnicos (sesión y seguridad) y analíticos (medición de tráfico y mejora del sitio). Las cookies analíticas solo se activarán con el consentimiento del visitante, recogido mediante el aviso dispuesto en el sitio. El visitante puede configurar su navegador para rechazar o eliminar las cookies, sin perjuicio de la correcta funcionalidad del sitio. La información de navegación se tratará conforme a esta Política y se conservará por los períodos definidos por las herramientas de analítica utilizadas.

23. Tratamiento de datos de trabajadores

La Empresa garantiza que el Tratamiento de los datos de sus trabajadores se realiza dentro del marco de la relación laboral, de conformidad con la ley, los reglamentos internos y los contratos de trabajo. Para ello:

- La autorización se obtendrá mediante la cláusula y el anexo correspondiente del contrato de trabajo, así como en los formatos de hoja de vida y vinculación.
- El trabajador será informado sobre las finalidades del Tratamiento y los canales para ejercer sus derechos.
- Los datos cuyo Tratamiento sea necesario para el cumplimiento de obligaciones legales y de seguridad social no requerirán autorización adicional a la prevista en la ley, sin perjuicio del deber de información.
- Los datos sensibles, en especial los relativos a la salud, se tratarán exclusivamente con autorización explícita del trabajador, para las finalidades de seguridad social, seguridad y salud en el trabajo y gestión de incapacidades, con medidas reforzadas de seguridad y reserva.
- El trabajador podrá ejercer en cualquier momento sus derechos de conocer, actualizar, rectificar, suprimir y revocar, sin perjuicio de las obligaciones legales de conservación.
- La información entregada en procesos de selección se tratará con las mismas garantías de esta Política y se suprimirá cuando pierda su finalidad, salvo autorización del aspirante para conservarla en el banco de hojas de vida.

24. Vigencia y actualización de la Política

La presente Política de Tratamiento de Datos Personales rige a partir del 28 de agosto de 2026 y permanecerá vigente hasta tanto sea modificada o sustituida. La versión vigente estará disponible en www.avmsas.com, sección de protección de datos, y será comunicada a los Titulares a través de los canales de la Empresa.

Las bases de datos administradas por Asesorías Vega Martínez S.A.S. permanecerán vigentes durante el término necesario para cumplir las finalidades descritas en esta Política y, en todo caso, mientras subsista la relación contractual, comercial o laboral con el Titular. Vencido ese término, los datos se conservarán únicamente durante los plazos exigidos por las normas contables, tributarias, laborales y comerciales aplicables, tras lo cual serán suprimidos, destruidos de forma segura o anonimizados.

Los cambios a la Política se realizarán sin perjuicio de las autorizaciones ya otorgadas. Todo cambio sustancial será comunicado a los Titulares de manera eficiente antes de su implementación, conforme al artículo 13 del Decreto 1377 de 2013; cuando el cambio implique una modificación sustancial de las finalidades del Tratamiento, la Empresa solicitará una nueva autorización.

25. Datos del Responsable del Tratamiento

- **Razón social:** Asesorías Vega Martínez S.A.S.
- **NIT:** 800.148.262-1
- **Representante legal:** Armando Vega Sanclemente
- **Responsable de Protección de Datos:** Jhon Edison Sánchez Díaz – Coordinador de TI
- **Dirección:** Calle 26 Norte # 4N–23, segundo piso, oficina AVM, Cali, Valle del Cauca, Colombia
- **Correo electrónico:** asevega@avmsas.com
- **Teléfono y WhatsApp:** (+57) 300 651 8983
- **Sitio web:** www.avmsas.com

26. Quejas ante la Superintendencia de Industria y Comercio

Agotado el trámite de consulta o reclamo ante la Empresa, el Titular podrá presentar queja ante la Superintendencia de Industria y Comercio, autoridad de protección de datos personales, a través de sus canales oficiales (sede electrónica www.sic.gov.co), señalando los hechos que configuran el presunto incumplimiento.

El incumplimiento de las obligaciones de la Ley 1581 de 2012 puede acarrear las sanciones previstas en su artículo 23, entre ellas multas de carácter personal e institucional de hasta dos mil (2.000) salarios mínimos mensuales legales vigentes, la suspensión de las actividades relacionadas con el Tratamiento, el cierre temporal o definitivo de las operaciones que involucren Tratamiento de datos sensibles y, en general, las demás medidas previstas en la ley.

Aprobación de la Política

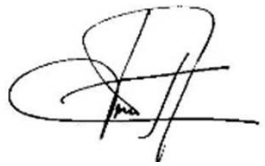
La presente Política de Tratamiento de Datos Personales fue revisada y aprobada por la administración de Asesorías Vega Martínez S.A.S., que ordena su adopción, implementación y ejecución a partir de la fecha de su entrada en vigencia.

Elaboró:

_____

Jhon Edison Sánchez
Responsable de Protección de Datos Personales – Asesorías Vega Martínez S.A.S.
Cali, Valle del Cauca, Fecha: Agosto 28 del 2026

Aprobó:



_____

Armando Vega Sanclemente
Representante Legal – Asesorías Vega Martínez S.A.S.
Cali, Valle del Cauca, Fecha: Agosto 28 del 2026

Anexo A. Formato de registro de incidente de seguridad

Campo	Contenido
Consecutivo	
Fecha y hora de detección	
Reportado por	
Canal de reporte	
Descripción del incidente	
Base de datos afectada	
Tipo y volumen de datos comprometidos	
Titulares afectados (número y categoría)	
Calidad de la Empresa (Responsable / Encargada)	
Nivel de riesgo	
Medidas de contención adoptadas y fecha	
¿Se notificó a los Titulares? Fecha y soporte	
¿Se notificó al Responsable (si actúa como Encargada)? Fecha y soporte	
¿Se reportó a la SIC? Fecha, canal y número de radicado	
Acciones correctivas y responsable	
Fecha de cierre	
Actualización de la matriz de riesgos	