PAVIMENTOS COLOMBIA S.A.S.

MANUAL HABEAS DATA

Manual de declaración de políticas de tratamiento de datos personales, procedimientos y medidas de seguridad.

Versión No. 6

Marzo de 2026

2026

TABLA DE CONTENIDO

APÉNDICE

ANEXOS

FORMATOS

PRESENTACIÓN

Mediante el presente documento, **LA ORGANIZACIÓN** presenta a todos aquellos interesados el Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad que tiene como objetivo fundamental documentar todos los principios, medidas, herramientas, instrumentos y reglas mediante las cuales se busca garantizar el correcto manejo en el Tratamiento de Datos Personales de todo Titular, establecer reglas para el ejercicio del derecho de habeas data y las medidas mínimas de seguridad de la información.

Mediante la implementación del Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad, **LA ORGANIZACIÓN** busca promover la seguridad, transparencia y cuidado en el manejo de la información contenida en sus Bases de Datos para que se vea reflejada en todas sus actuaciones y la aplicación de medidas de forma tal que se logre el compromiso y respeto de su contenido por parte de todos los que la integran.

Este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad aplica igualmente para todo el Grupo Empresarial del que hace parte Pavimentos Colombia S.A.S., de acuerdo a lo contenido en el certificado de cámara de comercio de Bogotá.

CAPÍTULO I – DECLARACIÓN DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES.

La Política de Tratamiento de Datos Personales está dirigida a todos los actores que se relacionan de manera directa o indirecta con **LA ORGANIZACIÓN** o a quienes participan o deben tener conocimiento de las medidas incorporadas para dar cumplimiento a la Ley 1581 de 2012; por lo cual, está dirigida a los clientes, proveedores, accionistas, administradores y Titulares en los términos definidos por la Ley estatutaria, así como para los empleados y demás colaboradores de **LA ORGANIZACIÓN.**

La Política de Tratamiento de Datos Personales corresponde a los lineamientos, orientaciones o aspectos que fundamentan el manejo de los Datos Personales y las Medidas de Seguridad de la información en **LA ORGANIZACIÓN,** la cual ha sido elaborada en desarrollo de sus buenas costumbres y principios éticos, con la finalidad de establecer los lineamientos de **LA ORGANIZACIÓN** y como mínimo, los previstos en las disposiciones legales vigentes, en esta materia.

En desarrollo de la Política de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad, se declaran los siguientes lineamientos.

LA ORGANIZACIÓN MANIFIESTA QUE:

i. Reconoce que en todo momento deberá anteponer la observancia de los principios éticos al logro de las metas comerciales.

ii. Acatará las normas que se impartan en materia de tratamiento de Datos Personales, con el propósito no sólo de contribuir a la realización de los fines del Estado y de cumplir la Ley, sino de proteger los derechos de los Titulares.

iii. Cumplirá con las directrices emitidas por la Asamblea de Accionistas, la Junta Directiva (si fuera el caso) y la Gerencia, sobre el Tratamiento de Datos Personales.

iv. Cumplirá con las políticas de seguridad reguladas en el presente Manual y en el APÉNDICE BASES DE DATOS Y MEDIDAS DE SEGURIDAD , para el manejo de información física y electrónica o digital, y así mismo con las correspondientes medidas de seguridad y protección para el acceso remoto a la información.

v. Implementará acuerdos de confidencialidad, mediante los cuales garantizará la reserva de la información, inclusive después de finalizada la relación laboral con el personal que intervenga en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos.

vi. Divulgará en lo pertinente, el Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad, creado para asegurar el cumplimiento de la normativa legal. El nuevo personal de la Organización al momento de vincularse con la Organización, recibirá capacitación sobre protección de datos personales y seguridad de la información dejando constancia de su asistencia y conocimiento. Se asegurará que el personal de la Organización, contratistas y terceros conozcan sus responsabilidades con respecto a Protección de datos personales y seguridad de la información. Así mismo, desde el proceso de Gestión de Talento Humano, con el Oficial de Protección de Datos Personales u área encargada de la protección de datos personales, se definirán los planes de capacitación y evaluación de los empleados de acuerdo con los cambios normativos que se presenten.

vii. Informará a sus clientes, proveedores, empleados, colaboradores y en general a todo Titular, la existencia del Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad.

viii. Velará porque en el almacenamiento de la información entregada por sus Clientes, Proveedores y empleados, sea acorde al cumplimiento de las normas sobre Tratamiento de Datos Personales y medidas de seguridad y monitoreará su seguimiento.

ix. Colaborará con las autoridades en proveer la información que sea solicitada en el Tratamiento de Datos Personales y medidas de seguridad.

x. Colaborará y apoyará, en sus competencias con la política estatal para el Tratamiento de Datos Personales y medidas de seguridad.

xi. Apoyará y facilitará la atención de todo requerimiento de clientes, proveedores, empleados, colaboradores y en general a todo Titular sobre el manejo de la información.

xii. Velará por el correcto manejo y custodia de la información de todos los Titulares.

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN DE LA DECLARACIÓN DE POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES.

La presente Política de Tratamiento de Datos Personales es elaborada de conformidad con lo dispuesto en los artículos 15 y 20 de la Constitución Política; la Ley 1581 de 2012 (artículos 17 literal k y 18 literal f); el **Capítulo 25 del Decreto 1074 de 2015 (el cual compiló las disposiciones del Decreto 1377 de 2013);** las Circulares Externas 002 de 2015 y 005 de 2017 de la Superintendencia de Industria y Comercio; el Título V de la Circular Única de la Superintendencia de Industria y Comercio, y demás disposiciones complementarias. Esta política será aplicada por LA ORGANIZACIÓN respecto de la recolección, almacenamiento, uso, circulación, supresión y de todas aquellas actividades que constituyan Tratamiento de Datos Personales.

La ORGANIZACIÓN tiene como actividad principal, la prestación de servicios de construcción de obras civiles, producción de mezclas asfálticas y agregados pétreos y proyectos inmobiliarios que brindan de manera integral a clientes y demás partes interesadas, elevados niveles de eficiencia en el desarrollo de sus actividades, mediante un equipo humano altamente calificado, respaldado con capacidad financiera y tecnológica.

En virtud de sus relaciones contractuales, La ORGANIZACIÓN conoce información personal de los clientes, así como también conoce o puede llegar a conocer información personal de contacto de personas que no son sus clientes pero que podrían llegar a serlo, bien sea porque la persona se acerca a La ORGANIZACIÓN, para conocer sobre sus productos y servicios, o porque dentro del marco de contratación, dejan sus datos para ser contactados posteriormente.

Ahora bien, cuando en desarrollo de su objeto social La ORGANIZACIÓN busque acercarse a Titulares de Datos que no sean sus clientes o usuarios, pero que podrían llegar a serlo, y para ello utilicen los datos de contacto de tales Titulares estará actuando bajo el escenario de la Ley General. Igualmente, cuando soliciten, obtengan o administren información personal de Titulares con quienes tuvo en el pasado una relación contractual, pero esta ya expiró, estará bajo el marco de dicha Ley. Así como, cuando recopilen, administren y circulen información sobre sus proveedores y/o contratistas, candidatos a empleados, exempleados y empleados.

La ORGANIZACIÓN está comprometida en garantizar la protección de los derechos de Habeas Data, la privacidad, la intimidad y el buen nombre de todas las personas cuyos Datos Personales reposen en sus Bases de Datos. Las actuaciones en el manejo de Datos Personales se regirán por los principios de buena fe, legalidad, autodeterminación informática, libertad y transparencia, y todas aquellas contenidas en el numeral 3 del presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad.

Como consecuencia de la prestación de los servicios de La ORGANIZACIÓN, se transfiere y comparte información personal de los clientes actuales y potenciales que se encuentran en las Bases de Datos, así como de proveedores, empleados y demás personas naturales o jurídicas.

La Política será aplicable a las Bases de Datos que se encuentren bajo la administración de La ORGANIZACIÓN o sean susceptibles de ser conocidas por ésta en virtud de las relaciones comerciales desarrolladas de conformidad con su objeto social o en virtud de las relaciones comerciales desarrolladas a través de alianzas comerciales, de convenios o eventos publicitarios.

Así mismo, la Política será aplicable cuando el Tratamiento de los datos se efectúe en territorio colombiano o que en virtud de normas internacionales o tratados le sea aplicable la legislación colombiana.

Las bases de datos son sujetas a registro en el Registro Nacional de Bases de Datos de la SIC y de conformidad con el Decreto 1074 de 2015, artículo 2.2.2.26.3.3. y 2.2.2.26.3.1. De conformidad con la Circular de la SIC N° 001 de 11 de enero de 2017, los Responsables del Tratamiento de las bases de datos deberán actualizar en el Registro Nacional de Bases de Datos a partir de la inscripción de Bases de Datos, la información inscrita cuando haya Cambios Sustanciales dentro de los primeros diez

(10) días hábiles de cada mes y anualmente, entre el dos (2) de enero y el treinta y uno (31) de marzo, a partir del 2018. Dichos cambios sustanciales están definidos en la Circular Única de la SIC, Título V "Protección de Datos Personales", Capítulo 2, numeral 2.3., como *"(...) los que se relacionen con la finalidad de la base de datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de datos personales almacenados en cada base de datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información y la transferencia y transmisión internacional de datos personales"*.

Las Bases de Datos que se creen con posterioridad a ese plazo, deberán inscribirse **dentro de los dos (2) meses siguientes, contados a partir de su creación.**

De conformidad con la Circular Externa de la SIC N° 003 de 2018, dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de la inscripción de la Base de Datos, el Responsable del Tratamiento debe actualizar la información de los reclamos presentados por los Titulares y los incidentes de seguridad que afecte a la Base de Datos dentro del semestre calendario anterior. Asimismo, dentro de los primeros días (10) días hábiles de cada mes, las Bases de Datos registradas deben ser actualizadas si han tenido cambios sustanciales o anualmente entre el dos (2) de enero y el treinta y uno (31) de marzo.

- La Ley de Tratamiento de Datos Personales no se aplica a los Datos Personales siguientes:
- A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
- Las que tengan por finalidad la seguridad y defensa nacional, prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.
- Las que tengan como fin y contengan información de inteligencia y contrainteligencia.
- Las que contengan información periodística y otros contenidos editoriales
- Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

Este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad será aplicable a todos los Datos Personales registrados en Bases de Datos que sean objeto de Tratamiento por el Responsable del Tratamiento.

1.1. Marco Legal.

a) Constitución Política de Colombia, artículo 15, 20, 23 y 74.

b) Ley 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales".

c) Decreto 886 de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".

d) Decreto 1074 de 2015, ""Por medio del cual se expidió el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".

e) Circulares aplicables de la Superintendencia de Industria y Comercio.

f) Decreto 1759 de 2016, "Por el cual se modifica el artículo 2.2.2.26.3.1. del Decreto 1074 de 2015 – Decreto Único Reglamentario del Sector Comercio, Industria y Turismo".

g) Convención Americana sobre Derechos Humanos, artículo 11 y 13[1].

1 **Artículo 11.** Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Artículo 13. Libertad de Pensamiento y de Expresión

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) el respeto a los derechos o a la reputación de los demás, o

b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley

h) Declaración Universal de los Derechos Humanos artículo 12 y 19[2].

i) Pacto Internacional de Derechos Civiles y Políticos artículo 17 y 19[3].

a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional.

2 Artículo 12

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Artículo 19

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

3 Artículo 17

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

Artículo 19

1. Nadie podrá ser molestado a causa de sus opiniones.2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas.

1.2. Objeto.

La Declaración de Políticas y los procedimientos previstos buscan desarrollar de manera suficiente el derecho constitucional al habeas data que tienen todas las personas respecto de las cuales La ORGANIZACIÓN haya recogido, administre o conserve información de carácter personal contiene, entre otras, el conjunto de principios, reglas e instituciones determinado por la Ley para garantizar la efectividad del derecho fundamental de habeas data de los ciudadanos, cuyo objeto es asegurar el poder de decisión y el control que tienen los ciudadanos sobre la información que permita individualizarlos, concretamente sus Datos Personales, el Tratamiento y destino que se les da a los mismos.

La información en aplicación de las políticas acá presentadas, será tratada para asegurar a las personas naturales cuyos datos obran en nuestras Bases de Datos la integridad de su información y la eficacia de sus derechos.

El presente manual contiene los documentos, obligaciones e instrucciones, controles, garantías y procedimientos para el desarrollo de las actividades en materia de captura y Tratamiento de información personal con el fin de ser una herramienta de conocimiento y consulta para La ORGANIZACIÓN y los Titulares en el ejercicio de las funciones que involucren el manejo de Datos Personales.

2. DEFINICIONES LEY DE PROTECCIÓN DE DATOS -LEPD-.

- **Acceso Autorizado:** Autorización concedida a un Usuario para el uso de determinados recursos. En dispositivos automatizados es el resultado de una autentificación correcta, generalmente mediante el ingreso de Usuario y contraseña.
- **Autenticación:** Procedimiento de verificación de la identidad de un Usuario.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de Datos Personales.
- **Aviso de Privacidad:** Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus Datos

Personales, mediante la cual se le informa acerca de la existencia de la Declaración de Políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los Datos Personales.

- **Base de Datos:** Conjunto organizado de Datos Personales (de personas naturales) que es objeto de Tratamiento para una finalidad o varias finalidades determinadas.
- **Bases de Datos Automatizadas y No Automatizadas:** Hace referencia a los diferentes medios en los que se aloja la información, siendo los automatizados los que están digitalizados y los no automatizados los que se encuentran en formato físico.
- **Bases de Datos Originarias y Derivadas:** Las originarias son macro-conjuntos que agrupan la información de personas naturales que son administradas por el Responsable. Su nombre se consolida dependiendo del Titular, finalidad, forma de tratamiento y obligatoriedad legal de la misma y están sujetas a registro ante el RNBD. Las derivadas consisten en información que proviene o se desprende de las Bases de Datos Originarias. Son subgrupos o subcategorías de información que responde al desarrollo diario de las actividades de LA ORGANIZACIÓN y no están sujetas a registro pero sí a Inventario por el Oficial de Protección de Datos Personales.
- **Cajas Negras:** Sistemas en los que solo se conoce la entrada y la salida, pero no se entiende cómo se procesan los datos internamente. Son sistemas donde el usuario (y a veces ni siquiera sus desarrolladores) conoce las variables que ingresan y el resultado que generan, pero no los pasos intermedios que se ejecutan internamente.
- **Cambios Sustanciales:** Los que se relacionan con la finalidad de la Base de Datos, el Encargado del Tratamiento, los canales de atención al Titular, la clasificación o tipos de Datos Personales almacenados en cada Base de Datos, las medidas de seguridad de la información implementadas, la Política de Tratamiento de la Información y la transferencia y transmisión internacional de Datos Personales.
- **Comité de Protección de Datos Personales:** Conformado por la Gerencia Jurídica y la Dirección de Prevención de Riesgos.
- **Consulta:** Es la revisión que hace el Titular de los Datos Personales que se encuentren en las Bases de Datos de La ORGANIZACIÓN y que se logra a través de una petición del Titular, según los procedimientos establecidos en este documento.
- **Contraseña:** Seña secreta que permite el acceso a dispositivos, información o Bases de Datos antes inaccesibles. Se utiliza en la autentificación de Usuarios que permite el acceso autorizado.
- **Control de Acceso:** Mecanismo que permite acceder a dispositivos, información o Bases de Datos mediante la autentificación.
- **Copia de Respaldo:** Copia de los datos de una Base de Datos en un soporte que permita su recuperación.
- **Datos Biométricos:** Los Datos Biométricos son aquellos rasgos físicos, biológicos o de comportamiento de un individuo que lo identifican como único del resto de la población.
- **Dato Personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Datos personales de menores:** Pueden ser objeto de tratamiento, mediando la autorización correspondiente por los padres, guardianes o adultos responsables, siempre y cuando no se ponga en riesgo la prevalencia de sus derechos fundamentales e inequívocamente responda a la realización del principio de su interés superior.
- **Dato Privado:** El Dato Privado es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. Son considerados Datos Privados, entre otros, el correo electrónico personal, teléfono y celular personal, dirección de residencia, datos biográficos, filiación, firma manuscrita o digital, fórmula dactiloscópica, datos de acceso como contraseñas, claves, patrones. Llamadas telefónicas y mensajería instantanea. El contenido de correos electrónicos. La ubicación de una persona.
- **Dato Público:** Es el dato que no sea semiprivado, privado o sensible. Por su naturaleza, los Datos Públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. Son considerados Datos Públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión

u oficio y a su calidad de comerciante o de servidor público. Nombres y apellidos, tipo y número de identificación, fecha y lugar de nacimiento, estado civil, correo electrónico institucional, nacionalidad, teléfono y celular corporativo, dirección de trabajo, datos relativos a la actividad comercial y profesional.

- **Dato Semiprivado:** El Dato Semiprivado es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector, personas o a la sociedad en general, como el dato financiero y crediticio. Son considerados Datos Semiprivados, entre otros, datos de afiliación al Sistema integral de seguridad social: EPS, IPS, ARL, fechas de ingreso, retiro, datos financieros, crediticios y/o de carácter económico de las personas, datos patrimoniales de las personales, salario u honorarios, datos socioeconómicos como estrato, propiedad de vivienda, bienes muebles e inmuebles, ingresos, regresos, inversiones, acciones, datos de la historia laboral: fecha de ingreso y retiro, anotaciones, llamados de atención, etc. Datos relacionados con el nivel educativo, capacitaciones y/o historial académico de personas, datos de antecedentes judiciales y/o disciplinarios de las personas, datos de información tributaria de la persona.

- **Datos Sensibles:** Se entiende por Datos Sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación. Se encuentra prohibido su tratamiento a no ser que el Titular haya otorgado autorización expresa. Son considerados Datos Sensibles, entre otros, los datos biométricos de la persona (Huella, ADN, Videos, voz), siempre y cuando se pueda identificar ante un sistema de información, datos relacionados con la salud de la persona (pruebas, laboratorios, estudios, diagnósticos). Datos de preferencia, identidad y orientación sexual de la persona. Origen étnico- racial. Población en condición vulnerable. Datos sobre personas en situación de discapacidad. Datos relacionados con la pertenencia a sindicatos, organizaciones sociales, derechos humanos, religiosas, políticas, convicciones religiosas, filosóficas o políticas.

- **Delegados del Responsable del Tratamiento:** Áreas, Direcciones o Departamentos al interior de LA ORGANIZACIÓN que, por la naturaleza de sus funciones, administran o custodian Bases de Datos Personales. Estos actúan como garantes operativos y son responsables directos ante el Responsable del Tratamiento por la ejecución, vigilancia y cumplimiento efectivo de las políticas, procedimientos y medidas de seguridad establecidas en este Manual.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada (incluyendo de forma enunciativa pero no limitada a proveedores y subcontratistas), que por sí misma o en asocio con otros, realice el Tratamiento de Datos Personales por cuenta y nombre de LA ORGANIZACIÓN en virtud de una relación contractual o legal. En estos casos, LA ORGANIZACIÓN conserva su calidad de Responsable del Tratamiento, mientras que el Encargado asume la obligación de ejecutar sus labores bajo las instrucciones dadas por aquel, garantizando el cumplimiento estricto de las políticas, finalidades y medidas de seguridad contenidas en el presente Manual.

- **Finalidades:** Motivo o propósito por lo cual el Responsable da uso a la información de los Titulares. La Superintendencia de Industria y Comercio, establece una lista taxativa para determinar las finalidades con las cuales el Responsable da Tratamiento de los Datos Personales.

- **Identificación:** Proceso de reconocimiento de la identidad de los Usuarios.

- **Incidentes de Seguridad:** Se refiere a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado, que deberán reportarse al RNBD por parte de los Responsables del Tratamiento que se encuentran obligados a registrar sus bases de datos en el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

- **Niveles de Seguridad:** Medidas a tener en cuenta de acuerdo a la naturaleza del Dato Personal. Nivel alto corresponde a medidas para tratamiento de Datos Sensibles y nivel básico a medidas para tratamiento de Datos no considerados sensibles.

- **Oficial de Protección de Datos Personales:** Persona natural designada al interior de la empresa, como responsable de vigilar el cumplimiento del Sistema de Gestión de Datos Personales, especialmente, desde su estructuración, diseño y administración. El Oficial de Protección dará igualmente trámite a las solicitudes de los Titulares, para el ejercicio

de los derechos a que se refiere la Ley 1581 de 2012, el Decreto 1074 de 2015.

- **Perfil de Usuario:** Grupo de Usuarios a los que se da acceso.
- **Recolección:** Los Datos Personales conforman la información necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios.
- **Recurso Protegido:** Cualquier componente del sistema de información, como Bases de Datos, programas, soportes o equipos, empleados para el almacenamiento y Tratamiento de Datos Personales.
- **Responsable del Tratamiento:** Pavimentos Colombia S.A.S. o las sociedades que hacen parte del Grupo Empresarial.
- **Responsable de Seguridad:** Pavimentos Colombia S.A.S. o las sociedades que hacen parte del Grupo Empresarial, a través de la Dirección de Prevención de Riesgos.
- **Sistema de Información:** Conjunto de Bases de Datos, programas, soportes y/o equipos empleados para el Tratamiento de Datos Personales.
- **Sistemas de Tratamiento Mixto:** Se refiere al tratamiento de Bases de Datos Automatizadas y No Automatizadas.
- **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como el papel, la cinta de video, el CD, el DVD, el disco duro, etc.
- **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:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de Datos Personales, ubicado en Colombia, envía la información o los Datos Personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país. Es el envío de datos personales a un receptor que no actúa bajo nuestras órdenes, sino que se convierte en un nuevo Responsable (dueño) de esa información para sus propios fines. Ej: Enviamos los datos de nuestros empleados a la EPS o al Fondo de Pensiones. Una vez ellos reciben la información, ellos deciden cómo tratarla según sus propias políticas y obligaciones legales.
- **Transmisión:** Tratamiento de Datos Personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable. Es la comunicación de datos a un tercero (Encargado) para que realice un trabajo específico únicamente por cuenta y nombre de LA ORGANIZACIÓN. El tercero no puede usar los datos para nada más que para la tarea contratada. Ej: Contratamos a una empresa externa de seguridad o de software de nómina. Nosotros les "transmitimos" los datos para que ellos nos presten el servicio, pero ellos no pueden usar esos datos para venderles productos o contactarlos para otros fines; solo pueden usarlos para cumplir nuestro contrato y en respeto de las finalidades comunicadas y aceptadas por los Titulares.
- **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos. Se limita a consulta.
- **Usuario Autorizado:** Sujeto autorizado y responsable del control y manejo de la Base de Datos y el acceso a recursos, o proceso que accede a los datos o recursos para el Tratamiento de Datos Personales por cuenta del Responsable.

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

El artículo 4 de la Ley de Protección de Datos (LEPD), establece unos principios para el Tratamiento de Datos Personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley.

Los principios legales de la protección de datos son los siguientes:

- **Principio de Legalidad:** El Tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Ley de Protección de Datos (LEPD), y en las demás disposiciones que la desarrollen.

- **Principio de Finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

- **Principio de Libertad:** El Tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los Datos Personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El Tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad.

- **Principio de 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.

- **Principio de Transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del Responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al Titular, el Responsable del Tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

  - El Tratamiento al cual será sometidos sus datos y la finalidad del mismo.

  - El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre Datos Sensibles o sobre datos de niños, niñas o adolescentes.

  - Los derechos que le asisten como Titular.

  - La identificación, correo electrónico y teléfono del Responsable del Tratamiento.

- **Principio de acceso y circulación restringida:** El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los Datos Personales, de las disposiciones de la Ley de Protección de Datos (LEPD) y la Constitución Política. En este sentido, el Tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los Datos Personales, salvo la información pública, no podrán estar disponibles en internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

- **Principio de seguridad:** La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

  El Responsable del Tratamiento tiene la responsabilidad de implementar las medidas de seguridad correspondientes y de ponerlas en conocimiento de todo el personal que tenga acceso, directo o indirecto, a los datos. Los Usuarios que accedan a los sistemas de información del Responsable del Tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad y son de obligatorio cumplimiento para todo Usuario, Usuario Autorizado y personal de LA ORGANIZACIÓN.

  Cualquier modificación de las normas y medidas en materia de seguridad de Datos Personales por parte del Responsable del Tratamiento ha de ser puesta en conocimiento de los Usuarios.

- **Principio de confidencialidad:** Todas las personas que intervengan en el Tratamiento de Datos Personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo solo realizar suministro o comunicación de Datos Personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de esta.

- **Principio de necesidad y proporcionalidad:** Los Datos Personales registrados en una Base de Datos deben ser los estrictamente necesarios para el cumplimiento de las finalidades del Tratamiento, informadas al Titular. En tal sentido, deben ser adecuados,

pertinentes y acordes con las finalidades para los cuales fueron recolectados.

- **Principio de temporalidad o caducidad:** El período de conservación de los Datos Personales será el necesario para alcanzar la finalidad para la cual se han recolectado.

4. ALGUNAS CATEGORÍAS ESPECIALES DE DATOS.

4.1. Datos Sensibles.

Los Datos Sensibles son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los Datos Biométricos.

Según el artículo 6 de la LEPD, se prohíbe el Tratamiento de Datos Sensibles, excepto cuando:

- El Titular haya dado su Autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha Autorización.

- El Tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

- El Tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la Autorización del Titular.

- El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

- El Tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2. Derechos de los niños, niñas y adolescentes.

El Tratamiento de Datos Personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho Tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.

- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus Datos Personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus Datos Personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo Responsable y Encargado involucrado en el Tratamiento de los Datos Personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD. En todo caso, en el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas adolescentes se ejercerán por las personas que estén facultadas para representarlos.

5. AUTORIZACIÓN DEL TRATAMIENTO DE DATOS PERSONALES.

De acuerdo con el artículo 9 de la LEPD, para el Tratamiento de Datos Personales se requiere la autorización previa e informada del Titular, la cual se realiza mediante la aceptación del presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad. Todo Titular que facilite información relativa a sus Datos Personales está consintiendo el Tratamiento de sus datos por parte de LA ORGANIZACIÓN, en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una 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 de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

6. RESPONSABLE DEL TRATAMIENTO.

El Responsable del Tratamiento de las Bases de Datos objeto de este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad es PAVIMENTOS COLOMBIA S.A.S., cuyos datos de contacto son los siguientes:

- Dirección: Calle 84ª N° 10 - 50 Piso 9 Bogotá (Colombia)
- Correo electrónico: habeasdata@pavcol.com
- Teléfono: 3760030. Ext. 1135.

7. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES O ÁREA ENCARGADA DE LA PROTECCIÓN DE DATOS PERSONALES.

El Decreto 1074 de 2015 *"Por medio del cuál se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo"*[4], establece que se debe designar a un Oficial de Protección de Datos Personales, encargado de proteger los datos personales y vigilar la correcta implementación de las políticas de tratamiento de datos personales de la Organización.

El área que asume la función de protección de Datos Personales en LA ORGANIZACIÓN y que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581, el Decreto 1074 de 2015, será la **Gerencia Jurídica**. Asimismo, el **Oficial de Protección de Datos Personales** será responsable de consolidar y mantener un **Inventario de Evidencias de Responsabilidad Demostrada**, que incluya registros de capacitaciones, actas de atención de incidentes, y resultados de las auditorías semestrales, con el fin de acreditar ante la autoridad de control la efectividad real del Programa Integral de Gestión de Datos Personales. Las siguientes son sus funciones:

7.1. Gestión y Cumplimiento Normativo.

- **Implementación Efectiva:** Velar por la ejecución real de las políticas y procedimientos internos, asegurando la aplicación de buenas prácticas en la gestión de datos.
- **Integración Organizacional:** Integrar la protección de datos y las medidas de seguridad en el ADN de todas las áreas de la empresa.
- **Enlace Interno:** Actuar como el puente de comunicación y coordinación entre los diferentes departamentos de LA ORGANIZACIÓN.

4 ARTÍCULO 2.2.2.25.4.4. «Medios para el ejercicio de los derechos. Todo Responsable y Encargado deberá designar a una persona o área que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el presente capítulo».

7.2. Control de Riesgos y Auditoría

- **Sistema de Riesgos:** Promover y liderar la creación de un sistema que identifique y administre los riesgos asociados al tratamiento de información personal.

- **Controles del Programa:** Coordinar el diseño y la puesta en marcha de los controles necesarios para el Programa Integral de Gestión de Datos Personales.

- **Vigilancia y Seguimiento:** Realizar el seguimiento continuo del programa y asegurar la ejecución de planes de auditoría interna para verificar el cumplimiento de las políticas y medidas de seguridad.

7.3. Gestión de Inventarios y Registro

- **Inventario Clasificado:** Mantener un registro detallado de todas las bases de datos de LA ORGANIZACIÓN, clasificándolas según su tipo y sensibilidad de contenido.

- **Reporte ante la SIC:** Gestionar la inscripción, actualización y reporte de novedades de las bases de datos ante el Registro Nacional de Bases de Datos (RNBD), siguiendo las instrucciones de la Superintendencia de Industria y Comercio.

7.4. Relación con Terceros y Autoridades

- **Revisión Contractual:** Supervisar los contratos de transmisión de datos (nacionales o internacionales) que se firmen con Encargados (proveedores o subcontratistas) para asegurar que cumplan con la ley.

- **Atención a Autoridades:** Asistir y acompañar a LA ORGANIZACIÓN durante las visitas de inspección o ante cualquier requerimiento formal de la SIC.

7.5. Cultura y Atención al Titular.

- **Capacitación Continua:** Liderar programas de formación anual para los empleados, asegurando que conozcan sus responsabilidades legales.

- **Gestión de Habeas Data:** Administrar los canales oficiales para la recepción de consultas, quejas y reclamos (PQR).

- **Garantía de Respuesta:** Supervisar que cada solicitud de los titulares sea respondida de fondo, de manera clara y dentro de los términos que dicta la ley

8. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

LA ORGANIZACIÓN, en el desarrollo de su actividad empresarial, lleva a cabo el Tratamiento de Datos Personales relativos a personas naturales que están contenidos y son tratados en Bases de Datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

Las Bases de Datos de la Organización se encuentran incluidas en el APÉNDICE BASES DE DATOS Y MEDIDAS DE SEGURIDAD, el cual hace parte del presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad y las cuales serán sometidas a constante actualización por la Organización, sin por lo tanto requerir de la aprobación de la Asamblea de Accionistas.

8.1. Directrices para el uso de herramientas de Inteligencia Artificial (IA) Generativa.

LA ORGANIZACIÓN promueve la innovación y la eficiencia mediante el uso de herramientas de Inteligencia Artificial Generativa. Sin embargo, para garantizar el derecho al Habeas Data y la seguridad de la información, el uso de estas tecnologías se rige por las siguientes reglas:

- **Uso Exclusivo de Herramientas Corporativas:** Solo está permitido el tratamiento de información (incluyendo datos personales) a través de las herramientas de IA integradas en la suite corporativa de Google (Gemini, NotebookLM, etc.) vinculadas a la cuenta de correo institucional del empleado. Estas herramientas cuentan con niveles de protección y privacidad que garantizan que los datos no sean compartidos con terceros ni utilizados para el entrenamiento de modelos

públicos.

- **Prohibición de IA No Autorizada:** Queda estrictamente prohibido el uso de herramientas de IA externas o personales (versiones gratuitas o no autorizadas por la Dirección de Prevención de Riesgos) para procesar cualquier información de propiedad de LA ORGANIZACIÓN, especialmente bases de datos de empleados, clientes o proveedores.

- **Finalidad Estrictamente Laboral:** El uso de las herramientas de IA autorizadas debe estar vinculado exclusivamente al cumplimiento de las funciones laborales. Los datos ingresados deben ser pertinentes y limitados a la finalidad del cargo.

- **Gestión de Prompts (Comandos):** A pesar de la seguridad del entorno corporativo, el personal debe evitar ingresar datos innecesariamente sensibles en los prompts. Se debe preferir el uso de datos anonimizados o seudonimizados siempre que la tarea lo permita.

- **Derecho de Intervención Humana:** LA ORGANIZACIÓN garantiza que ninguna decisión administrativa o jurídica que afecte los derechos de un titular de datos será tomada de forma automatizada por la IA. Todo resultado generado por estas herramientas debe ser validado por un responsable humano antes de su aplicación.

9. SISTEMAS AUTOMATIZADOS Y TRANSPARENCIA ALGORÍTMICA.

9.1. Transparencia Algorítmica

La transparencia de tecnologías automatizadas es una expectativa creciente en el sector público y privado, especialmente con sistemas que procesan datos personales o tienen impacto en decisiones sobre personas. LA ORGANIZACIÓN utiliza, entre otros, los siguientes sistemas automatizados:

- **Fichajes biométricos** (huella digital) para control de asistencia.

- **Asignación automática de permisos o vacaciones** basada en reglas predefinidas.

- **Automatización de procesos repetitivos,** como notificaciones internas, envíos de correo e informes.

Para cumplir con los principios de transparencia, accountability y evitar Cajas Negras, la empresa documenta:

- La **finalidad** del tratamiento.

- Los **datos personales involucrados.**

- Las **áreas y responsables** del sistema.

Esta documentación está disponible internamente, y se mantiene actualizada para revisión y control interno.

9.2. Uso de herramientas con funcionalidades de inteligencia artificial (IA)

LA ORGANIZACIÓN informa que, en desarrollo de sus actividades, utiliza herramientas de productividad provistas por terceros, como la suite Microsoft 365, que integran funcionalidades de inteligencia artificial (IA).

Aunque LA ORGANIZACIÓN no desarrolla, entrena, ni opera directamente sistemas de IA propios, reconoce que el uso de estas herramientas puede implicar, en ciertos casos, el tratamiento incidental de datos personales contenidos en documentos, hojas de cálculo, comunicaciones o archivos utilizados por sus trabajadores.

En cumplimiento del principio de responsabilidad demostrada previsto en el artículo 17 de la Ley 1581 de 2012 y conforme a los lineamientos impartidos por la Superintendencia de Industria y Comercio en la Circular Externa No. 002 del 21 de agosto de 2024, LA ORGANIZACIÓN se compromete a:

- Verificar que los proveedores de estas herramientas cumplan con estándares adecuados de protección de datos personales.
- Promover el uso responsable de funcionalidades de IA.
- Capacitar al personal sobre las precauciones que deben observarse al utilizar herramientas de IA integradas en el entorno de trabajo.
- Abstenerse de utilizar dichas herramientas para la toma de decisiones automatizadas que afecten derechos de los titulares de datos personales.

En todo caso, la información personal eventualmente tratada mediante herramientas de IA estará sujeta a las garantías establecidas en este Manual, y su uso deberá respetar los principios de necesidad, proporcionalidad, finalidad, confidencialidad y seguridad de la información.

10. DERECHOS DE LOS TITULARES.

Los Titulares de los datos pueden ejercer una serie de derechos en relación con el Tratamiento de sus Datos Personales. Estos derechos podrán ejercerse por las siguientes personas:

a) Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el Responsable.

b) Por sus causahabientes, quienes deberán acreditar tal calidad.

c) Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.

d) Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas legalmente para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de Acceso o Consulta:** Se trata del derecho del Titular a ser informado por el Responsable del Tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus Datos Personales.
- **Derechos de Quejas y Reclamos:** La Ley distingue cuatro tipos de reclamos:

  - Reclamo de Corrección: El derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.

  - Reclamo de Supresión: El derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.

  - Reclamo de Revocación: El derecho del Titular a dejar sin efecto la Autorización previamente prestada para el Tratamiento de sus Datos Personales.

  - Reclamo de Infracción: El derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

- **Derecho de actualización:** El derecho del Titular a actualizar sus Datos Personales en cualquier momento.

- **Derecho a solicitar prueba de la Autorización otorgada al Responsable del Tratamiento:** Salvo cuando expresamente se exceptúe como requisito para el Tratamiento de conformidad con lo previsto en el artículo 10 de la LEPD. En caso de que el Titular lo requiera, puede solicitar el Formato VII *Solicitud de Prueba de Autorización para el Tratamiento de Datos*.

- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** El Titular o causahabiente solo podrá elevar esta queja una vez haya agotado el trámite de consulta o reclamo ante el Responsable del Tratamiento o Encargado del Tratamiento.

- **Derecho al olvido / Caducidad del Dato Negativo:** En ejercicio del derecho al habeas data, toda persona puede solicitar la supresión de sus datos personales que ya no sean necesarios conservar para fines legales o contractuales.

  Para ello, LA ORGANIZACIÓN adopta la siguiente política: (i) **Datos laborales y contractuales** necesarios (ej. históricos para seguridad social, nómina, obligaciones tributarias) se conservarán durante los plazos legales o contractuales. (ii) **Datos personales no obligatorios** (ej. información de contacto personal, evaluaciones internas) serán eliminados dentro de los seis **(6) meses posteriores** a la desvinculación, si no existe base legal o contractual para su retención. (iii) **Proveedores** pueden ejercer el mismo derecho después de la finalización de su vínculo contractual. (iv) Las solicitudes deben atenderse dentro de los **15 días hábiles,** conforme a la Ley 1581/2012. (v) Este derecho se fundamenta en el principio de **minimización de datos,** la jurisprudencia nacional sobre **caducidad de datos negativos,** y encuentra correspondencia con el **derecho de supresión del RGPD,** garantizando una gestión responsable y proporcional de la información personal

- **Derecho de Intervención Humana y Explicación:** El Titular tiene derecho a solicitar que una persona natural revise cualquier decisión tomada mediante el uso de herramientas de Inteligencia Artificial (IA) que afecte significativamente sus intereses, así como a recibir una explicación clara sobre la lógica aplicada por el algoritmo en dicho proceso.

11. ATENCIÓN A LOS TITULARES DE DATOS PERSONALES Y DISTRIBUCIÓN DE FUNCIONES AL INTERIOR DE LA ORGANIZACIÓN.

El Oficial de Protección de Datos Personales o área encargada de la protección de Datos Personales, Gerencia Jurídica, de la ORGANIZACIÓN será la encargada de recibir las peticiones, consultas y/o reclamos y ante el cual el Titular de los datos puede ejercer sus derechos enviando un correo electrónico a: habeasdata@pavcol.com o comunicándose al Teléfono: 3760030. Ext. 1135.

El Oficial de Protección de Datos Personales se encargará de redireccionar la petición, consulta y/o reclamo a los Usuarios Autorizados responsables de las Bases de Datos de la ORGANIZACIÓN o a los Encargados de Base de Datos objeto del requerimiento por cuenta del Responsable y realizará un seguimiento constante para asegurarse de que se dé respuesta y debido cierre a la solicitud en los términos legales incluidos en este manual y llevará un consolidado de todos los requerimientos de los Titulares.

Igualmente, en el **APÉNDICE BASES DE DATOS Y MEDIDAS DE SEGURIDAD** de este Manual, se encuentra a disposición de los Titulares la distribución de roles de los Delegados del Responsable del **Tratamiento,** en todo lo relacionado con la puesta en marcha del sistema descrito en el presente documento.

12. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR.

12.1. Derecho de Acceso o Consulta.

El Titular podrá consultar de forma gratuita sus Datos Personales en dos casos:

a) Al menos una vez cada mes calendario.

b) Cada vez que existan modificaciones sustanciales del Manual de Declaración de

Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, LA ORGANIZACIÓN solamente podrá cobrar al Titular gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el Responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a PAVIMENTOS COLOMBIA S.A.S., enviado mediante correo electrónico a habeasdata@pavcol.com, indicando en el asunto "ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a la dirección: Calle 84ª N° 10 - 50 Piso 9 Bogotá (Colombia).

En caso de que lo requiera, el Titular podrá solicitar el Formato I *Ejercicio del Derecho de Acceso o Consulta,* con el fin de que pueda diligenciar y dirigir su requerimiento.

La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la Base de Datos para recibir la información solicitada:

- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la Base de Datos o a la naturaleza del Tratamiento, ofrecido por LA ORGANIZACIÓN.

Una vez recibida la solicitud, la Gerencia Jurídica, como Oficial de Protección de Datos Personales u área encargada de la protección de Datos Personales, deberá diligenciar el Anexo I *Solicitudes de Acceso y Reclamos por los Titulares* con el fin de que quede constancia en la Organización de la solicitud del Titular.

LA ORGANIZACIÓN, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma, haciendo uso del Formato VIII *Atención al derecho de consulta* en caso de existir información a proporcionar al Titular o diligenciando el Formato IX *Atención al derecho de consulta* en caso de que esta no exista. En caso de que el Titular de la información haya solicitado prueba de Autorización del Tratamiento de Datos Personales, se le dará debida respuesta diligenciando el Formato XIII *Atención a la solicitud de prueba de autorización*.

Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

El Oficial de Protección de Datos Personales o área encargada de la protección de datos personales, Gerencia Jurídica, se asegurará de que se le dé debida respuesta al Titular dentro de los términos legales.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio, ante lo cual, si lo requiere, podrá solicitar al Responsable del Tratamiento el Formato V *Queja ante la Superintendencia de Industria y Comercio*.

12.2. Derechos de Quejas y Reclamos.

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a PAVIMENTOS COLOMBIA S.A.S. enviado mediante correo electrónico a habeasdata@pavcol.com, indicando en el asunto "ejercicio del derecho de queja o reclamo", o a través de correo postal remitido a la dirección: Calle 84ª N° 10 - 50 Piso 9 Bogotá (Colombia).

En caso de que lo requiera, el Titular podrá solicitar uno de los siguientes formatos con el fin de que pueda diligenciar y dirigir su requerimiento: (i) Formato II *Ejercicio del Derecho de Acceso o Consulta*, (ii) *Formato III Ejercicio del Reclamo de Supresión,* (III) *Formato IV Ejercicio del Reclamo por Infracción* y (VI) *Revocación de la Autorización.*

La solicitud en todo caso deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo 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.

Una vez recibida la solicitud, el Oficial de Protección de Datos Personales o área encargada de la protección de datos personales, Gerencia Jurídica, deberá diligenciar el Anexo I *Solicitudes de Acceso y Reclamos por los Titulares* con el fin de que quede constancia en la Organización de la solicitud del Titular.

Una vez recibido el reclamo completo, se incluirá en la Base de Datos una leyenda que diga *"reclamo en trámite"* y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

LA ORGANIZACIÓN, resolverá la petición de queja o reclamo en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma haciendo uso del Formato X *Atención al reclamo de corrección*, Formato XI *Atención al reclamo de supresión* y Formato XII *Atención al reclamo por infracción*.

Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

El Oficial de Protección de Datos Personales o área encargada de la protección de datos personales, Gerencia Jurídica, se asegurará de que se le dé debida respuesta al Titular dentro de los términos legales.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio, ante lo cual, si lo requiere, podrá solicitar al Responsable del Tratamiento el Formato V *Queja ante la Superintendencia de Industria y Comercio*.

CAPÍTULO II – DECLARACÍON DE POLÍTICAS INTERNAS DE SEGURIDAD.

13. BASE LEGAL Y ÁMBITO DE APLICACIÓN.

El derecho a la protección de los datos tiene como finalidad permitir a todas las personas conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o Bases de Datos. Este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política; en la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la ley de Protección de Datos Personales (LEPD).

Cuando el Titular de los datos presta su consentimiento para que estos formen parte de una Base de Datos de la ORGANIZACIÓN, pública o privada, ésta se hace Responsable del Tratamiento de estos datos y adquiere una serie de obligaciones como son la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el Titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consulta y reclamos.

Si bien, la responsabilidad del Tratamiento de los datos recae en la ORGANIZACIÓN Responsable del Tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio.

El personal de la ORGANIZACIÓN responsable del Tratamiento con acceso, directo o indirecto, a Bases de Datos que contienen Datos Personales ha de conocer el Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad y debe cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar por el cumplimiento de sus obligaciones de seguridad, LA ORGANIZACIÓN designa como Responsable de **Seguridad,** encargado de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad, a la **Dirección de Prevención de Riesgos.**

Este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad será aplicable a todos los Datos Personales registrados en Bases de Datos que sean objeto de Tratamiento por el Responsable del Tratamiento y se encuentra dirigida a todos los Usuarios de datos, que son tanto el personal propio como al personal externo de LA ORGANIZACIÓN.

Todos los Usuarios Autorizados o no, están obligados a cumplir con las medidas de seguridad establecidas para el Tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con LA ORGANIZACIÓN. El deber de confidencialidad, recogido en el artículo 4 literal h) de la ley de Protección de Datos (LEPD), se formaliza a través de la firma de un acuerdo de confidencialidad suscrito mediante el instrumento contractual que el Responsable estime pertinente entre el Usuario y el Responsable del Tratamiento.

- Dirección: Calle 84ª N° 10 - 50 Piso 9 Bogotá (Colombia)
- Correo electrónico: habeasdata@pavcol.com
- Teléfono: 3760030. Ext. 1135.

13.1. Cumplimiento y actualización.

Las Políticas internas de seguridad de la empresa son de obligatorio cumplimiento para todo el personal de LA ORGANIZACIÓN, con acceso a los sistemas de información que contengan Datos Personales.

Este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad debe ser sometido a permanente revisión y actualización siempre que se produzcan cambios en los sistemas de información, el sistema de Tratamiento, LA ORGANIZACIÓN o el contenido de la información de las Bases de Datos, que puedan afectar a las medidas de seguridad implementadas. Asimismo, la declaración debe adaptarse en todo momento a la normativa legal en materia de seguridad de Datos Personales.

14. RESPONSABLE DE LA SEGURIDAD.

El Responsable de la Seguridad en materia de *habeas data* es la Dirección de Prevención de Riesgos.

De acuerdo con la normativa sobre protección de datos, la designación del Responsable de Seguridad no exonera de responsabilidad al Responsable del Tratamiento o al Encargado del Tratamiento.

El Delegado Responsable de la Seguridad tiene las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el Responsable del Tratamiento y el Oficial de Protección de Datos Personales o área encargada de la protección de datos personales, Gerencia Jurídica en la difusión de las políticas de seguridad.

- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las Bases de Datos.

- Gestionar los permisos de acceso a los datos por parte de los Usuarios Autorizados.

- Habilitar el registro de Incidencias (Anexo III *Registro de Incidencias*) a todos los Usuarios para que comuniquen y registren las Incidencias relacionadas con la seguridad de los datos; así como acordar con el Responsable del Tratamiento y el Oficial de Protección de Datos Personales o área encargada de la protección de Datos Personales, Gerencia Jurídica, las medidas correctoras y registrarlas.

- Comprobar periódicamente, la validez y vigencia de la lista de Usuarios Autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización de estas políticas y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

- Recibir y analizar el informe de auditoría de este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad para elevar sus conclusiones y proponer medidas correctoras al Responsable del Tratamiento.

- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan Datos Personales.

15. MEDIDAS DE SEGURIDAD.

LA ORGANIZACIÓN, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, LA ORGANIZACIÓN, mediante la suscripción de los correspondientes otrosíes a los contratos existentes, ha requerido al Responsable de la Seguridad y Encargados del Tratamiento con los que trabaja la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el Tratamiento de los Datos Personales.

Las Bases de Datos son accesibles únicamente por las personas designadas por LA ORGANIZACIÓN o por los Usuarios Autorizados.

El Responsable de la Seguridad de LA ORGANIZACIÓN se encarga de gestionar los permisos de acceso a los Usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

Las medidas de seguridad deben ser objeto de divulgación entre el personal de la Organización, quien debe estar informado de las consecuencias de su incumplimiento y recibir capacitaciones anuales, manteniendo a disposición permanente un video de capacitación en la red de la Organización para acceso del personal.

Las medidas de seguridad de la Organización se encuentran en el **APÉNDICE BASES DE DATOS Y MEDIDAS DE SEGURIDAD,** el cual hace parte del presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad y las cuales serán sometidas a constante actualización por el Director de Prevención de Riesgos, sin por lo tanto requerir de la aprobación de la Asamblea de Accionistas.

16. FUNCIONES Y OBLIGACIONES DEL PERSONAL.

Todas las personas que intervienen en el almacenamiento, Tratamiento, consulta o cualquier otra actividad relacionada con los Datos Personales y sistemas de información de LA ORGANIZACIÓN, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

LA ORGANIZACIÓN, se encargará de informar a su personal de servicio de las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que estime pertinente. De igual modo, pone a disposición del personal el presente Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad para que puedan conocer la normativa de seguridad de la ORGANIZACIÓN y sus obligaciones.

LA ORGANIZACIÓN, cumple con el deber de información con la inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los Usuarios de sistemas de identificación y sistemas de información y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de LA ORGANIZACIÓN se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la empresa y, específicamente, por el contenido de este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad. Cuando un Usuario trate documentos o soportes que contiene Datos Personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad por parte del personal al servicio de LA ORGANIZACIÓN es sancionable de acuerdo a la relación jurídica y/o contractual existente entre el Usuario y la Organización.

Las funciones y obligaciones de los Usuarios de las Bases de Datos personales bajo responsabilidad de LA ORGANIZACIÓN son las siguientes:

- **Deber de Secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a Bases de Datos Personales y vincula tanto a Usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los Usuarios de la ORGANIZACIÓN no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones y deben velar por la confidencialidad e integridad de los mismos.

- **Funciones de control y autorizaciones delegadas:** El Responsable del Tratamiento puede delegar el Tratamiento de Datos a terceros, para que actúe como Encargado del Tratamiento, mediante un contrato de transmisión de datos o la inclusión de las cláusulas y disposiciones contractuales respectivas dentro del marco de la relación contractual existente.

- **Obligaciones relacionadas con las medidas de seguridad implementadas:**

  - Acceder a las Bases de Datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.

  - No revelar información a terceras personas ni a Usuarios no autorizados.

  - Observar las normas de seguridad y trabajar para mejorarlas.

  - No realizar acciones que supongan un peligro para la seguridad de la información.

- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo.

- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos y ante la existencia de Datos Sensibles, se procede a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de estos.

- **Deber de custodia de los soportes utilizados:** Obliga al Usuario Autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen Bases

de Datos identifican el tipo de información que contienen mediante un sistema de clasificación y son inventariados. En caso de existir información clasificada con nivel de seguridad sensible el sistema de clasificación solo debe ser comprensible para los Usuarios Autorizados a acceder a dicha información.

- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada Usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral.

- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la Organización.

- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los Usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el Usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el Usuario debe comunicarlo a la Dirección de Prevención de Riesgos .

- **Copias de respaldo y recuperación de datos:** La Dirección de Prevención de Riesgos realiza copias de seguridad de toda la información de Bases de Datos Personales de la Organización.

- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes son debidamente archivados con las medidas de seguridad mínimas requeridas para que terceros no autorizados no puedan acceder a ellas.

17. FUNCIONES Y OBLIGACIONES DE LA ORGANIZACIÓN EN MATERIA DE SEGURIDAD.

Las principales obligaciones de LA ORGANIZACIÓN en materia de seguridad son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en este Manual de Declaración de Políticas de Tratamiento de Datos Personales, Procedimientos y Medidas de Seguridad.

- Difundir el referido documento al personal de la Organización.

- Mantener la Declaración de Políticas de Seguridad interna actualizada y revisada siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la empresa, el contenido de la información de las Bases de Datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.

- Existencia de un Responsable de la Seguridad e identificación de los Usuarios Autorizados para acceder a las Bases de Datos.

- Cuidado que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.

- Verificar anualmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.

- Garantizar la existencia de una lista de Usuarios Autorizados y perfiles de usuario.

- Analizar las Incidencias registradas para establecer las medidas correctoras oportunas.

- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos dos veces al año, o de forma extraordinaria ante incidentes graves que afecten a la integridad de las bases de datos personales.

18. BASES DE DATOS Y SISTEMAS DE INFORMACIÓN.

Las Bases de Datos almacenadas y tratadas por LA ORGANIZACIÓN, deben indicar el nivel de seguridad y el sistema de Tratamiento de cada una de ellas, el cual se puede apreciar en el **APÉNDICE**

BASES DE DATOS Y MEDIDAS DE SEGURIDAD.

El Director de Prevención de Riesgos está encargado de desarrollar medidas de seguridad específicas para cada Base de Datos y el acceso a la información y a las instalaciones de la ORGANIZACIÓN.

El nombramiento del Responsable de la Seguridad no exonera al Responsable del Tratamiento o Encargado del Tratamiento de sus obligaciones.

Nota: Toda nueva Base de Datos Personales que sea creada debe ser reportada de manera inmediata al Oficial de Protección de Datos Personales o área encargada de la protección de datos personales, Gerencia Jurídica, para ser incluida en el respectivo Apéndice y reportada a la Superintendencia de Industria y Comercio. Las Bases de Datos que se creen deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación. Todas las áreas de la Organización encargadas de la administración de una Base de Datos Personales, deben reportar a más tardar la última semana de junio y última semana de diciembre de cada año, si existen Bases de Datos Personales que han sido eliminadas.

19. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENTES DE SEGURIDAD.

Un Incidente de Seguridad es toda violación de la seguridad que ocasione el acceso no autorizado, destrucción, pérdida, alteración accidental o ilícita de Datos Personales administrados por el Responsable del Tratamiento o por su Encargado. Es decir, cualquier circunstancia que afecte la confidencialidad, disponibilidad e integridad de los Datos Personales que son administrados por LA ORGANIZACIÓN.

Los Usuarios tienen la obligación de notificar los Incidentes de Seguridad de los que tengan conocimiento al Oficial de Protección de Datos Personales y al Responsable de la Seguridad, quienes se encargarán de su gestión y resolución y de registrarlos a través del diligenciamiento del Anexo III Registro de Incidencias. Algunos ejemplos de Incidencias son: la caída del sistema de seguridad informática que permita el acceso a los Datos Personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérdida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de Bases de Datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.

LA ORGANIZACIÓN, establece un procedimiento de notificación, gestión y respuesta de Incidentes de Seguridad con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las Bases de Datos que están bajo su responsabilidad.

Todos los Usuarios y Usuarios Autorizados responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, Tratamiento o consulta de las Bases de Datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de Incidentes de Seguridad.

El procedimiento de notificación, gestión y respuesta es el siguiente:

a) Cuando una persona tenga conocimiento de un Incidente de Seguridad que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa deberá comunicarlo, de manera inmediata, al Responsable de la Seguridad y al Oficial de Protección de Datos Personales, describiendo detalladamente el tipo de Incidente producido, e indicando las personas que hayan podido tener relación con el mismo, la fecha y hora en que se ha producido, la persona que notifica el Incidente, la persona a quién se le comunica y los efectos que ha producido.

b) Una vez comunicado el Incidente de Seguridad, se debe solicitar al Responsable de Seguridad un acuse de recibo en el que conste la notificación del Incidente.

c) LA ORGANIZACIÓN, crea un registro de Incidentes de Seguridad (Anexo III *Registro de Incidencias*) que debe ser diligenciado por el Director de Prevención de Riesgos o su equipo de trabajo, según el caso, la cual contiene: El tipo de Incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la Incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Responsable de Seguridad de la Base de Datos.

d) Todos los Usuarios y/o personas que deseen reportar una Incidencia deberán llenar el formato de Registro de Incidencias disponible en la Gerencia Jurídica y en cada una de las áreas que manejan una Base de Datos en la Organización, y enviar dicho formato al Oficial de Protección de Datos Personales o área encargada de la protección de Datos Personales y la Gerencia Jurídica, para guardar un consolidado de los Incidentes de Seguridad.

e) Cierre de Incidentes de Seguridad y seguimiento: El Responsable de la Seguridad junto con el Oficial de Protección de Datos Personales y las áreas que usen o requieren información, documentarán todo el proceso de gestión del incidente, incluyendo las acciones que fueron ejecutadas para remediar el Incidente de Seguridad.

El proceso de gestión no se dará por concluido hasta que la Dirección de Prevención de Riesgos emita una Certificación Técnica de Mitigación, que asegure que la vulnerabilidad detectada ha sido corregida. La documentación deberá incluir las acciones ejecutadas para remediar el incidente y las medidas preventivas adoptadas para evitar su repetición.

f) El Oficial de Protección de Datos Personales, deberá reportar cualquier violación a los códigos de seguridad de las Bases de Datos al Registro Nacional de Bases de Datos dentro de los **15 días hábiles** siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.

g) El Oficial de Protección de Datos Personales debe garantizar que se tomen acciones para investigar y diagnosticar las causas que generaron el Incidente de Seguridad, apoyado por el Responsable de Seguridad. En caso de que se identifique un delito informático en términos de la Ley 1273 de 2009, el Oficial de Protección de Datos Personales reportará la información a las autoridades judiciales respectivas.

Durante los procesos de investigación se debe garantizar la Cadena de Custodia y preservarla en caso de requerirse acción legal.

Finalmente, se implementan procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

20. TRANSFERENCIA DE DATOS A TERCEROS PAÍSES.

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de Datos Personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.

- Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.

- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.

- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.

- Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de Datos Personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de Datos Personales que se efectúen entre un Responsable y un Encargado para permitir que el Encargado realice el Tratamiento por cuenta del Responsable, no requerirán ser informadas al Titular ni contar

con su consentimiento, siempre que exista un contrato de transmisión de Datos Personales.

De conformidad con la Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio y el artículo 26 de la Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales.”, hay 3 supuestos que habilitan la transferencia internacional de datos personales, a saber:

(i) El país receptor ofrece un nivel adecuado de protección, de acuerdo con los estándares fijados por la Superintendencia de Industria y Comercio, que no podrán ser inferiores a los dispuestos en la ley.

(ii) La operación de transferencia se encuentra enmarcada dentro de las excepciones fijadas por el artículo 26.

(iii) La Superintendencia de Industria y Comercio profiere una declaración de conformidad relativa a la viabilidad de la transferencia internacional de datos personales que en concreto se somete a su consideración.

Mediante Sentencia C-748 de 2011, la Corte Constitucional precisó las condiciones que la Superintendencia de Industria y Comercio debe considerar para fijar los estándares del nivel adecuado de protección de un país receptor de datos personales transferidos desde Colombia.

El simple tránsito transfronterizo de datos no comporta una transferencia de datos a terceros países. El tránsito transfronterizo de datos se refiere al simple paso de los datos por uno o varios territorios utilizando la infraestructura compuesta por todas las redes, equipos y servicios requeridos para alcanzar su destino final.

21. VIGENCIA.

Las Bases de Datos responsabilidad de la ORGANIZACIÓN, serán objeto de Tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del Tratamiento, y sin perjuicio de normas legales que dispongan lo contrario, la ORGANIZACIÓN, procederá a la supresión de los Datos Personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación.

Por todo esto, dicha Base de Datos ha sido creada sin un periodo de vigencia definido.

Este manual fue revisado y actualizado en marzo de 2026 para integrar los criterios de responsabilidad demostrada y transparencia algorítmica exigidos por la Superintendencia de Industria y Comercio.

APÉNDICE BASES DE DATOS Y MEDIDAS DE SEGURIDAD.

Ingrese al documento aquí

PAVIMENTOS COLOMBIA S.A.S.

MANUAL HABEAS DATA

Manual de declaración de políticas de tratamiento de datos personales, procedimientos y medidas de seguridad.

Versión No. 6

Marzo de 2026

2026