


Contenido

| | |
|--|----|
| 1. MARCO LEGAL Y AMBITO DE APLICACIÓN..... | 3 |
| 2. ALCANCE..... | 3 |
| 3. NORMATIVIDAD APLICABLE..... | 3 |
| 4. DEFINICIONES..... | 4 |
| 5. PRINCIPIOS DE LA PROTECCIÓN DE DATOS..... | 5 |
| 5.1. PRINCIPIO DE LEGALIDAD..... | 5 |
| 5.2. PRINCIPIO DE FINALIDAD..... | 5 |
| 5.3. PRINCIPIO DE LIBERTAD..... | 5 |
| 5.4. PRINCIPIO DE VERACIDAD O CALIDAD..... | 6 |
| 5.5. PRINCIPIO DE TRANSPARENCIA..... | 6 |
| 5.6. PRINCIPIO DE ACCESO Y CIRCULACIÓN RESTRINGIDA..... | 6 |
| 5.7. PRINCIPIO DE SEGURIDAD..... | 6 |
| 5.8. PRINCIPIO DE CONFIDENCIALIDAD..... | 7 |
| 6. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO..... | 7 |
| 7. RESPONSABLE DEL TRATAMIENTO..... | 7 |
| 8. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS..... | 8 |
| 9. DERECHOS DE LOS TITULARES..... | 8 |
| 9.1. DERECHO DE ACCESO O CONSULTA..... | 8 |
| 9.2. DERECHOS DE QUEJAS Y RECLAMOS..... | 8 |
| 9.3. DERECHO A SOLICITAR PRUEBA DE LA AUTORIZACIÓN OTORGADA AL RESPONSABLE DEL TRATAMIENTO..... | 9 |
| 9.4. DERECHO A PRESENTAR ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO QUEJAS POR INFRACCIONES..... | 9 |
| 10. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL..... | 9 |
| 11. TRATAMIENTO DE DATOS DE MENORES DE EDAD..... | 9 |
| 12. ATENCIÓN A LOS TITULARES DE DATOS..... | 10 |
| 13. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR..... | 10 |
| 13.1. DERECHOS DE ACCESO O CONSULTA..... | 10 |
| 13.2. DERECHOS DE QUEJAS Y RECLAMOS..... | 11 |
| 14. MEDIDAS DE SEGURIDAD..... | 12 |


Elaborado por
Oficial de Cumplimiento
Maria Isabel Bedoya Sierra

Revisado por
Director de Proyectos
Jorge Iván Granados Segua

Aprobado por
Representante legal
Lizeth Jimena Rosillo

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 2 de 21 |

| | | |
|-----|---|----|
| 15. | PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS..... | 16 |
| 16. | ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS..... | 18 |
| 17. | ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES..... | 19 |
| 18. | TRANSFERENCIA DE DATOS A TERCEROS PAISES..... | 19 |
| 19. | REGISTRO NACIONAL DE BASES DE DATOS – RNBD..... | 20 |
| 20. | SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES. | 20 |
| 21. | GESTIÓN DE DOCUMENTOS..... | 20 |
| 22. | VIGENCIA..... | 21 |

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 3 de 21 |

1. MARCO LEGAL Y AMBITO DE APLICACIÓN.

Las políticas de tratamiento de la información se desarrollan en cumplimiento de los artículos 15 y 20 de la **Constitución Política**; de los artículos 17 literal k) y 18 literal f) de la **Ley Estatutaria 1581 de 2012**, por la cual se dictan disposiciones generales para la Protección de Datos Personales (**LEPD**), del artículo 2.2.2.25.1.1 sección 1 capítulo 25 del **Decreto 1074 de 2015**, el cual, reglamenta parcialmente la **Ley 1581 de 2012** (Artículo 13 del Decreto 1377 de 2013).

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.


2. ALCANCE.

El presente documento aplicará para todos aquellos datos personales o de cualquier otro tipo de información que sea utilizada o repose en las bases de datos y archivos en las bases de datos de GEOSINC S.A.S., en adelante **LA COMPAÑÍA** respetando los criterios para la obtención, recolección, uso, tratamiento, procesamiento, intercambio, transferencia y transmisión de datos personales, y fijar las responsabilidades de **LA COMPAÑÍA** y de sus empleados en el manejo y tratamiento de los datos personales que reposen en sus bases de datos y archivos.

3. NORMATIVIDAD APLICABLE.

- **Artículo 15 de la Constitución Política:** Derecho a la intimidad personal, familiar y al buen nombre.
- **Ley 1266 de 2008:** Habeas Data – Bases de datos personales, crediticia y comercial (Financiero).
- **Ley Estatutaria 1581 de 2012:** Marco general de la protección de los datos personales en Colombia.
- **Decreto 1377 de 2013:** Reglamenta parcialmente la Ley 1581 de 2012.
- **Decreto 886 de 2014:** Reglamenta el artículo 25 de la Ley 1581 de 2012 referente al Registro Nacional de Bases de Datos (RNBD).
- **Decreto 1074 de 2015:** Por medio del cual se expide el Decreto Único Reglamentario del sector comercio, industria y turismo.

| | | |
|--|--|--|
| Elaborado por Oficial de Cumplimiento Maria Isabel Bedoya Sierra | Revisado por Director de Proyectos Jorge Iván Granados Segua | Aprobado por Representante legal Lizeth Jimena Rosillo |
|--|--|--|

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 4 de 21 |

4. DEFINICIONES.

Las siguientes definiciones se encuentran establecidas en el **artículo 3 de la LEPD y artículo 2.2.2.25.1.3 sección 1 Capítulo 25 del decreto 1074 de 2015** (Artículo 3 del decreto 1377 de 2013).

AUTORIZACIÓN: Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.

BASE DE DATOS: Conjunto organizado de datos personales que sea objeto de tratamiento.


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

DATO 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 o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

DATO PRIVADO: Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.

DATO SENSIBLE: Se entiende por datos sensibles 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.

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.

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 5 de 21 |

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/o el tratamiento de los datos.

OFICIAL DE PROTECCIÓN DE DATOS: Es la persona natural que asume la función de coordinar la implementación del marco legal en 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.

TITULAR: Persona natural cuyos datos personales sean objeto de tratamiento.

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.

TRANSMISIÓN: Tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento determinado por el encargado por cuenta del responsable.

5. PRINCIPIOS DE LA PROTECCIÓN DE DATOS.

El artículo 4 de la 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:

5.1. PRINCIPIO DE LEGALIDAD.


El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 Compilado en el Capítulo 25 del Decreto 1074 de 2015 y en las demás disposiciones que la desarrollen.

5.2. 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.

5.3. 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.

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 6 de 21 |

5.4. 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.

5.5. 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 de este.
El carácter facultativo de la respuesta del titular a las preguntas que le sean hechas cuando estas traten sobre datos sensibles o sobre datos niños, niñas o adolescentes.
- Los derechos que le asisten como titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

5.6. 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 LEPD y la Constitución. 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.

5.7. 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 implantar 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 Manual Interno de Seguridad, de obligado cumplimiento para todo usuario y personal de la empresa. 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.

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 7 de 21 |

5.8. 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.

6. AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO.

De acuerdo con el artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte del **LA COMPAÑÍA** 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 Personas.

7. RESPONSABLE DEL TRATAMIENTO.

El responsable del tratamiento de las bases de datos objeto de esta política es el **LA COMPAÑÍA** cuyos datos de contacto son los siguientes:

- Dirección: Autopista Medellín Kilometro 2.5 Parque industrial Portos Sabana 80 Bodega 106, Cota – Cundinamarca
- Correo electrónico: transparencia@geosinc.com.co
- Teléfono: (310) 5775411

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 8 de 21 |

8. TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS.

LA COMPAÑÍA 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. El “Anexo 1 denominado Organización Bases de Datos”, contiene la información relativa a las distintas bases de datos responsabilidad de la empresa y las finalidades asignadas a cada una de ellas para su tratamiento.

9. DERECHOS DE LOS TITULARES.

De acuerdo con el **artículo 8 de la LEPD, artículo 2.2.2.25.4.1 sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículos 21 y 22 del Decreto 1377 de 2013)**, 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:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas y adolescentes (**NNA**) se ejercerán por las personas que estén facultadas para representarlos.


9.1. DERECHO DE ACCESO O CONSULTA.

Se trata del derecho del titular a ser informado por el responsable del tratamiento, previa solicitud, respecto de origen, uso y finalidad que les han dado a sus datos personales.

9.2. DERECHOS DE QUEJAS Y RECLAMOS.

La Ley distingue cuatro tipos de reclamos:

- **RECLAMO DE CORRECCIÓN:** El derecho del titular a que se actualicen rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento este 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

| | | | |
|---|---|---------|---------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 9 de 21 |

incumplimiento de la normativa en materia de Protección de Datos.

9.3. 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**.

9.4. DERECHO A PRESENTAR ANTE LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO QUEJAS POR INFRACCIONES.

El titular o causahabiente solo podrá elevar ante la SIC – Superintendencia de Industria y Comercio la petición (queja), una vez haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

10. SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL.


Con antelación y/ al momento de efectuar la recolección del dato personal, **LA COMPAÑÍA** solicitará al titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el **artículo 2.2.2.25.2.2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 7 del Decreto 1377 de 2013)**.

11. TRATAMIENTO DE DATOS DE MENORES DE EDAD.

De acuerdo con el artículo 7° de la Ley 1581 de 2012, el Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo lo dispuesto en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013) y en cumplimiento de los siguientes parámetros y 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 **LA COMPAÑÍA** solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. El 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, aplicando los principios y obligaciones establecidas en la **Ley 1581 de 2012** y normas reglamentarias.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 10 de 21 |

12. ATENCIÓN A LOS TITULARES DE DATOS.

MARIA ISABEL BEDOYA SIERRA, identificada con cedula de ciudadanía **No. 32.299.922**, Oficial de Cumplimiento de **LA COMPAÑÍA** será la encargada de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos.

A los siguientes contactos:

- Dirección: Autopista Medellín Kilometro 2.5 Parque industrial Portos Sabana 80 Bodega 106, Cota – Cundinamarca
- Correo electrónico: transparencia@geosinc.com.co
- Teléfono: (310) 5775411

13. PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR.

13.1. DERECHOS DE ACCESO O CONSULTA.

Según el artículo 2.2.2.25.4.2. Sección 4 capítulo 25 del Decreto 1074 de 2015 (Artículo 21 del Decreto 1377 de 2013), el Titular podrá consultar de forma gratuita sus datos personales en dos casos:


- Al menos una vez cada mes calendario.

Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, **LA COMPAÑÍA** 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, **LA COMPAÑÍA** demostrará 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 **LA COMPAÑÍA** enviado, mediante correo electrónico a: transparencia@geosinc.com.co indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a la Autopista Medellín Kilometro 2.5 Parque industrial Portos Sabana 80 Bodega 106, Cota – Cundinamarca. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos completos del titular.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 11 de 21 |

- Fotocopia de la cedula de ciudadanía del titular, y en su caso, por la persona que lo esté representando, además de enviar el documento de poder o mandato acreditando 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:

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por **LA COMPAÑÍA**.


Una vez recibida la solicitud por **LA COMPAÑÍA** resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de esta. 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**.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

13.2. DERECHOS DE QUEJAS Y RECLAMOS.

El titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a **LA COMPAÑÍA** enviado, mediante correo electrónico a transparencia@geosinc.com.co indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a la Autopista Medellín Kilometro 2.5 Parque industrial Portos Sabana 80 Bodega 106, Cota – Cundinamarca. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos completos del titular.
- Fotocopia de la cedula de ciudadanía del titular, y en su caso, por la persona que lo esté representando, además de enviar el documento de poder o mandato acreditando 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 quieren ejecutar, cuando corresponda.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 12 de 21 |

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 recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga “reclamo en trámite” y el motivo de este, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

LA COMPAÑÍA resolverá la petición de reclamo en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de esta. 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.

Una vez agotado el trámite de reclamo, el titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio – SIC.

14. MEDIDAS DE SEGURIDAD.

LA COMPAÑÍA 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 a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, **LA COMPAÑÍA** mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación, se exponen las medidas de seguridad implantadas por **LA COMPAÑÍA** que están recogidas y desarrolladas en su Manual Interno de Seguridad (Tablas 1, 2, 3 y 4)


| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 13 de 21 |

TABLA 1.

| MEDIDAS DE SEGURIDAD GENERALES | |
|---|---|
| GESTIÓN DE DOCUMENTOS Y SOPORTES | <ol style="list-style-type: none"> 1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes. |
| CONTROL DE ACCESO | <ol style="list-style-type: none"> 1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado. |
| INCIDENCIAS | <ol style="list-style-type: none"> 1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias. |
| PERSONAL | <ol style="list-style-type: none"> 1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación al personal de las normas y de las consecuencias del incumplimiento de estas. |
| MANUAL INTERNO DE SEGURIDAD | <ol style="list-style-type: none"> 1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento. |


| | | | |
|---|---|----------------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 14 de 21 |

TABLA 2.

| MEDIAS DE SEGURIDAD SEGÚN EL TIPO DE BASE DE DATOS | | |
|---|---------------------|--|
| ARCHIVO | Física | Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y permitan el ejercicio de los derechos de los Titulares. |
| ALMACENAMIENTO DE DOCUMENTOS | Física | Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas. |
| CUSTODIA DE DOCUMENTOS | Física | Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de estos. |
| IDENTIFICACIÓN Y AUTENTICACIÓN | Automatizada | <ol style="list-style-type: none"> 1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado. |
| TELECOMUNICACIONES | Automatizada | Acceso a datos mediante redes seguras. |



| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 15 de 21 |

TABLA 3.

| MEDIAS DE SEGURIDAD -DATOS PRIVADOS | | |
|--|---------------------------------|--|
| AUDITORÍA | Automatizada- Física | <ol style="list-style-type: none"> 1. Auditoría ordinaria (interna o externa) cada seis meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. |
| RESPONSABLE DE SEGURIDAD | Automatizada- Física | <ol style="list-style-type: none"> 1. Designación de uno o varios responsables de administrar las bases de datos. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en los responsables de administrar las bases de datos. |
| MANUAL INTERNO DE SEGURIDAD | Automatizada- Física | Controles periódicos de cumplimiento. |
| GESTIÓN DE DOCUMENTOS Y SOPORTES | Automatizada | Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega. |
| CONTROL DE ACCESO | Automatizada | Control de acceso al lugar o lugares donde se ubican los sistemas de información. |
| IDENTIFICACIÓN Y AUTENTICACIÓN | Automatizada | Mecanismo que limite el número de intentos reiterados de acceso no autorizados. |
| INCIDENCIAS | Automatizada | <ol style="list-style-type: none"> 1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación. |


TABLA 4.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 16 de 21 |

| MEDIAS DE SEGURIDAD - DATOS SENSIBLES | | |
|--|---------------------------------|--|
| CONTROL DE ACCESO | Automatizada- Física | <ol style="list-style-type: none"> 1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados. 4. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 5. Control mensual del registro de accesos por el responsable de administrar las bases de datos. |
| ALMACENAMIENTO DE DOCUMENTOS | Física | Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. |
| COPIA O REPRODUCCIÓN | Física | <ol style="list-style-type: none"> 1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos. |
| TRASLADO DE DOCUMENTACIÓN | Física | Medidas que impidan el acceso o manipulación de documentos. |
| GESTIÓN DE DOCUMENTOS Y SOPORTES | Automatizada | <ol style="list-style-type: none"> 1. Definición de perfiles de usuarios acordes con su función. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando se encuentren fuera. |
| TELECOMUNICACIONES | Automatizada | Transmisión de datos mediante redes electrónicas cifradas. |

15. PROCEDIMIENTOS DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS.

LA COMPAÑÍA establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la


| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 17 de 21 |

información contenida en las bases de datos que están bajo su responsabilidad.

Todos los usuarios y 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 incidencia.

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

- Cuando una persona tenga conocimiento de una incidencia (perdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
- Una vez comunicada la incidencia ha de solicitar al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- **LA COMPAÑÍA** crea un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de esta, 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 Oficial de Protección de Datos, remitirse al Registro de incidencias y plan de acción.
- Asimismo, debe implementar los procedimientos para la recuperación de los datos cuando aplica, 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.
- Adicional, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 18 de 21 |

Finalmente, **LA COMPAÑÍA** notificará del incidente a los titulares, cuando se identifique que puedan verse afectados de manera significativa.


16. ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS.

LA COMPAÑÍA ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas, mediante la implementación de las políticas internas de seguridad. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

El sistema de gestión de riesgos determinará las fuentes tales como: tecnología, recurso humano, infraestructura y procesos que requieren protección, sus vulnerabilidades y las amenazas, con el fin de valorar su nivel de riesgo. Por lo que, para garantizar la protección de datos personales se tendrá en cuenta el tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso. Asimismo, se observará la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial), tales como:

- **Criminalidad:** Entendida como las acciones, causadas por la intervención humana, que violan la Ley y que se encuentran tipificadas en el Código Penal Colombiano.
-
- **Sucesos de origen físico:** Entendidos como en los eventos naturales y técnicos, así como, los eventos indirectamente causados por la intervención humana.
- **Negligencia y decisiones institucionales:** Entendidos como las acciones, decisiones u omisiones por parte de las personas que tienen poder e influencia sobre el sistema. Al mismo tiempo son las amenazas menos predecibles porque están directamente relacionado con el comportamiento humano.

LA COMPAÑÍA en el sistema de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 19 de 21 |

17. ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES.


Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten al **LA COMPAÑÍA** acceso y/o entrega de datos de carácter Personal contenidos en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad, y se suscribirá acta de la entrega de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

18. TRANSFERENCIA DE DATOS A TERCEROS PAISES.

- 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 **Ley 1581 de 2012** exige a sus destinatarios. Esta prohibición no regirá cuando se trate de Información de empleados remitidas con la finalidad de recursos humanos, celebraciones y cumpleaños, gestión de claves, administración de usuarios, soporte técnico, bienestar social, seguridad y salud en el trabajo, condiciones de trabajo.
- 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 Republica 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 salvaguardar el interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Se debe tener en cuenta que, 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.

Las transmisiones internacionales de datos personales que se efectúen en **LA COMPAÑÍA** y un encargado para permitir que dicho encargado realice el tratamiento por cuenta del responsable, no requerirán se informadas al titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 20 de 21 |

19. REGISTRO NACIONAL DE BASES DE DATOS – RNBD.

El término para registrar las bases de datos en el **RNBD** será el establecido legalmente. Asimismo, de acuerdo con el **artículo 12 del Decreto 886 de 2014**, los responsables del Tratamiento deberán inscribir sus bases de datos en el **Registro Nacional de Bases de Datos** en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. 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.

20. SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES.


El cumplimiento del marco normativo en **Protección de Datos Personales**, la seguridad, reserva y/o confidencialidad de la información almacenada en las bases de datos es de vital importancia para **LA COMPAÑÍA**. Por ello, hemos establecido políticas, lineamientos y procedimientos y estándares de seguridad de la información, los cuales podrán cambiar en cualquier momento ajustándose a nuevas normas y necesidades de **LA COMPAÑÍA** cuyo objetivo es proteger y preservar la integridad, confidencialidad y disponibilidad de la información y datos personales.

Asimismo, garantizamos que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

En caso de ser necesario suministrar información a un tercero por la existencia de un vínculo contractual, suscribimos contrato de transmisión para garantizar la reserva y confidencialidad de la información, así como, el cumplimiento de la presente Política del tratamiento de los datos, de las políticas y manuales de seguridad de la información y los protocolos de atención a los titulares establecidos por el **LA COMPAÑÍA**. En todo caso, adoptamos compromisos para la protección, cuidado, seguridad y preservación de la confidencialidad, integridad y privacidad de los datos almacenados.

21. GESTIÓN DE DOCUMENTOS.

Los documentos que contengan datos personales deben ser fácilmente recuperables, es por ello que se debe dejar documentado el lugar donde reposa cada uno de los documentos tanto físicos como digitales, se deben hacer inspecciones a estas rutas de almacenamiento de forma frecuente, se debe garantizar su conservación dejando definido en que soporte y bajo qué condiciones se llevará a cabo esta conservación, teniendo en cuenta condiciones ambientales, lugares de almacenamiento, riesgos a los cuales están expuestos entre otros, el tiempo de retención de los documentos se determina en función de los requisitos legales si aplica, de lo contrario cada organización lo define de acuerdo a sus necesidades, así mismo debe tener clara la disposición final de los mismos, identificando si se recicla,

| | | | |
|---|---|---------|----------|
|  | DOCUMENTO INTERNO DE POLÍTICAS Y PROCEDIMIENTOS (POLÍTICAS DE TRATAMIENTO) | VERSIÓN | 01 |
| | | PÁGINA | 21 de 21 |

reutiliza, se conserva, se digitaliza entre otros.

Los documentos que tienen que ver con la protección de datos personales deben ser elaborados por personal o una entidad competente para ello, así mismo la organización debe ser quien revise y apruebe todos los documentos y lo deje registrado en la casilla de aprobación de los documentos.

A fin de que sean fácilmente trazables, los documentos deberán estar codificados, serán actualizados y modificados por el personal responsable, esta modificación se efectuara siempre y cuando sea necesario, para la eliminación de un documento se debe tener la justificación para ello descrita en el histórico el cual se encuentra en la parte inferior de todos los documentos.

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su contenido, siguiendo los lineamientos descritos en el Manual Interno de Políticas de Seguridad.

La distribución de los documentos que contengan datos personales la efectuara el responsable del tratamiento, este dejará documentada la evidencia de dicha distribución, donde entre otros se especifique; el tipo de documento y la identificación de la persona a la cual se le entregó la información.

Se deberá designar un responsable de garantizar la confidencialidad de los datos personales de los titulares, este será quien custodie documentos, garantice su protección tanto física como digital, evite alteraciones de la información, así mismo garantizará que los documentos que salgan de su custodia sean identificados y fácilmente trazables.

22. VIGENCIA.

Las bases de datos responsabilidad de LA **COMPAÑÍA** 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 COMPAÑÍA** 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 ello, dichas bases de datos han sido creadas sin un periodo de vigencia definido.

La presente política de tratamiento entrara en vigor desde el mismo instante que sea publicada para la Contraparte empleados del **LA COMPAÑÍA**.