TABLA DE CONTENIDO

1. OBJETIVO

En línea con el valor corporativo de Integridad, la Transportadora de Gas Internacional TGI S.A. ESP. (en adelante "TGI" o la "Organización") se encuentra comprometida con el adecuado tratamiento de los datos personales de sus titulares de la información, y por esto, reconoce la vital importancia contar con un Manual Interno de Políticas y Procedimientos para la Protección de Datos Personales, mediante el cual se establezcan los lineamientos corporativos generales para una adecuada implementación, aplicación, monitoreo, sostenimiento y mejora continua de las políticas y procedimientos relacionados con el adecuado tratamiento de los datos personales.

A través del presente manual, TGI busca dar cumplimiento al Régimen de Protección de Datos Personales - Ley 1581 de 2012-, al Decreto 1074 de 2015, a la Guía de Accountability de la Superintendencia de Industria y Comercio, y al Principio de Responsabilidad Demostrada en materia de Protección de Datos Personales.

2. ALCANCE

El presente Manual es de obligatorio y estricto cumplimiento por parte de todos los representantes y administradores de la Organización, empleados y/o colaboradores del TGI; personas naturales o jurídicas vinculadas a través de cualquiera de las modalidades contractuales establecidas en el Manual de Contratación de TGI, contratistas y terceros que obran en nombre de TGI.

Todos los empleados y/o colaboradores de TGI en el cumplimiento de sus funciones deben observar y respetar la regulación en materia de protección de datos, la Política de Tratamiento de datos personales y los deberes contenidos en el presente Manual.

Cualquier inquietud o duda en torno al cumplimiento de la Ley, de las Políticas de Tratamiento de datos personales o el presente Manual deberá ser dirigida al Oficial de Protección de Datos Personales quien se encargará de resolverlas y dar las instrucciones correspondientes.

3. ÁMBITO DE APLICACIÓN

El presente Manual es aplicable a cualquier base de datos personales o archivos creados, administrados y/o custodiados por la Organización, ya sea como Responsable o Encargado del Tratamiento. De igual forma, este manual aplica para el tratamiento de datos personales o bases de datos personales que los Titulares de la información en su calidad de oferentes, proveedores, contratistas, colaboradores, aspirantes, clientes o remitentes, entre otras, hayan entregado a TGI. De igual manera, aplicará a los datos personales que sean objeto de recolección y manejo por parte de TGI en territorio colombiano.

El presente manual no aplicará a:

3.1. A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

3.2. A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;

3.3. A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;

3.4. A las bases de datos y archivos de información periodística y otros contenidos editoriales;

3.5. A las bases de datos y archivos regulados por la Ley 1266 de 2008;

3.6. A las bases de datos y archivos regulados por la Ley 79 de 1993.

En todo caso, los principios de administración de datos personales serán aplicables a cualquier base de datos con información personal de la cual sea responsable TGI SA ESP

4. DEFINICIONES

4.1. **Autorización:** Consentimiento previo, expreso e informado del titular, para llevar a cabo el tratamiento de datos personales.[1]

4.2. **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 las 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.

4.3. **Base de datos:** Conjunto organizado de datos personales que sean objeto de tratamiento.[2]

4.4. **Causahabiente:** Persona que ha sucedido o se ha subrogado por cualquier título en el derecho de otra u otras.

4.5. **Colaborador**: Persona natural que tiene un vínculo laboral directo con TGI.

4.6. **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.[3] Los datos personales se clasifican en:

4.6.1. **Datos públicos:** Son los datos que no sean semiprivados, privados o sensibles. Son considerados datos públicos, los siguientes Datos: nombre, documento de identidad, estado civil de las personas, entre otros Así mismo, son datos públicos, los que, en virtud de una decisión del titular o de un mandato legal, se encuentren en archivos de libre acceso y consulta.

4.6.2. **Dato Semiprivado**: Es semiprivado el dato 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 el dato financiero y crediticio de actividad comercial o de servicios.

4.6.3. **Dato Privado**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para la persona titular del dato, como la información salarial, la información de contacto, la información académica, entre otros.

4.6.4. **Dato Sensible:** Es el dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tal como aquel que revele 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 el dato relativo a la salud, a la vida sexual y a la información biométrica, entre otros.

[1] Ley 1581 de 2012, Artículo 3, Literal a.
[2] Ley 1581 de 2012, Artículo 3, Literal b.
[3] Ley 1581 de 2012, Artículo 3, Literal c.

4.7. **Encargado del tratamiento**: Persona natural o jurídica, de naturaleza pública o privada que por sí misma o en asocio con otros, realice el tratamiento de datos personales de colaboradores, proveedores, oferentes y demás titulares de datos personales por cuenta de TGI. El encargado del tratamiento o tercero realizará el tratamiento de los datos personales dando cumplimiento a los lineamientos y directrices dadas por TGI.

4.8. **Evaluación de impacto de privacidad**: Es considerada una medida proactiva para cumplir con el Principio de Responsabilidad demostrada, asimismo sirve para poner en funcionamiento un sistema efectivo de riesgos y controles internos para garantizar que los datos se tratarán debidamente y conforme a la regulación existente. Dicha evaluación deberá incluir descripción detallada de las operaciones de tratamiento de datos personales. - Evaluación de riesgos específicos para los derechos y libertades de los titulares (identificar y clasificar riesgos), así como la adopción de medidas para mitigarlos. [4]

4.9. I**ncidente de protección de datos personales**: Un incidente de protección de datos personales ocurre cuando un evento genera la recopilación, uso, divulgación, destrucción no autorizada, pérdida o robo de datos personales de la Organización, ya sea accidental o intencional, y por tanto se presenta un incumplimiento a la Política de Tratamiento de Datos Personales y los demás procedimientos que hacen parte del Programa de Protección de Datos de TGI, así como del Régimen de Protección de Datos Personales – Ley 1581 de 2012.

4.10. **Normativa:** Hace referencia a la Constitución Política de Colombia, leyes, decretos, resoluciones, ordenanzas, acuerdos, conceptos de la Autoridad Nacional de Protección de Datos Personales y jurisprudencia.

4.11. **Oficial de protección de datos personales:** Persona responsable de la atención de peticiones, consultas y reclamos ante la cual el titular de la información puede ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización. El Oficial de Protección de Datos Personales apoyará y guiará el proceso de implementación del principio de responsabilidad demostrada. El Oficial de Protección de Datos Personales para TGI hace parte de la Dirección de Cumplimiento y el canal de contacto es datospersonales@tgi.com.co

4.12. **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 habeas data y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas en la normatividad vigente. Los datos personales, salvo la información pública, no podrá estar disponibles en Internet u 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.

4.13. **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 sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la normatividad que desarrolla el derecho al Habeas Data.

[4] Guía sobre el tratamiento de datos personales para fines de marketing y Publicidad- Superintendencia de Industria y Comercio.

4.14. **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]

4.15. **Principio de legalidad en materia de protección de datos personales:** El tratamiento de los datos personales, es una actividad reglada por la Ley 1581 de 2012 o Ley General de Protección de Datos Personales, normas constitucionales, siendo así una actividad reglada que debe sujetarse a lo establecido en la norma y en las demás disposiciones que la desarrollan.[6]

4.16. **Principio de libertad:** El tratamiento de los datos personales, solo puede ejercerse con el consentimiento libre, previo, expreso e informado del titular. Por esto los datos personales no podrán ser obtenidos o divulgados sin previa autorización del titular, o en ausencia de algún mandato legal o judicial que releve el consentimiento o autorización del titular.

4.17. **Principio de seguridad:** La información sujeta a tratamiento por parte de TGI, a que se refiere la ley 1581 de 2012, se manejará con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros de información, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.[7]

4.18. **Principio de transparencia:** En el tratamiento de los datos personales, se debe garantizar el derecho del titular a obtener del Responsable y Encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.[8]

4.19. **Principio de veracidad o calidad:** Los datos personales sujetos a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Es por lo anterior que se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.[9]

4.20. **Privacidad por diseño y por defecto:** La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan, para lo cual desde antes que se recolecte información y durante todo el ciclo de vida de esta, se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional. Humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información.[10]

4.21. **Responsabilidad demostrada:** O también denominado internacionalmente como "Accountability", en el cual se enfatiza el rol del Responsable del tratamiento a implementar medidas necesarias dentro de las organizaciones que permitan cumplir con los principios y obligaciones como tal. Observando así el compromiso por las organizaciones para incrementar los estándares de protección de la información personal y garantizar a los titulares el adecuado tratamiento de datos personales[11].

4.22. **Responsable del tratamiento**: Persona natural o jurídica, de naturaleza 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 personales. TGI ostenta la calidad de Responsable del Tratamiento de sus bases de datos.

[5] Ley 1581 de 2012, Artículo 4, Literal b.
[6] Ley 1581 de 2012, Artículo 4, Literal a.
[7] Ley 1581 de 2012, Artículo 4, Literal g.
[8] Ley 1581 de 2012, Artículo 4, Literal e.
[9] Ley 1581 de 2012, Artículo 4, Literal d.
[10] Decreto 620 del 2020, artículo 2.2.17.1.6.
[11] Superintendencia de Industria y Comercio – Guía para la implementación del Principio de Responsabilidad Demostrada (Accountability).

4.23. **Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.[12]

4.24. **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, 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 del cual se remitió.

4.25. **Transmisión:** Tratamiento de datos personales que implica la comunicación de estos dentro o fuera de cada país cuando tenga por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

4.26. **Tratamiento:** Cualquier operación o conjunto de operaciones sobre los datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.[13]

5. POLÍTICA PARA LA RECOLECCIÓN DE DATOS PERSONALES

5.1. Ámbito de aplicación

Las disposiciones contenidas en la presente política serán aplicables a todas las formas de recolección de datos personales que realice TGI, toda vez que en su calidad de Responsable del tratamiento de los datos personales deberá obtener el consentimiento previo, libre, expreso e informado de los titulares, tal y como lo establece el artículo 9 de la Ley 1581 de 2012.

5.2. Naturaleza del Dato Personal

Una de las principales inquietudes que surge al momento de manipular datos de personas naturales es determinar si se está o no frente a un dato personal. Para estos efectos se requiere identificar si con la información o con el conjunto de información que se tiene sobre una persona, es posible o no identificarla.

A manera de ilustración, los principales ejemplos de datos personales son, entre otros: nombre, apellido, correo electrónico, dirección de residencia, teléfono, etc.

Nota: Las imágenes contenidas en fotografías y grabaciones son consideradas como datos personales. Adicionalmente, los datos corporativos de las personas naturales, tales como: correo electrónico corporativo, son datos personales de carácter público.

En caso de que no se encuentre seguro acerca de si la información que se encuentra tratando es o no un dato personal, contacte al Oficial de Protección de Datos Personales al correo electrónico: datospersonales@tgi.com.co

5.3. Categorías de los Datos Personales

Una vez se tenga seguridad de que esta frente a un dato personal, es necesario entrar a determinar la naturaleza del mismo, de acuerdo con la clasificación que presenta la regulación colombiana de datos personales. Esto es de vital importancia, debido a que los formatos de autorización y las medidas de seguridad dependerán de la categoría a la que pertenezca el dato personal objeto de Tratamiento.

5.3.1. **Dato Público***:* es todo dato personal que se encuentre contenido en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales. Las normas han dado algunos ejemplos de datos públicos, como: los datos relativos al estado civil de una

12 Ley1581 de 2012, Artículo 3, Literal f.
13 Ley 1581 de 2012, Artículo 3, Literal g.

persona, su profesión, oficio o calidad de servidor público. Para realizar el Tratamiento de estos datos no se requiere de autorización. No obstante, los datos personales públicos están sujetos a la aplicación de todas las normas establecidas en materia de datos personales. Ej. La cédula de ciudadanía, los nombres y los apellidos de las personas. Así mismo, son datos públicos, los que, en virtud de una decisión del titular o de un mandato legal, se encuentren en archivos de libre acceso y consulta.

5.3.2. **Dato Semiprivado***:* es toda información de carácter financiera, comercial y crediticia que, principalmente, es utilizada en el análisis de riesgo de crédito. Para realizar el Tratamiento de estos datos, se requiere de una autorización expresa por parte del Titular. Ej. Los datos financieros y crediticios, la información laboral o educativa, entre otros.

5.3.3. **Dato Privado***:* es todo dato personal que no es público o semiprivado. Estos datos están sometidos a reserva y su Tratamiento afecta la privacidad del Titular. Para realizar el Tratamiento de estos datos, se requiere de una autorización expresa por parte del Titular. Ej. El correo electrónico del Titular, teléfono fijo o celular, dirección de residencia, gustos o tendencias, entre otros.

5.3.4. **Dato Sensible**: es todo dato personal cuyo uso puede llevar a la discriminación de un individuo y que por ende requieren de una autorización especial. Estos datos son de acceso restringido, requieren autorización expresa e inequívoca de conformidad con las disposiciones legales, entre otras, y además deberá informarse al Titular que su obtención no puede impedir el acceso a ningún bien o servicio. Ej. Los datos relativos a la salud del Titular, datos biométricos, datos de orientación sexual o religiosa, entre otros.

5.3.5. **Datos de Niños, Niñas y Adolescentes**: los datos personales de menores de 18 años se entienden como una categoría especial debido a las restricciones que conlleva su Tratamiento. Estos solo pueden ser utilizados para finalidades muy específicas relacionadas con el interés superior del menor y únicamente con el consentimiento expreso de los padres o representantes legales del menor.

Como lineamiento orientador, TGI tendrá en cuenta que entre más confidenciales sean los datos personales, por tratarse por ejemplo de Datos Sensibles o Datos de Niños, Niñas y Adolescentes mayor diligencia deberá tener el Responsable y/o exigir al Encargado en el cuidado de las Bases de Datos y su contenido.

5.4. Requisitos para la recolección de datos personales

El tratamiento de datos personales solo se realizará por TGI, si de manera previa se ha solicitado autorización al titular, en lo que tiene que ver con datos semiprivados, privados o sensibles. Para el efecto, el personal de la Organización hará uso de los distintos medios que contienen las autorizaciones, atendiendo a la calidad de cada titular.

Asimismo, y atendiendo a lo establecido por los principios de finalidad y libertad, la recolección de datos personales se limitará a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos conforme a la normatividad vigente.

Salvo en los siguientes escenarios, se podrán recolectar datos personales sin autorización del titular:

5.4.1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;

5.4.2. Datos de naturaleza pública;

5.4.3. Casos de urgencia médica o sanitaria;

5.4.4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos;

5.4.5. Datos relacionados con el Registro Civil de las Personas.

Los datos personales recolectados con motivo de la celebración de un contrato, relación laboral o legal, únicamente serán tratados para las finalidades directamente relacionadas con el vínculo que se trate. Si se desea utilizar los datos para finalidades distintas se deberá obtener el consentimiento del titular.

5.5. Autorización para el tratamiento de información personal

La Ley 1581 de 2012 define la autorización como: *"Aquel consentimiento previo, expreso e informado del titular, para llevar a cabo el tratamiento de datos personales."*[14]

TGI solicitará a los titulares de la información personal relacionada en sus bases de datos la autorización, previa, expresa, inequívoca e informada para realizar el tratamiento de sus datos.

La autorización podrá ser otorgada de las siguientes formas:

5.5.1. **Escrita:** Mediante modelos incorporados en formatos físicos de la Organización, en los cuales el titular autoriza el tratamiento de sus datos personales mediante su firma.

5.5.2. **Verbal:** Mediante modelos incorporados en canales telefónicos o de video, o cualquier otro canal que permita capturar la autorización verbal.

5.5.3. **Digital:** Mediante modelos incorporados en formularios web y demás desarrollos tecnológicos de TGI.

5.5.4. **Conductas inequívocas:** Son aquellas conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización. En ningún caso el silencio podrá asimilarse a una conducta inequívoca.[15]

5.6. Características de la autorización

TGI al momento de solicitar al titular la autorización para el tratamiento de sus datos personales, deberá informarle de manera clara y expresa lo siguiente:

5.6.1. El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
5.6.2. El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.

5.6.3. Los derechos que le asisten como Titular.

5.6.4. La identificación, dirección física o electrónica y teléfono del Responsable del Tratamiento.

5.7. Custodia de las autorizaciones

TGI deberá conservar las pruebas o evidencias que permitan demostrar que ha solicitado a sus titulares de la información, su autorización previa, expresa, e informada.

[14] Ley 1581 de 2012, Artículo 3, Literal a.
[15] Decreto 1074 de 2015, Artículo 2.2.2.25.2.4.

Para esto, TGI garantizará la adecuada custodia de las autorizaciones obtenidas por sus diferentes canales de recolección, físicos, verbales o digitales.

5.7.1. **Autorizaciones recolectadas a través de formatos físicos:** TGI custodiará adecuadamente en sus repositorios físicos, todos aquellos formatos o formularios mediante los cuales solicite la autorización del tratamiento de los datos personales a sus diferentes titulares de la información.

5.7.2. **Autorizaciones recolectadas a través de canales verbales:** TGI custodiará de manera adecuada aquellas evidencias tecnológicas que permitan soportar la solicitud de autorización para el tratamiento de datos personales a través de sus canales telefónicos o de video, o cualquier otro canal que permita capturar la autorización verbal.

5.7.3. **Autorizaciones recolectadas a través de canales digitales:** TGI custodiará en sus repositorios digitales, todos aquellos soportes tecnológicos o "logs" de aceptación de las autorizaciones para el tratamiento de datos personales recolectados por plataformas tecnológicas, sitios web, apps, entre otras.

El titular de la información podrá en cualquier momento y en el ejercicio de sus derechos solicitarle a TGI, le entregue el soporte o la evidencia de la autorización para el tratamiento de datos personales otorgada por este a favor de TGI.

5.8. Autorización respecto de los datos sensibles

El tratamiento de datos sensibles se encuentra prohibido expresamente por el artículo 6 de la Ley 1581 de 2012. Sin embargo, la anterior prohibición contempla las siguientes excepciones:

5.8.1. 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.

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

5.8.3. 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;

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

5.8.5. 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.[16]

La autorización del tratamiento de los datos personales de carácter sensible deberá darse en todos los casos de manera explícita, teniendo en cuenta la identidad que los mismos implican. Adicionalmente, cuando se deba realizar el tratamiento de este tipo de datos personales, se informará al titular la facultad que tiene de abstenerse de entregar esta información.

[16] Ley 1581 de 2012, Artículo 6.

5.9. Lineamientos para la recolección de datos sensibles

Si se recolectan datos sensibles (cuando exista una finalidad para ello, de conformidad con el numeral anterior), se deben cumplir además las siguientes obligaciones.

5.9.1. Informar al Titular que, por tratarse de datos personales sensibles, no está obligado a autorizar su tratamiento.

5.9.2. Informar al Titular, de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de Dato Personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.

5.9.3. No condicionar las actividades del Titular para que suministre Datos Personales sensibles, salvo que exista una causa legal.

5.10. Autorización respecto de los datos de niños, niñas y adolescentes

El tratamiento de los datos personales de niños, niñas y adolescentes se encuentra prohibido, salvo aquellos que sean de naturaleza pública, tal y como lo dispone el artículo 7 de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes requisitos:

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

5.10.2. Que en el tratamiento se asegure el respeto de los derechos fundamentales de los niños, niñas y adolescentes.

5.10.3. Que el tratamiento de los datos personales de menores sea precedido de la autorización expresa de su representante legal.

5.10.4. Que se informe al representante legal del menor que por tratarse de datos de menores no está obligado a autorizar su tratamiento.

5.10.5. Que se informe al representante legal del menor la finalidad del tratamiento de los datos.

La autorización para el tratamiento de los datos personales deberá ser otorgada por el representante legal del niño, niña o adolescente, 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.

5.11. Política de Tratamiento de Datos Personales

Con el fin de garantizar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en las bases de datos o archivos que TGI haya recopilado y dando cumplimiento a lo establecido en el Decreto 1377 de 2013, hoy compilado en el Decreto 1074 de 2015 y a la Ley 1581 de 2012, TGI como responsable de la información personal, ha diseñado y puesto a disposición de sus diferentes titulares de la información, su *Política de Tratamiento de Datos Personales.* Esta Política se encuentra publicada en el sitio web www.tgi.com.co

5.12. Finalidades para la recolección y tratamiento de los datos personales

Con el fin de dar cumplimiento a los principios de finalidad y libertad consagrados en la Ley 1581 de 2012, la recolección de datos personales que realice TGI se limitará a aquellos datos personales que son pertinentes y adecuados para la finalidad para la cual son recolectados o requeridos.

TGI podrá recolectar o realizar el tratamiento de los datos personales de sus titulares de la información para el cumplimiento de las siguientes finalidades, las cuales se encuentran disponibles para su consulta en la *Política de Tratamiento de Datos Personales de TGI.*

5.13. Finalidades generales para el Tratamiento de Datos Personales

TGI como Responsable del Tratamiento, realizará el Tratamiento de sus Datos Personales para cumplir con una finalidad legítima. Por consiguiente, la recolección de Datos Personales se limitará a aquellos que son pertinentes, adecuados, necesarios y útiles para el (o los) propósito (s) para el (los) cual (es) son recolectados o requeridos de conformidad con la normatividad. Frente a todos los Titulares, sin perjuicio de las finalidades específicas que se señalan a continuación, se recolectan los Datos Personales con las siguientes finalidades generales:

5.13.1. Enviar correspondencia y notificaciones.

5.13.2. Contactar al Titular de los Datos Personales a través de cualquier medio, especialmente, pero sin limitarse a su correo electrónico y/o celular.

5.13.3. Remitir información sobre actividades, productos y/o servicios de la Organización a través de los canales o medios que establezca para tal fin.

5.13.4. Mantener un registro de accionistas, control de las acciones y pago de utilidades.

5.13.5. Realizar convocatorias de junta directiva, realizar el pago de honorarios de los miembros de junta y enviar comunicaciones de interés a miembros de junta.

5.13.6. Realizar gestiones orientadas a la comunidad en general, donde se brinda información y se realizan actividades en torno al objeto de la Organización.

5.13.7. Realizar estudios de mercado, estadísticas y encuestas enmarcadas dentro del estatuto social y las políticas de TGI.

5.13.8. Permitir el ingreso a las instalaciones de TGI.

5.13.9. Capturar imágenes a través de sistemas de videovigilancia para garantizar la seguridad de las personas y los bienes que se encuentren en las instalaciones de TGI.

5.13.10. Utilizar la imagen del titular para generar notas o videos y publicarlos en distintos medios en los que se destaquen actividades y servicios de TGI.

5.13.11. Consultar la información del titular registrada en otras Bases de Datos o archivos de cualquier entidad pública o privada, nacional o internacional.

5.13.12. Adelantar trámites ante autoridades respecto de las cuales dicha información resulte pertinente.

5.13.13. Atender requerimientos de entidades públicas o privadas, quienes en cumplimiento de mandatos legales o contractuales estén autorizadas para solicitar y acceder a los Datos Personales.

5.13.14. Suministrar información a auditores quienes verifican la adecuada administración de TGI.

5.13.15. Contactar a grupos de interés para realizar posicionamiento de marca y gestión de reputación.

5.13.16. Realizar invitaciones a eventos y ofrecer nuevos productos y servicios.

5.13.17. Gestionar trámites (solicitudes, quejas y reclamos).

5.13.18. Efectuar las gestiones pertinentes para el desarrollo del objeto social de TGI en lo que tiene que ver con el cumplimiento del objeto del contrato celebrado con el Titular de la información o de la relación legal.

5.13.19. Efectuar encuestas de satisfacción de los productos y servicios ofrecidos por TGI.

5.13.20. Negociar y administrar las servidumbres requeridas para la infraestructura y operación de TGI.

5.13.21. Transferir los Datos Personales dentro o fuera del país a las empresas vinculadas económicamente con TGI (casa matriz, filiales y demás empresas del Grupo Energía Bogotá “GEB”), terceros, contratistas o aliados de TGI para que estas realicen el Tratamiento de los Datos Personales de conformidad con lo dispuesto en esta Política.

5.13.22. Transmitir los Datos Personales dentro o fuera del país a las empresas vinculadas económicamente con TGI (casa matriz, filiales, subordinadas y demás empresas del GEB), terceros, contratistas o aliados de TGI para que estas realicen el Tratamiento de los Datos Personales de conformidad con lo dispuesto en esta Política.

5.13.23. Transferir los Datos Personales en el marco de la definición, estructuración y ejecución de transacciones estratégicas, tales como la venta de activos en caso de que la Organización o partes de su negocio sean vendidas, fusionadas o adquiridas por terceros.

5.13.24. Cualquier otra finalidad que se encuentre directamente relacionada con el objeto social de TGI.

5.14. Finalidades del Tratamiento de Datos Personales específicas para proveedores y/o contratistas.

Los Datos Personales de titularidad de proveedores y/o contratistas de TGI, adicionalmente serán tratados para las siguientes finalidades específicas:

5.14.1. Efectuar las actividades necesarias requeridas en la etapa precontractual, contractual y post contractual de la Organización.

5.14.2. Realizar procesos de selección y registrarlos en categorías y/o clases de proveedores. Así mismo, realizar el registro como proveedores en los sistemas contables e informáticos de TGI y realizar los pagos correspondientes a las obligaciones contraídas y llevar una relación histórica de los proveedores.

5.14.3. Acceder, consultar, validar o corroborar los Datos Personales que reposen o estén contenidos en Bases de Datos o archivos de cualquier Entidad Pública o Privada nacional o extranjera, esta verificación podrá realizarse de manera directa o a través de terceros contratados por TGI.

5.14.4. Ejercer la supervisión o interventoría de los contratos; así como evaluar y calificar el desempeño de los proveedores y contratistas de la Organización.

5.14.5. Cumplir con las obligaciones contractuales y legales y para que ejerza los derechos que se derivan de su calidad de Sociedad Comercial y en general, de las actividades propias de su objeto social principal y conexo, así como de las políticas internas de la compañía.

5.14.6. Transferir y/o Transmitir a nivel nacional y/o internacional los Datos Personales a las empresas vinculadas económicamente con TGI (casa matriz, filiales y demás empresas del GEB), terceros, contratistas o aliados de TGI para que estas realicen el Tratamiento de los Datos Personales a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube.

5.14.7. Para fines de seguridad de las personas, los bienes e instalaciones de la Organización y ser utilizados como prueba en cualquier tipo de proceso, respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de TGI.

5.14.8. Suministrar información a terceros tales como empresas de correo, de servicios tecnológicos, aliados comerciales y/o estratégicos, entre otros en Colombia y en el exterior.

5.14.9. Realizar un registro de proveedores en el sistema SAP que contiene indicadores de impuestos para efecto del pago de facturas.

5.14.10. Para fines probatorios, legales, judiciales y/o administrativos en eventuales procesos internos o legales.

5.14.11. Desarrollar el objeto del contrato celebrado.

5.14.12. Evaluar el desempeño y las calidades del equipo designado para la ejecución del contrato por parte del contratista y/o proveedor oferente.

5.14.13. Remitir publicidad y publicaciones relacionadas con las actividades que desarrolla la Organización.

5.14.14. La realización de estudios de mercado, estadísticas y encuestas, enmarcadas dentro del objeto social de la Organización.

5.14.15. Transferir los Datos Personales de los proveedores en el marco de la definición, estructuración y ejecución de transacciones estratégicas, tales como la venta de activos en caso de que la Organización o partes de su negocio sean vendidas, fusionadas o adquiridas por terceros.

5.14.16. Negociar y administrar las servidumbres requeridas para la infraestructura y operación de TGI.

5.14.17. Reportar, en los términos de la Ley 1266 de 2008 ante cualquier operador de información o central de riesgo legalmente autorizada, sobre el cumplimiento oportuno o incumplimiento de obligaciones dinerarias o deberes de contenido patrimonial, presentando información veraz, pertinente, exacta, completa y actualizada.

5.18. Finalidades del Tratamiento de Datos Personales específicas para oferentes

Los Datos Personales de titularidad de oferentes de TGI, adicionalmente serán tratados para las siguientes finalidades específicas:

5.18.1. Evaluar la solicitud de habilitación para presentar ofertas.

5.18.2. Verificar los Datos de los Representantes que participarán en los procesos de selección contractual.

5.18.3. La realización de estudios de mercado, estadísticas, almacenamiento de información de contratistas y encuestas de la Organización.

5.18.4. Las demás relacionadas con el desarrollo del proceso de selección contractual en particular en el que se presente el oferente. Validar las calidades del equipo propuesto por el oferente para la ejecución del contrato.

5.19. Finalidades del Tratamiento de Datos Personales específicas para aspirantes a colaboradores y colaboradores

Los Datos Personales de titularidad de aspirantes a colaboradores y colaboradores de TGI, adicionalmente serán tratados para las siguientes finalidades específicas:

5.19.1. Selección de personal, estudio de hojas de vida, verificación de datos suministrados por el candidato, verificación de los contactos de referencias Personales, familiares y/o comerciales, datos de localización.

5.19.2. Realizar y verificar exámenes de salud de ingreso, periódicos y/o de egreso de la Organización.

5.19.3. Realización de pruebas escritas y orales de selección, pruebas psicotécnicas y/o entrevistas.

5.19.4. La aceptación de los procedimientos internos de selección, ingreso, salud ocupacional y contratación.

5.19.5. Permitir el ingreso a las instalaciones de la Organización.

5.19.6. Llevar un control de acceso y garantizar la seguridad de personas y bienes.

5.19.7. Tener registro de las actividades realizadas por la Organización.

5.19.8. Realizar el diligenciamiento de las afiliaciones a la Entidades Promotoras de Salud (EPS), Administradoras de Fondos de Pensiones y de Cesantía (AFP), Caja de Compensación Familiar (CCF), pólizas de seguros o plan adicional de salud cuando aplique.

5.19.9. Realizar estudios de seguridad para ingreso y monitoreo durante el tiempo que dure la relación laboral.

5.19.10. Verificar la información relacionada con el Sistema de Prevención de Lavado de Activos y Financiación del Terrorismo, conflictos de intereses, inhabilidades e incompatibilidades.

5.19.11. Garantizar el cumplimiento de los derechos sindicales consagrados en los artículos 38, 39 y 55 de la Constitución Política de Colombia, así como dar cumplimiento a la convención colectiva de trabajo vigente, cuando aplique.

5.19.12. Mantener un registro de colaboradores y excolaboradores.

5.19.13. Recolección y custodia de las hojas de vida.

5.19.14. Revisión de los antecedentes penales, contractuales y fiscales de los Titulares ante las autoridades pertinentes.

5.19.15. Identificación plena de los Titulares, mediante archivo y manejo de sus datos de contacto, información profesional y académica, entre otros.

5.19.16. Celebrar el contrato de trabajo, de aprendizaje, de prestación de servicios o cualquiera que aplique.

5.19.17. Dar cumplimiento a cualquier otra prestación que se derive de la relación contractual entre los Titulares y la Organización.

5.19.18. Informar instrucciones con ocasión del contrato con los Titulares, de ser aplicable.

5.19.19. Evaluar el desempeño de los Titulares.

5.19.20. Gestionar la nómina, el pago del apoyo económico, entre otros, por parte de la Organización o un tercero; administrar y realizar los pagos necesarios en la cuenta bancaria que señalen los Titulares o entidades expresamente indicadas por los Titulares.

5.19.21. Contratación de seguros de vida y de gastos médicos con la Organización o un tercero.

5.19.22. Notificar a familiares de los Titulares en casos de emergencia durante el horario de trabajo o con ocasión del desarrollo del contrato.

5.19.23. La comunicación, reproducción y publicación de fotografías y/o videos de los Titulares por parte de la Organización para fines de mercadeo, publicitarios, en medios internos de la Organización o externos.

5.19.24. Mantener la seguridad y salud de los Titulares en el lugar de trabajo directamente por la Organización o por parte de un tercero, de conformidad con las normas aplicables al Sistema de Gestión de la Seguridad y Salud en el Trabajo (en adelante “SG-SST”).

5.19.25. Recolectar información y evidencia con el fin de realizar procesos disciplinarios, de ser el caso.

5.19.26. Usar la información para procedimientos y documentos relacionados a la relación contractual de los Titulares con la Organización.

5.19.27. Enviar información sobre la Organización a los Titulares.

5.19.28. Comunicar y realizar al interior de la Organización actividades de bienestar para los Titulares y sus familias.

5.19.29. Toma de fotografías de los Titulares y sus familias en el marco de actividades de bienestar u otras actividades.

5.19.30. Toma de decisiones en materia laboral y/o contractual con respecto a la ejecución y terminación del contrato con los Titulares, bien sea por el área jurídica de la Organización o su asesor externo.

5.19.31. La transferencia de los Datos Personales de los Titulares a las compañías del Grupo Energía Bogotá ubicadas dentro o fuera de Colombia para las finalidades anteriormente señaladas.

5.19.32. La transferencia y/o Transmisión, nacional o internacional, de los Datos Personales de los Titulares a terceros o aliados comerciales para fines de prospección comercial o mercadeo.

5.19.33. La transferencia de los Datos Personales de los Titulares en el marco de la definición, estructuración y ejecución de transacciones estratégicas, tales como la venta de activos en caso de que la Organización o partes de su negocio sean vendidas, fusionadas o adquiridas por terceros.

5.19.34. La transmisión de los Datos Personales de los Titulares para que sean tratados por terceros, en calidad de Encargados, que se encuentren ubicados en Colombia o por fuera del país, para las finalidades anteriormente señaladas.

5.19.35. Registrar al colaborador en los sistemas informáticos de la Organización, con el propósito de que se puedan llevar a cabo las actividades contables, administrativas y financieras propias del vínculo contractual.

5.19.36. Coordinar el desarrollo profesional, y de los programas de capacitación de los colaboradores y el acceso a los recursos informáticos para tal fin.

5.19.37. Hacer uso de la información suministrada para hacer análisis e investigaciones forenses directamente o con el concurso de terceros, sean de naturaleza privada o de orden judicial en aras de proteger y salvaguardar los bienes del colaborador o de TGI.

5.19.38. Las demás finalidades necesarias y que se presten en el entorno de la ejecución laboral o contractual a efectos de cumplir con el objeto y las obligaciones derivadas de la relación entre los Titulares y la Organización.

5.20. Finalidades del Tratamiento de Datos Personales específicas para clientes o remitentes

Los Datos Personales de titularidad de clientes de TGI, adicionalmente serán tratados para las siguientes finalidades específicas:

5.20.1. Efectuar las actividades necesarias requeridas en la etapa precontractual, contractual y post contractual de la Organización.

5.20.2. Realizar el registro como clientes en los sistemas contables e informáticos de TGI y realizar la facturación y gestión de pago correspondientes a las obligaciones contraídas y llevar una relación histórica.

5.20.3. Transferir y/o Transmitir a nivel nacional y/o internacional los Datos Personales a aliados comerciales, socios estratégicos, casa matriz filiales, subsidiarias y empresas del GEB o a terceros a consecuencia de un contrato, ley o vínculo lícito que así lo requiera o para implementar servicios de computación en la nube.

5.20.4. Contactar al titular por medios telefónicos, correos electrónicos, chats o SMS, para la realización de encuestas de satisfacción.

5.20.5. Reportar, en los términos de la Ley 1266 de 2008 ante cualquier operador de información o central de riesgo legalmente autorizada, sobre el cumplimiento oportuno o incumplimiento de obligaciones dinerarias o deberes de contenido patrimonial, presentando información veraz, pertinente, exacta, completa y actualizada.

5.20.6. Transferir los Datos Personales de los clientes o remitentes en el marco de la definición,

estructuración y ejecución de transacciones estratégicas, tales como la venta de activos en caso de que la Organización o partes de su negocio sean vendidas, fusionadas o adquiridas por terceros.

5.20.7. Transmitir los Datos Personales de los clientes o remitentes para que sean tratados por terceros, en calidad de Encargados (por ejemplo, terceras empresas de marketing), ubicados en Colombia o por fuera del país, para las finalidades anteriormente señaladas.

5.20.8. Contactar posteriormente a los clientes o remitentes a través de llamadas, correo electrónico, y cualquier otro medio de comunicación para indagar sobre el posible interés de continuar con el servicio ofrecido por TGI

5.20.9. Realizar campañas de envío de información a los correos electrónicos, a través de redes sociales u otras plataformas de terceros, eventos, productos y servicios de la marca que pudieran ser de interés.

5.20.10. Acceder, consultar, validar o corroborar los Datos Personales que reposen o estén contenidos en Bases de Datos o archivos de cualquier Entidad Pública o Privada nacional o extranjera, esta verificación podrá realizarse de manera directa o a través de terceros contratados por TGI.

5.20.11. Administrar los contratos; así como evaluar, calificar y llevar estadísticas de los clientes de la Organización.

5.20.12. Para fines de seguridad de las personas, los bienes e instalaciones de la Organización y ser utilizados como prueba en cualquier tipo de proceso, respecto de los datos (i) recolectados directamente en los puntos de seguridad, (ii) tomados de los documentos que suministran las personas al personal de seguridad y (iii) obtenidos de las videograbaciones que se realizan dentro o fuera de las instalaciones de TGI.

5.20.13. Suministrar información a terceros tales como empresas de correo, de servicios tecnológicos, aliados comerciales y/o estratégicos, entre otros en Colombia y en el exterior.

5.20.14. Para fines probatorios, legales, judiciales y/o administrativos en eventuales procesos internos o legales.

5.20.15. Desarrollar el objeto del contrato celebrado.

5.20.16. Realizar estudios de mercado, estadísticas y encuestas, enmarcadas dentro del objeto social de la Organización.

5.21. Avisos de privacidad y de videovigilancia

TGI con el fin de dar cumplimiento al Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015 y a la Ley 1581 de 2012, ha puesto a disposición su Aviso de Privacidad y de Videovigilancia, mediante el cual informa a sus titulares las condiciones del tratamiento de sus datos personales.

El Aviso de Privacidad de TGI se encuentra publicado en el sitio web www.tgi.com.co y en nuestras oficinas. Respecto del Aviso de Videovigilancia, este se encuentra instalado en las oficinas de TGI que cuentan con un sistema de videovigilancia por circuito cerrado de televisión. Los avisos dispuestos en las oficinas se encuentran instalados en sitios de fácil acceso e identificación.

5.22. Lineamiento para la videovigilancia en las instalaciones de TGI

El presente lineamiento es de observancia general y obligatoria para todo el personal de TGI. La finalidad de la videovigilancia es de mantener la seguridad de las personas que ingresan a las instalaciones de la Organización, mediante la grabación de imágenes captadas por las cámaras de video fijas instaladas en los lugares determinados para ello, con el propósito de identificar conductas de riesgo, constitutivas de delito o que pongan en peligro a las personas que laboran e ingresan a las Organización y sus propias instalaciones.

5.22.1. Parámetros Generales

5.22.1.1. Se encuentran instaladas en TGI, cámaras de videovigilancia fijas que conforman un sistema cerrado de televisión con grabaciones en tiempo real que guarda imágenes, las cuales se conservarán por un periodo máximo de 180 días o acorde a la capacidad de los servidores del sistema bajo resguardo y responsabilidad del área de Seguridad.

5.22.1.2. Los datos recolectados a través de sistemas de videovigilancia podrán ser utilizados para recolectar información y evidencia con el fin de realizar procesos disciplinarios o investigaciones internas, de ser el caso.

5.22.1.3. El equipo de seguridad está autorizado para realizar las siguientes funciones:

5.22.1.3.1. Grabación en formato de video digital del perímetro seleccionado en forma permanente;

5.22.1.3.2. Almacenamiento diario de los videos obtenidos por las cámaras de videovigilancia por un periodo de tiempo limitado, designado por el área de seguridad. De no reportarse alguna situación que amerite la revisión de los videos, éstos serán removidos automáticamente, mediante el mecanismo de sobreescritura automática.

5.22.1.3.3. Se considera una situación de riesgo que amerite la revisión de los videos, las siguientes: - Robo de equipo o cualquier activo propio de TGI, - Vandalismo en los equipos o instalaciones físicas de TGI, - Alteraciones en las configuraciones de los equipos de TGI, y - Conductas que puedan ser constitutivas de delitos, entre otros.

5.22.1.4. Revisión del material videograbado: el personal de TGI al identificar alguna de las situaciones de riesgo antes expuestas, deberá notificar al área de seguridad para que, en coordinación con el área de tecnología, lleven a cabo la revisión del material videograbado y procedan a identificar la situación de riesgo o posible delito.

5.22.1.5. Prohibiciones: El personal responsable del sistema de videovigilancia deberá hacer uso adecuado del mismo, únicamente para los fines establecidos. Por lo tanto, quedan prohibidas las siguientes prácticas:

5.22.1.5.1. La creación de archivos de fotografía;

5.22.1.5.2. Divulgación no autorizada del material obtenido en la videograbación;

5.22.1.5.3. Grabación de áreas o personas específicas y con finalidades distintas a las previamente establecidas; y

5.22.1.5.4. Las demás que resulten contrarias a los fines propuestos en los presentes lineamientos.

5.23. Lineamientos para la recolección de datos personales en el proceso de Talento Humano

Los datos personales de los aspirantes a colaboradores, colaboradores activos, aprendices Sena, practicantes universitarios, familiares de colaboradores, excolaboradores, entre otros, están directamente vinculados a la Vicepresidencia de Talento Humano y Gestión Administrativa. Esta Vicepresidencia está a cargo de la recepción, custodia, almacenamiento y disposición final de la información asociada a datos personales de los titulares de la información anteriormente relacionados.

5.23.1. Proceso de Selección

5.23.1.1. **Recolección de Hojas de Vida:** La Organización ha establecido diferentes tipos de procedimientos para realizar la convocatoria de vacantes laborales, recolectando la

información a través de la publicación de vacantes en buscadores de empleo en la web y en las cuentas oficiales de la Organización de redes sociales.

5.23.1.2. **Selección de candidatos:** Las hojas de vida que son recibidas en la Organización, son objeto de revisión y surten un proceso en la selección del candidato de acuerdo con los parámetros establecidos por la Vicepresidencia de Talento Humano y Gestión Administrativa.

TGI una vez ha seleccionado a los candidatos que surtirán el proceso de selección, le solicita a cada uno de estos su autorización para el tratamiento de los datos personales recolectados en dicho proceso, a través del *Formato: Autorización Para El Tratamiento De Datos Personales – Aspirantes (F-GTH-047).*

Una vez se culmina con el proceso de selección de candidatos, los aspirantes a colaboradores dan comienzo al proceso de selección, mediante el cual son convocados a entrevistas, se les realizan pruebas de conocimiento o psicotécnicas, visitas domiciliarias, estudios de seguridad, pruebas psicotécnicas, entre otras actividades propias del proceso de selección.

Finalizado el proceso de selección convocado, TGI almacenará las hojas de vida recibidas en el marco de este proceso, por un término máximo de un (1) año, al cabo del cual, eliminará las hojas de vida recibidas de los candidatos no seleccionados.

5.23.1.3. **Proceso de contratación:** El proceso de contratación está definido por procedimientos que lo componen. Sin embargo, en relación con la protección de los datos personales, la Dirección de Gestión del Talento y el líder de proceso que esté llevando a cabo la contratación, deberá garantizar que el colaborador firme el formato: *Autorización Para El Tratamiento De Datos Personales Colaboradores TGI (F-GTH-059)*

Mediante esta autorización el colaborador otorgará a la Organización su consentimiento con el propósito de que ésta pueda realizar el tratamiento de sus datos personales, para las finalidades requeridas por la Organización y publicadas en nuestra *Política de Tratamiento de Datos Personales.*

5.23.1.4. **Almacenamiento de historias laborales de colaboradores activos e inactivos:** Las historias laborales de los colaboradores activos o inactivos deberán resguardarse bajo condiciones de seguridad que impidan el acceso a terceros o personas no autorizadas.

5.23.1.5. **Toma de exámenes médicos ocupacionales:** Dentro del proceso de contratación y de ejecución de los contratos, existen disposiciones de salud ocupacional que obligan a Organización a realizar exámenes médicos ocupacionales de ingreso, periódicos y de retiro, según cada caso.

En los casos en los cuales se deban realizar exámenes médicos de carácter ocupacional, los resultados de estos deben ser custodiados por la Organización, garantizando el cumplimiento de medidas de seguridad adecuadas para su almacenamiento, teniendo en cuenta el carácter sensible de esta información personal. A esta información solo podrán tener acceso aquellas personas que por sus funciones o rol deben conocerla.

5.23.1.6. **Incapacidades médicas:** Las incapacidades médicas, al ser información de tipo sensible debido a su contenido médico, deben ser custodiadas con medidas adecuadas para garantizar e impedir el acceso a terceros o colaboradores no autorizados. El almacenamiento de estas debe estar enfocado a que la consulta de la información solo pueda ser realizada por quienes tienen el derecho de hacerlo por el desarrollo de sus labores en la Organización, y estos funcionarios, deben guardar absoluta confidencialidad sobre esta información.

5.24. Lineamientos para la recolección de datos personales en la vinculación de oferentes, contratistas y/o proveedores

Nuestra Organización al momento de la vinculación de los oferentes, contratistas y/o proveedores, recolectará su autorización para el tratamiento de los datos personales recolectados, de titularidad del representante legal de la persona jurídica, del contacto autorizado por el proveedor para las comunicaciones objeto del contrato suscrito, o de cualquier persona natural cuyos datos personales sean suministrados a TGI. La autorización se solicitará a través de la herramienta tecnológica dispuesta por el área de Abastecimiento.

5.25. Lineamiento para el manejo de fotografías y/o videos

TGI previo al registro de imágenes, cualquiera sea su formato fotografía, ilustración o video y cuyo objetivo sea su publicación en medios impresos, online y/o audiovisuales implementará los siguientes parámetros con el fin de proteger los derechos fundamentales de sus titulares y dar cumplimiento a las regulaciones de protección de datos personales.

5.25.1. Parámetros generales

5.25.1.1. Las imágenes cuyo propósito sea la publicación en revistas, publicidad, redes sociales, entre otros; deberán contar además con la autorización del Titular de la cesión de los derechos del uso de su imagen en estos contextos.

5.25.1.2. Obtener consentimiento previo para la captura y publicación de fotografías en cualquier eventualidad. Este consentimiento debe contar con las finalidades específicas para las cuales será usada esa fotografía.

5.25.1.3. Cuando se trate de imágenes personales que se encuentren dentro del banco de imágenes autorizado por TGI, se debe comprobar que dichas imágenes cuentan con la autorización de su titular para el tratamiento y la finalidad que se le pretende dar.

5.25.1.4. En caso de hacer uso de una imagen y/o fotografía capturada por un tercero externo de TGI, se debe corroborar que el mismo cuente con la autorización en debida forma del Titular de la imagen.

5.25.1.5. Aplicar medidas de anonimización correctivas en caso de que no haya sido posible obtener el consentimiento de los titulares de las imágenes a tratar.

5.25.1.6. El tratamiento de imágenes personales debe velar por el cumplimiento de derechos fundamentales como la dignidad o buen nombre, y en especial, evitar que el uso de imágenes personales pueda generar algún tipo de discriminación.

5.25.1.7. En la toma de fotografías y/o grabaciones durante eventos y reuniones se deberá mostrar a los titulares, en un lugar visible, un aviso previo a la toma de las mismas que informe acerca del tratamiento de sus datos personales e incluya los requisitos de información mínima establecidos por ley, así:

AVISO PROTECCIÓN DE DATOS

Estimado asistente, usted será grabado durante el termino de duración de la presente reunión por parte de Transportadora de Gas Internacional S.A. ESP (en adelante "TGI"), identificado con NIT 900.134.459-7 y con domicilio en Bogotá D.C., dirección Carrera 9 No. 73 – 44 Pisos 2, 3 y 7. TGI realizará el tratamiento de sus datos personales a través de la toma de fotografías y/o grabaciones de voz y video, motivo por el cual con su permanencia en este evento autoriza a realizar el tratamiento de sus datos personales. La recolección, almacenamiento, uso y circulación de las fotografías y grabaciones tomadas durante el evento se harán para las siguientes finalidades: i) Capturar su imagen mediante la toma de fotografías o grabación de evidencias fílmicas con el fin de contar con evidencias de los eventos realizados por TGI. ii) Publicar las evidencias fotográficas y fílmicas en nuestro sitio web, redes sociales y demás medios de comunicaciones internos y externos.

Como titular de información Usted tiene los siguientes derechos (i) acceder en forma gratuita a los datos personales proporcionados a TGI que hayan sido objeto de tratamiento; (ii) conocer, actualizar y rectificar su información personal; (iii) solicitar prueba de la autorización otorgada a TGI; (iv) ser informado por el responsable o encargado sobre el uso que se le ha dado a sus datos personales; (v) presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad vigente; (vi) revocar la autorización otorgada y solicitar la supresión del dato cuando no se representen los principios, derechos y garantías constitucionales y legales; (vii) abstenerse de responder preguntas sobre datos sensibles o que versen sobre niños, niñas y adolescentes. Usted podrá ejercer cualquiera de sus derechos, incluyendo sin limitación sus derechos de acceso, rectificación, cancelación y oposición (ARCO), al correo electrónico datospersonales@tgi.com.co o en la dirección: carrera 9 No. 73 – 44 Pisos 2, 3 y 7.

Es compromiso de TGI mantener los datos personales protegidos, por lo cual le informamos que usted podrá consultar nuestra ***Política de Tratamiento de Datos Personales*** *y/o cualquier cambio sustancial en la misma, en nuestra página web www.tgi.com.co*

El organizador del evento o de la reunión deberá dejar constancia de: i) la fijación del aviso de protección de datos; ii) el contenido del aviso y iii) la fecha de la reunión o del evento.

5.26. Parámetros especiales para el uso de imágenes de menores de edad

TGI previo a realizar captura de imágenes en dónde aparezcan menores de edad, obtendrá el respectivo consentimiento de los representantes legales o tutores. Para el uso de las imágenes personales de menores de edad TGI aplicará los siguientes criterios adicionales a los requisitos planteados en la ley para la autorización del tratamiento de datos:

5.26.1. La finalidad del tratamiento responda al interés superior de los niños, niñas y adolescentes.

5.26.2. Se asegure el respeto de sus derechos fundamentales de los niños, niñas y adolescentes.

5.26.3. De acuerdo con la madurez del niño, niña o adolescente se tenga en cuenta su opinión.

Por lo tanto, tendrá en cuenta que los datos de los niños, las niñas y adolescentes pueden ser objeto de tratamiento 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.

5.27. Lineamientos para el tratamiento de datos personales relacionados con el COVID-19

TGI recolecta datos sensibles de salud de todos sus colaboradores mediante el reporte diario de salud, a su vez, recolecta información relacionada con el proceso de vacunación, entre otros aspectos relacionados con los protocolos de bioseguridad.

TGI, previo a la recolección y tratamiento de datos personales relacionados con la pandemia del COVID-19 y los protocolos de bioseguridad implementados como consecuencia de aquella, implementará los siguientes parámetros con el fin de proteger los derechos fundamentales de sus titulares y dar cumplimiento a las regulaciones de protección de datos personales.

5.27.1. Parámetros generales

5.27.1.1. Los datos personales recolectados con relación al COVID-19 y los protocolos de bioseguridad adoptados por TGI serán los expresamente exigidos por el Ministerio de Salud y Protección Social para efectos de dar cumplimiento a los protocolos.

5.27.1.2. Obtener consentimiento previo para la recolección y tratamiento de datos personales relacionados con los protocolos de bioseguridad. Este consentimiento debe contar con las finalidades específicas para las cuales será usada esa información. Dichas finalidades podrán ser únicamente las indicadas por el Ministerio de Salud y Protección Social.

5.27.1.3. Al momento de obtener consentimiento previo para la recolección y tratamiento de datos personales relacionados con el COVID-19, se deberá informar al ciudadano la norma específica que ordena recolectar los datos solicitados para dar cumplimiento a los protocolos de bioseguridad.

5.27.1.4. TGI implementará las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como garantizar los principios de confidencialidad, acceso y circulación restringida.

5.27.1.5. Los datos personales recolectados con relación al COVID-19 y los protocolos de bioseguridad serán almacenados sólo durante el tiempo razonable y necesario para cumplir con las finalidades señaladas. Una vez cumplida la finalidad, TGI suprimirá los datos recolectados.

5.27.1.6. Las bases de datos que sean creadas para dar cumplimiento a los protocolos de bioseguridad adoptados por TGI y ordenados por la regulación vigente serán registradas ante el Registro Nacional de Bases de Datos.

5.27.2. Parámetros especiales para el uso de datos sensibles- datos de salud

TGI, previo a la recolección y tratamiento de datos sensibles relacionados con el COVID-19 y los protocolos de bioseguridad adoptados obtendrá el respectivo consentimiento de los titulares, salvo en los casos donde la ley no lo requiera. Para el tratamiento de datos sensibles, TGI aplicará los siguientes criterios adicionales, de conformidad con la Ley 1581 de 2012, el Decreto 1377 de 2013 y demás normas que regulan la materia:

5.27.2.1. Se informará al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento.

5.27.2.2. Se informará al titular que, por tratarse de datos sensibles, no está obligado a responder preguntas relacionadas a los mismos.

5.27.2.3. No se podrá condicionar ninguna actividad a que el titular suministre datos personales sensibles.

5.27.2.4. La recolección, uso, circulación y tratamiento de datos sensibles estará rodeada de especial cuidado y diligencia en su recolección, uso, seguridad o cualquier otra actividad que se realice con estos.

5.28. Lineamiento relacionado con el tratamiento de datos en reuniones de trabajo a través de herramientas corporativas

TGI cuenta con herramientas corporativas para sus reuniones de trabajo, en donde los colaboradores que asisten pueden grabar la reunión y tener acceso a dichas grabaciones. Los presentes lineamientos son de carácter obligatorio para todo personal de TGI y establecen los parámetros generales que se deberán respetar para el adecuado cumplimiento de la normativa de protección de datos personales colombiana.

5.28.1. Parámetros Generales

5.28.1.1 Se deberá notificar a los asistentes con antelación cuando las reuniones sean grabadas y/o monitoreadas para su posterior acceso, uso y almacenamiento.

5.28.1.2 En el acceso a las grabaciones de las reuniones del personal de TGI, deberá respetarse y garantizarse la intimidad y confidencialidad en el uso de las tecnologías de la información. Asimismo, todos los usuarios al hacer uso de los recursos tecnológicos lo harán con responsabilidad, eficiencia, eficacia, ética y legalidad.

5.28.1.3 Las grabaciones de voz y/o imagen que sean recolectados para estos fines deberán conservarse bajo medidas de seguridad y confidencialidad de la información.

5.28.1.4 Se deberá hacer uso adecuado de las grabaciones de voz y/o imagen únicamente para los fines previamente establecidos y autorizados por los titulares.

5.29. Bases de Datos de la Organización

5.29.1. Inventario de los datos personales que componen una base de datos

Para dar adecuado tratamiento a los datos personales, TGI identificará y mantendrá actualizado el inventario de los datos personales, definiendo y validando los elementos que a continuación se describen:

5.29.1.1. Identificación de las bases de datos de información donde se almacenan los datos personales.

5.29.1.2. Naturaleza de datos personales contenidos en cada una de las bases de datos.

5.29.1.3. Cantidad de titulares asociados a cada una de las bases de datos.

5.29.1.4. Finalidades del tratamiento para cada una de las bases de datos.

5.29.1.5. Encargados del tratamiento asociados a cada una de las bases de datos.

5.29.1.6. Medidas de seguridad de la información para cada una de las bases de datos.

5.30. Criterios que definen una base de datos

Una base de datos se define como aquel conjunto organizado de datos personales que sea objeto de tratamiento[17]. Las bases de datos pueden clasificarse en dos categorías: (i) Bases de datos físicas: Son aquellas cuya información personal se encuentra organizada y almacenada de manera física y; (ii) Bases de datos automatizadas: Son aquellas cuya información se encuentra organizada y almacenada con la ayuda de herramientas informáticas. [18]

A continuación, se establecen los criterios que TGI ha establecido para la identificación de sus bases de datos:

CRITERIO	BASE DE DATOS	REPOSITORIO DE INFORMACIÓN
Identidad	Se encuentra asociada al contenido que permite identificar un grupo de personas determinado. La base de datos se caracteriza por contener datos que de manera directa revelan la identidad de un grupo de personas asociadas a una finalidad de la base de datos.	Un repositorio será el que contenga información anónima o con elementos que dificulten determinar a los titulares cuya información les pertenece.
Formalidad	Hace referencia a la estructura de la base de datos que permite realizar una consulta o registro de información personal dentro de las actividades de un proceso.	Se caracteriza por realizar la réplica innecesaria o no controlada de la información personal requerida para las actividades de un proceso.
Estructura	La estructura de la base de datos se identifica como aquella característica que permite establecer el contenido o entrada de información de ésta, de manera predeterminada o estandarizada.	Contenido no homogéneo, el cual no refleja una consistencia con el relacionamiento de los datos personales establecidos en éste; la información puede incluirse de una forma no consistente.

[17] Ley 1581 de 2012, Artículo 3, Literal b.
[18] Decreto 1074 de 2015, Artículo 2.2.2.26.2.6

Vigencia	Tiene una finalidad asociada a la conservación de la información en ella incorporada, con el propósito de realizar consultas o servir de insumo para la toma de decisiones. Es aquella que conserva información de tipo personal por un periodo de tiempo determinado, durante el cual su contenido es requerido por su utilidad práctica o por exigencia legal.	Se encuentra en tránsito temporal dentro de las actividades del proceso o se caracteriza por ser un flujo de información procedente de una base de datos formal con destino a otra base de datos formal o a un repositorio informal de datos.
Unidad	El contenido se encuentra asociado a una finalidad y medio. Ejemplo: Documentación almacenada en varias carpetas físicas que tienen el mismo propósito.	Es aquella que pese a tener un mismo contenido, se encuentra en medios de almacenamiento diferentes o se registra bajo criterios cuya finalidad no es la misma.

Los criterios previamente descritos han sido definidos como un instrumento que permite la identificación de las bases de datos que por su estructura pueden ser reportadas o registradas ante el Registro Nacional de Bases de Datos – RNBD- de la Superintendencia de Industria y Comercio.

Con base en los criterios expuestos, TGI registró ante el Registro Nacional de Bases de Datos – RNBD- de la Superintendencia de Industria y Comercio, sus bases de datos.

5.31. Permanencia de las bases de datos

TGI solo podrá recolectar, almacenar, usar o circular los datos personales durante el tiempo que sea razonable y necesario, de acuerdo con las finalidades que justificaron el tratamiento, atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplida la o las finalidades del tratamiento y sin perjuicio de normas legales que dispongan lo contrario, la Organización deberá proceder a la supresión de los datos personales en su posesión. No obstante lo anterior, los datos personales deberán ser conservados cuando así se requiera para el cumplimiento de una obligación legal o contractual.

5.32. Determinación de los titulares que componen la base de datos

La determinación de la cantidad de titulares en una base de datos permite tener el control en el flujo de información que la compone. A continuación, se establece la metodología para la identificación de la cantidad de titulares que componen las bases de datos:

5.32.1. **Consecutivo:** Es el mecanismo mediante el cual se determina el número total de titulares, a través del último dato registrado en un control numérico consecutivo de ingresos a la base de datos. Por lo general existen índices que permiten determinar el seguimiento numérico en ascenso de los registros.

5.32.2. **Conteo:** Es el procedimiento a través del cual se realiza el conteo uno a uno de los titulares registrados en la base de datos.

5.32.3. **Estimado:** De acuerdo con la naturaleza de la base de datos y ante la imposibilidad de realizar un conteo a través de consecutivo o del conteo, se procederá a verificar de manera global un promedio de titulares de acuerdo con los registros establecidos y que permita dar

cuenta del ingreso de información registrada en la base de datos. Este método se aplicará en los casos en los cuales por el volumen de la información, no podría llevarse a cabo un conteo en un tiempo razonable.

5.33. Registro de las Bases de Datos Personales en el RNBD

TGI deberá inscribir todas las Bases de Datos Personales en el RNBD dentro de los dos (2) siguientes meses, contados a partir de su creación. El registro deberá ser actualizado en los términos que se indican a continuación:

5.33.1. Anualmente, entre el 2 de enero y el 31 de marzo.

5.33.2. Cuando se realicen Cambios Sustanciales en la información registrada, estos cambios deberán registrarse dentro de los primeros diez (10) días hábiles de cada mes.

5.33.3. Cuando se presenten reclamos de los Titulares de los Datos Personales, deberá realizarse la actualización dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año.

5.33.4. Cuando se presenten incidentes de seguridad relacionados con la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una Base de Datos administradas por TGI, deberá reportarlo en el RNBD dentro de los quince (15) días hábiles siguientes al momento en que se detecten y ser puestos en conocimiento del Oficial de Protección de Datos Personales de TGI.

6. POLÍTICA PARA EL USO DE DATOS PERSONALES

6.1. Ámbito de aplicación

Las disposiciones contenidas en la presente política serán aplicables a todas aquellas formas de uso de los datos personales que realice TGI, toda vez que en su calidad de Responsable del tratamiento de los datos personales deberá garantizar el cumplimiento de los principios de acceso y circulación restringida, seguridad y confidencialidad consagrados en la Ley 1581 de 2012.

6.2. Confidencialidad de la información personal

En el cumplimiento o ejercicio de sus funciones, los colaboradores de nuestra Organización podrán hacer uso de la información personal confiada a TGI por sus titulares de la información. En este uso, todos los colaboradores tienen la obligación de salvaguardar la confidencialidad de la información y dar un manejo adecuado a la misma. Esta obligación continúa aún después de finalizado el vínculo laboral con nuestros Colaboradores.

Mediante el presente Manual, la Organización establece aquellas pautas y directrices que deben ser cumplidas por sus colaboradores, en especial las relacionadas con la confidencialidad, la protección de la información personal y el uso adecuado de la misma. Algunas directrices que deben acatar los colaboradores de TGI, frente a la privacidad de la información personal, son:

6.2.1. Cumplir con las políticas, procedimientos y procesos para almacenar, guardar y controlar el acceso a información confidencial electrónica y física.

6.2.2. Cumplir todas las políticas, procedimientos y procesos para transmitir información confidencial.

6.2.3. No enviar información confidencial a través de medios no seguros como correo electrónico o Internet (esto incluye las plataformas internas de medios sociales). Se deben seguir los procedimientos seguros de operación de correo electrónico cuando se debe enviar

información confidencial fuera de TGI.

6.2.4. No mostrar descuidadamente información confidencial (por ej., dejar información en la pantalla de una computadora, o documentos confidenciales a la vista, o que puedan perderse o extraviarse).

6.2.5. No divulgar información confidencial a personas fuera de TGI (incluyendo familia o miembros de esta o asociados cercanos) o a otros empleados que no requieren la información para hacer su trabajo.

6.2.6. Tener cuidado de no discutir información confidencial donde pueda ser escuchada accidentalmente o interceptada (como al usar el celular) por ejemplo, asegurándose con quién está hablando y que su conversación no puede ser escuchada accidentalmente por personas no autorizadas. No discutir información confidencial en lugares públicos, como restaurantes, elevadores y otros lugares públicos.

6.2.7. Destruir o deshacerse de la información de acuerdo con los requisitos de seguridad y de acuerdo con las políticas y procedimientos para la retención y destrucción de documentos.

6.2.8. Conocer y dar cumplimiento a la Política de Tratamiento de Datos Personales de TGI, así como las demás políticas y procedimientos que este ha establecido para proteger la información personal.

6.2.9. No acceder a información personal de un titular, sin una razón de negocios legítima y con la debida autorización.

6.2.10. Solicitar la realización de las Evaluaciones de Impacto a la Privacidad ante las nuevas iniciativas de la Organización y contratación de proveedores que accederán a información personal.

6.2.11. Reportar los incidentes de protección de datos personales adecuada y oportunamente.

6.2.12. El personal de TGI se abstendrá de utilizar bases de datos que no cuenten con la autorización del titular de los datos o que no provengan de los registros públicos, toda vez que son conscientes de que la información personal sólo puede ser usada si la misma ha sido debidamente captada y autorizada.

6.2.13. Todos los funcionarios de TGI deberán utilizar la información con el único fin de cumplir con las tareas asignadas relacionadas estrictamente según la operación de cada unidad.

6.2.14. El personal de TGI deberá en todo momento ser consiente que la falta de autorización del tratamiento de datos personales genera un incumplimiento de la normatividad vigente en materia de protección de datos, pues el titular no faculta al colaborador sino a la entidad a tratar sus datos de carácter personal. Se debe recordar por parte de todos los colaboradores que la autorización recae sobre TGI. Cuando se trate de datos personales provenientes de los registros públicos no se requiere la autorización previa del titular para su tratamiento, pero se deberán cumplir en todo caso, las demás disposiciones contenidas en la normatividad para su uso adecuado.

6.2.15. En el evento que el personal de la entidad realice alguna actividad que implique captación de datos personales, deberá siempre utilizar los formatos autorizados por la entidad. Una vez los formatos de captación se encuentren diligenciados por parte del titular de información de carácter personal, deberá custodiar dichos documentos y no podrá en ningún momento elaborar bases de datos con dicha información para uso personal.

6.2.16. Ningún colaborador de TGI podrá revelar información que tenga el carácter de sensible o confidencial y que conozca en razón de su actividad laboral.

6.2.17. Todos los trabajadores de TGI y/o terceros Encargados deberán mantener la confidencialidad de los datos personales objeto de tratamiento por parte de TGI. Todos los contratos que celebre TGI con sus trabajadores o con terceros que vayan a tener acceso a los datos personales contenidos en las bases de datos de TGI, deberán contener una cláusula de confidencialidad respecto de dichos datos personales. Los datos personales únicamente podrán ser objeto de tratamiento para las finalidades descritas en el presente Manual o en la Política de Tratamiento de Datos Personales de TGI.

Nota: En caso de que tenga inquietudes frente a la confidencialidad de cierta información deberá acercarse al Oficial de Protección de Datos Personales de TGI para que le permitan tener claridad sobre las obligaciones especiales de cuidado que puedan existir frente a cierta información.

6.3. Sanciones internas

El incumplimiento a las obligaciones descritas en el presente Manual por parte de Colaboradores de la Organización acarreará sanciones disciplinarias de conformidad con el Reglamento Interno de Trabajo.

6.4. Sanciones por incumplimiento del deber de confidencialidad

Cualquier infracción a la obligación de confidencialidad por parte de los trabajadores, se considerará como una violación al Contrato de Trabajo, y estará sujeta a las consecuencias contenidas en el mismo.

Asimismo, cualquier infracción a la obligación de confidencialidad por parte de los terceros Encargados que ponga en riesgo los Datos Personales, podrá ser causal de terminación de los respectivos contratos con dichos Encargados.

6.5. Sanciones penales por el Tratamiento no autorizado de datos personales

De acuerdo con el artículo 269F del Código Penal señala lo siguiente:

> *"Violación de Datos Personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, Datos Personales contenidos en ficheros, archivos, Bases de Datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes."*

TGI podrá adelantar las denuncias correspondientes en caso de que tenga conocimiento de la participación de cualquier trabajador o tercero vinculado a TGI en la comisión de las conductas establecidas en el artículo 269F del Código Penal, cuando estas sean realizadas en relación con Datos Personales contenidos en Bases de Datos de TGI.

Los trabajadores que accedan a las Bases de Datos de TGI deberán realizar el Tratamiento en estricto cumplimiento de la Política de Tratamiento de Datos Personales de TGI, y de las establecidas en este Manual.

6.6. Seguridad de la información personal

La Organización cuenta con un Programa de Seguridad de la Información, el cual tiene como fin asegurar la confidencialidad de la información bajo su custodia, garantizando su integridad y asegurando la disponibilidad y continuidad de los sistemas.

Todas aquellas políticas y procedimientos que hacen parte integral del Programa de Seguridad de la Información de TGI, deben ser conocidos y aplicados integralmente por los colaboradores de la

Organización. Estos tienen la responsabilidad de proteger la información, ya sea que se trate de información de propiedad exclusiva o de información confiada a TGI por los titulares de la información. Por tanto, estos deben tener el cuidado, la diligencia y la habilidad que se esperaría de una persona razonablemente prudente al tratar información personal.

Para garantizar el cumplimiento de los lineamientos que hacen parte del Programa de Seguridad de la Información, se desarrollan actividades que garanticen medidas administrativas, técnicas y físicas que permitan:

6.6.1. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, para lo cual se cuenta con una *Clasificación Y Gestión De Activos De Información Y Tecnología De La Información (G-ADI-005)*, la cual contempla los pasos para la identificación, valoración, clasificación, protección y revisión o actualización de activos de información de TGI.

6.6.2. Implementar, operar, monitorear, revisar y mejorar las medidas de seguridad de la información; para lo cual se cuenta con un reglamento de seguridad de la información en el documento *Reglamento De Seguridad De La Información (R-ADI-001)* los cuales permiten reducir riesgos vinculados a amenazas a la infraestructura tecnológica de TGI, garantizando la protección a los datos personales, entre otros riesgos asociados a la información de TGI.

6.7. Privacidad por diseño y por defecto

La Superintendencia de Industria y Comercio, se ha referido a la privacidad desde el diseño y por defecto (*Privacy by Design and by Default*) como aquella medida proactiva para cumplir con el Principio de Responsabilidad Demostrada y que promueve la visión de que el futuro de la privacidad no puede ser garantizado sólo por cumplir con los marcos regulatorios; más bien, idealmente el aseguramiento de la privacidad debe convertirse en el modo de operación predeterminado de una organización.

Dado lo anterior, el ente de control recomienda que con anterioridad a cualquier recolección de información y durante todo el ciclo de vida de la misma, las organizaciones adopten medidas preventivas de diversa naturaleza (tecnológicas, organizacionales, humanas y procedimentales, entre otras) con el objeto de evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información, así como fallas de seguridad o indebidos tratamientos de datos personales.

Las medidas tecnológicas, humanas, administrativas, físicas, contractuales y de cualquier otra índole, adoptadas por las organizaciones, deben propender por evitar:

6.7.1. Accesos indebidos o no autorizados a la información.

6.7.2. Manipulación de la información.

6.7.3. Destrucción de la información.

6.7.4. Usos indebidos o no autorización de la información.

6.7.5. Circular o suministrar la información a personas no autorizadas.[19]

A su vez, el Decreto 620 del 2020, en su artículo 2.2.17.1.6. “Principios”, define la privacidad por diseño y por defecto como:

“La privacidad y la seguridad deben hacer parte del diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de las infraestructuras que lo soportan, para

[19] Superintendencia de Industria y Comercio, Guía Marketing, Publicidad y Tratamiento de datos Personales, página 12.

lo cual desde antes que se recolecte información y durante todo el ciclo de vida de la misma, se deben adoptar medidas preventivas de diversa naturaleza (tecnológica, organizacional. Humana, procedimental) para evitar vulneraciones al derecho a la privacidad o a la confidencialidad de la información."[20]

6.8. Nuevos productos, servicios o canales de recolección de datos personales

Para el desarrollo, estructuración, mejora o modificación de los productos o servicios que presta la compañía, o el desarrollo de planes de mercadeo o adecuaciones tecnológicas, entre otros, en los cuales se tenga que obtener, entregar, almacenar o realizar cualquier tipo de tratamiento o actividad sobre datos personales o bases de datos se deberá contar con el concepto previo y escrito del Oficial de Protección de Datos Personales, quien será el encargado de implementar mecanismos que permitan garantizar la Privacidad por diseño y por defecto en estas nuevas estrategias de la Organización.

6.9. Gestión de Incidentes de Protección de Datos Personales

Los incidentes de protección de datos personales ocurren por varias razones que van desde un simple error humano hasta ataques dirigidos desde el exterior. La gestión eficaz y oportuna de los incidentes en el momento en el que ocurren es crítica para contener el impacto. Los incidentes que no sean atendidos de forma eficaz y oportuna pueden crecer en términos de magnitud y podrían derivar en consecuencias adversas para el TGI, sus clientes, proveedores, colaboradores y demás titulares de la información.

El Oficial de Protección de Datos Personales de TGI deberá conocer, analizar y reportar oportunamente aquellos eventos que se puedan catalogar como Incidentes de seguridad ante la Autoridad de Control en los plazos legales establecidos.

6.10. Gestión de Consultas y Reclamos en Protección de Datos Personales

TGI se encuentra comprometida con el adecuado tratamiento de los datos personales de sus titulares de la información, y por esto, reconocemos la vital importancia de garantizar que estos puedan ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición) en cualquiera de los canales autorizados para dicho efecto, los cuales, se encuentran publicados en nuestra Política de Protección de Datos Personales.

6.11. Procedimientos para el ejercicio de los derechos de Acceso, Rectificación, Cancelación u Oposición (ARCO)

En cumplimiento de las disposiciones constitucionales y legales, TGI como Responsable del Tratamiento de la información personal, debe garantizarles a los titulares de la información el ejercicio de los siguientes derechos:

6.11.1. Conocer, actualizar y rectificar sus Datos Personales.

6.11.2. Solicitar prueba de la autorización otorgada a TGI, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con lo previsto en el artículo 10 de la Ley 1581 de 2012.

6.11.3. Ser informado por TGI, previa solicitud, respecto del Tratamiento que le da a sus Datos Personales.

6.11.4. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen.

[20] Decreto 620 del 2020, artículo 2.2.17.1.6.

6.11.5. Revocar la Autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el Tratamiento nosotros hemos incurrido en conductas contrarias a ley y a la Constitución.

6.11.6. Acceder en forma gratuita a sus Datos Personales que hayan sido objeto de Tratamiento.

6.11.7. Abstenerse de responder preguntas o proporcionar información relacionada a sus Datos sensibles, sin que por esto se condicione alguna actividad o servicio.

Estos derechos podrán ser ejercidos únicamente por las siguientes personas:

a. Por el Titular, quien deberá acreditar su identidad en forma suficiente.

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 o para otro.

Los titulares de la información tienen el derecho a acceder a sus Datos Personales y a los detalles del Tratamiento de dicha información personal, así como a rectificarlos y actualizarlos en caso de ser inexactos, o a solicitar su eliminación cuando considere que resulten ser excesivos o innecesarios para las finalidades que justificaron su obtención, u oponerse al Tratamiento de estos para fines específicos.

6.11.8. Gestión de Consultas

El titular de la información personal directamente o a través de su representante debidamente acreditado podrá:

6.11.8.1. Solicitar el acceso a su información personal.

6.11.8.2. Solicitar la prueba o constancia de la autorización otorgada por usted a TGI para el Tratamiento de su información personal.

6.11.8.3. Consultar el uso de su información personal.

Las consultas deberán ser presentadas a través de los canales habilitados y siguiendo el procedimiento que se describe a continuación:

a. En cualquier momento y de forma gratuita el titular o su representante podrán realizar consultas respecto de los Datos Personales que son objeto de Tratamiento por parte de TGI. En todos los casos, se deberá acreditar la identidad y la facultad para realizar la consulta.

b. La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir del recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado los motivos, señalando la nueva fecha en que será resuelta su consulta, la cual no será superior a los cinco (5) días hábiles siguientes al vencimiento del primer término.

6.11.9. Procedimiento interno para la atención de consultas

Cuando se presente una consulta, se actuará así:

6.11.9.1. Gestión Documental entregará en forma física y/o electrónica la consulta al Oficial de Protección de Datos Personales, quien prestará atención la consulta.

6.11.9.2. El Oficial de Protección de Datos Personales revisará, dentro de los dos días hábiles siguientes, que la consulta se haya presentado por el titular de la información o quien esté legitimado para ello con el cumplimiento de los requisitos establecidos en este manual.

6.11.9.3. Si la consulta no cumple con todos los requisitos establecidos en este manual, esta no se atenderá y se informarán los motivos al remitente.

6.11.9.4. Si la consulta cumple con los requisitos establecidos en este manual, se analizará el objeto de la misma para determinar si se requiere el suministro de información y/o apoyo de otra área de la Organización. De ser así, el Oficial de Protección de Datos Personales remitirá por correo electrónico la consulta al jefe de la respectiva área para que, en el término de dos (2) días hábiles a partir del recibo, se pronuncie de fondo y, si es del caso, allegue la documentación pertinente para atender la consulta.

6.11.9.5. La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atenderla dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se resolverá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

6.11.10. Gestión de Reclamos

El titular podrá solicitar la corrección y actualización de la información personal, la supresión del dato y la revocatoria parcial o total de la autorización entregada a TGI, a través de la presentación de un reclamo que seguirá el siguiente procedimiento.

6.11.10.1 En cualquier momento y de forma gratuita, el titular o su representante podrán realizar reclamaciones respecto de los Datos Personales que son objeto de Tratamiento por parte de TGI. En todos los casos se deberá acreditar la identidad y la facultad para realizar el reclamo.

6.11.10.2 El reclamo será atendido en un término máximo de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el 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.

6.11.11. Procedimiento interno para la atención de reclamos.

Cuando se presente un reclamo, se deberá cumplir con el siguiente procedimiento:

6.11.11.1. Gestión Documental entregará en forma física y/o electrónica el reclamo al Oficial de Protecciónde Datos Personales, quien prestará atención al reclamo.

6.11.11.2. El Oficial de Protección de Datos Personales revisará, dentro de los dos días hábiles siguientes,que el reclamo se haya presentado por el titular de la información o quien esté legitimado para ello con el cumplimiento de los requisitos establecidos en este manual.

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

6.11.11.4. En caso de que TGI no sea competente para resolver el reclamo, dará traslado a quien

corresponda en un término máximo de cinco (5) días hábiles e informará de la situación al interesado.

6.11.11.5. 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 cinco (5) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

6.11.11.6. Se analizará el objeto del reclamo para determinar si se requiere el suministro de información y/o apoyo de otra área de la Organización. De ser así, el Oficial de Protección de Datos Personales remitirá por correo electrónico el reclamo al jefe de la respectiva área para que, en el término dedos hábiles a partir del recibo, se pronuncie de fondo y, si es del caso, allegue la documentaciónpertinente para atender la consulta.

6.11.11.7. El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir deldía siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término,se informará al interesado los motivos de la demora y la fecha en que se resolverá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento delprimer término.

6.11.12. Requisitos para la atención de consultas y reclamos

Los requisitos mínimos establecidos en la Política de Tratamiento de Datos Personales son los estipulados en la Ley 1581 de 2012 normatividad que regula las consultas y reclamos derivados del ejercicio de derecho de Habeas Data, en concordancia con la Ley 1755 de 2015, normatividad que regula el Derecho de Petición en Colombia. De acuerdo a lo anterior, la solicitud debe estar dirigida a TGI y contar como mínimo con los siguientes ítems:

6.11.12.1. Contener la identificación del Titular (nombre y documento de identificación).

6.11.12.2. Contener la descripción de los hechos generadores de la consulta o reclamo.

6.11.12.3. El objeto de la petición.

6.11.12.4. Especificar la dirección de notificación del Titular, ya sea física o electrónica (correo electrónico).

6.11.12.5. Anexar los documentos que se quieren hacer valer (especialmente para reclamos).

Si el titular desea presentar una consulta o un reclamo a través de terceros, previa acreditación de la representación o apoderamiento, la solicitud deberá contener:

a. Identificación del titular que autoriza.

b. Copia de la cédula de ciudadanía o documento de identificación del titular.

c. Nombre, Datos de identificación y copia de la cédula o documento de identificación de la persona autorizada.

d. Tiempo por el cual puede consultar, actualizar o rectificar la información (solo una vez, por un año, por la duración de la relación jurídica, o hasta nueva orden, etc.).

e. Carácter voluntario y libre de la autorización.

f. En todo caso, TGI podrá solicitar documentos adicionales que acrediten la representación o apoderamiento del tercero

Los términos para las respuestas a las consultas y reclamos empezarán a contar a partir de que TGI tenga conocimiento efectivo de su solicitud, a través de los canales establecidos. En el evento en que se desee elevar una queja ante la Superintendencia de Industria y Comercio referida a Datos Personales, recuerde que previamente debe haber agotado el trámite de consulta o reclamo ante TGI, de acuerdo con las indicaciones anteriormente referidas, advirtiendo nuestra total disposición a atender sus inquietudes.

6.11.12. Requisito previo a presentación de quejas ante la Superintendencia de Industria y Comercio

En el evento en que el titular desee elevar una queja ante la Superintendencia de Industria y Comercio referida a Datos Personales, previamente debe haber agotado el trámite de consulta o reclamo ante TGI, de acuerdo con las indicaciones anteriormente referidas, advirtiendo nuestra total disposición a atender sus inquietudes.

6.11.13. Corrección o actualización de Datos Personales del titular

El reclamo consistente en la corrección de Datos Personales deberá contener además de los requisitos establecidos anteriormente, la especificación de las correcciones a realizar y acompañarse de la documentación que avale su petición.

6.11.14. Revocatoria parcial o total de la autorización del Tratamiento

Los Titulares de Datos Personales tienen derecho a revocar la autorización cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales, lo cual procederá en aquellos casos en los que presentada la solicitud la Organización así lo determina o en los cuales, la autoridad de protección de Datos Personales lo ordene. No obstante, si la Organización considera que no es procedente la revocación así lo informará mediante comunicación motivada. Por su parte, revocada la autorización la Organización procederá a eliminar de las bases de Datos respectivas las informaciones en ellas contenidas.

6.11.15. Canales de atención de Consultas y Reclamos

TGI ha implementado los siguientes canales para garantizar el ejercicio de los derechos de los titulares. Los canales establecidos son:

6.11.15.1. El correo electrónico: datospersonales@tgi.com.co

6.11.15.2. A la dirección Carrera 9 No. 73 – 44 Pisos 2, 3 y 7

Estos canales podrán ser utilizados por los Titulares de Datos Personales, o terceros autorizados por ley para actuar en su nombre, con el objeto de ejercer sus derechos.

6.11.16. Sobre el área responsable de dar trámite a las consultas y reclamos.

TGI a través del Oficial de Protección de Datos Personales, quien hace parte de la Dirección de Cumplimiento, atenderá todas las peticiones, consultas y reclamos de los Titulares de la información para que puedan ejercer sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización relacionados con la protección de Datos Personales.

6.12. Programa de Formación en Protección de Datos Personales

TGI entiende que, para garantizar un adecuado tratamiento de los datos personales de sus titulares de la información, debe propender por generar espacios de conocimiento que consoliden la cultura de Cumplimiento y Protección de Datos al interior de la Organización y en sus colaboradores.

Por esto, nuestra Organización cuenta con un Programa de Formación en Protección de Datos Personales, mediante el cual forma a sus colaboradores en el adecuado tratamiento de los datos

personales de los titulares de la información de TGI, y su rol para garantizar el cumplimiento de los lineamientos de la Organización en materia de Protección de Datos Personales.

El Oficial de Protección de Datos Personales es responsable de diseñar, administrar y supervisar el Programa de formación en materia de Protección de Datos Personales al interior de TGI. La ejecución de este programa será realizada de manera conjunta por el Oficial de Protección de Datos Personales y el área de formación TGI.

El programa de formación cuenta con diferentes mecanismos mediante los cuales se educa a nuestros colaboradores en protección de datos personales. Dichos mecanismos se relacionan a continuación:

6.12.1. Programas de capacitación, internos o externos, en materia de protección de datos personales a todos los colaboradores (nuevos y antiguos) de la compañía.

6.12.2. Programas de capacitación especiales, internos o externos, para la alta dirección y para aquellos colaboradores que por el tipo de función que desempeñan tengan mayor responsabilidad en gestión de datos personales.

6.12.3. Programas de capacitación para aliados estratégicos que realicen tratamiento de datos personales en nombre de la compañía.

6.12.4. Mediciones sobre la evaluación y participación de los colaboradores.

6.12.5. Establecer un banco de preguntas para las evaluaciones.

6.13. Gobierno Interno de Protección de Datos Personales

En su calidad de Responsable del Tratamiento de Datos Personales, TGI comprende la importancia de dar cumplimiento al Principio de Responsabilidad Demostrada desarrollado por el Decreto 1377 de 2013 y por la Guía para la Implementación del Principio de Responsabilidad Demostrada de la SIC. En razón a lo anterior, ha implementado medidas y/o políticas internas apropiadas y efectivas para dar cumplimiento a la Ley aplicable, en cuanto a la protección integral de Datos Personales. Como parámetro para el planteamiento de estas medidas se ha seguido lo establecido del artículo 27 del Decreto 1377 de 2013 al exigir que las medidas deben garantizar:

- La existencia de una estructura administrativa proporcional a la estructura y tamaño empresarial del Responsable para la adopción e implementación de políticas consistentes con la Ley aplicable.
- La adopción de mecanismos internos para poner en práctica estas políticas incluyendo herramientas de implementación, entrenamiento y programas de educación.
- La adopción de procesos para la atención y respuesta a consultas, peticiones y reclamos de los Titulares, con respecto a cualquier aspecto del Tratamiento.

6.13.1. Estructura Administrativa y de Cumplimiento

Con el fin de procurar altos estándares de cumplimiento de la regulación en materia de protección de datos, se asignan determinadas funciones a algunas áreas de la organización, quienes tendrán las siguientes funciones:

6.13.1.1. Junta Directiva

La junta directiva tendrá las funciones de:

- Apoyar mediante el suministro de los recursos económicos y de personal a TGI para la administración y funcionamiento del Programa de Protección de Datos;
- Revisar y pronunciarse sobre el informe de gestión de la Dirección de cumplimiento respecto del programa de protección de datos personales.

6.13.1.2. Alta Dirección

La alta dirección de TGI es responsable de la gestión del riesgo de incumplimiento al programa de protección de datos como parte de sus responsabilidades generales para la gestión del riesgo de cumplimiento. Esta es responsable de crear un entorno de control apto y contribuir al sostenimiento de una cultura de la protección de datos robusta y efectiva. Para lo anterior desde la alta dirección se llevan a cabo las siguientes funciones:

6.13.1.2.1. Apoyar y generar al interior de TGI una cultura de respeto a la protección de datos;

6.13.1.2.2. Aprobar la política de protección de datos personales.

6.13.1.2.3. Apoyar y socializar al interior de los equipos las iniciativas de comunicaciones, capacitaciones y recolección de información asociada al desarrollo del programa de PDP.

6.13.1.2.4. Designar y nombrar al Oficial de Protección de Datos Personales de TGI.

6.13.1.3. Dirección de Cumplimiento

La Dirección de cumplimiento tendrá las siguientes funciones:

6.13.1.3.1. Presentar a la Junta Directiva y a la alta dirección un informe periódico, por lo menos una vez al año sobre el funcionamiento, cumplimiento y monitoreo del programa de protección de datos.

6.13.1.3.2. Realizar la definición, ejecución y monitoreo del Programa de Protección de Datos Personales, asegurando el cumplimiento normativo.

6.13.1.3.3. Informar al comité de ética y cumplimiento cualquier desviación, oportunidad de mejora sobre el programa de protección de datos personales, así como, los monitoreos y seguimientos que se realicen sobre el mismo.

6.13.1.4. Comité de Auditoría y Riesgos de la Junta Directiva

El Comité de Auditoría y Riesgos de la Junta Directiva tendrá las siguientes funciones en lo relacionado con Protección de Datos Personales:

6.13.1.4.1. Revisar y evaluar los informes periódicos que presente la Dirección de Cumplimiento y/o el Oficial de Protección de Datos Personales sobre el cumplimiento y demás temas relacionados con el Programa de Protección de Datos Personales de TGI.

6.13.1.4.2. Adoptar las decisiones que consideren pertinentes para que al interior de la Organización se dé un adecuado cumplimiento en materia de protección de datos personales.

6.13.1.4.3. Impulsar la consolidación de la cultura organizacional de Protección de Datos Personales.

6.13.1.5. Oficial de Protección de Datos Personales

El Oficial de Protección de Datos Personales tendrá las siguientes funciones:

6.13.1.5.1. Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.

6.13.1.5.2. Liderar la elaboración e implementación de un sistema que permita administrar los riesgos del tratamiento de datos personales.

6.13.1.5.3. Ser el enlace y coordinar con las demás áreas de la organización para implementar el Programa Integral de Gestión de Datos Personales.

6.13.1.5.4. Definir e impulsar una cultura de protección de datos dentro de la organización.

6.13.1.5.5. Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.

6.13.1.5.6. Obtener las declaraciones de conformidad de la SIC cuando sea requerido.

6.13.1.5.7. Revisar junto con el área jurídica los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.

6.13.1.5.8. Adoptar las medidas necesarias con el fin de atenuar los posibles daños que se puedan producir como consecuencia del incumplimiento del régimen de protección de datos.

6.13.1.5.9. Informar a la SIC, previa notificación del Oficial de Seguridad de la Información, cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

6.13.1.5.10. Analizar junto con el Responsable del área de Recursos Humanos, las responsabilidades de cada cargo de la organización, para: i) sugerir cambios en los manuales de funciones; ii) diseñar un programa de entrenamiento en protección de datos específico para cada uno de ellos y iii) definir -en qué casos se deben firmar acuerdos especiales de confidencialidad.

6.13.1.5.11. Definir y realizar un entrenamiento general en protección de datos para todos los empleados de la compañía; este entrenamiento podrá ser presencial, virtual o mixto. Realizar un entrenamiento diferencial a los empleados, nuevos y antiguos, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.

6.13.1.5.12. Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización, como pueden ser: recursos humanos, seguridad, contabilidad, jurídica y abastecimiento, entre otros.

6.13.1.5.13. Medir la asistencia a los entrenamientos o capacitaciones y evaluar el desempeño de cada uno de los participantes.

6.13.1.5.14. Hacer seguimiento a la implementación de planes de auditoría interna para verificar el cumplimiento de sus políticas de tratamiento de la información personal.

6.13.1.5.15. Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.

6.13.1.5.16. Realizar seguimiento al Programa Integral de Gestión de datos personales

6.13.1.6. Vicepresidencia de Talento Humano y Gestión Administrativa

6.13.1.6.1. Apoyar al Oficial de protección de datos personales en las capacitaciones y/o entrenamientos que deban realizarse al interior de TGI.

6.13.1.6.2. Apoyar al Oficial de protección de datos personales en la revisión y adecuación de los manuales de funciones de los cargos que tengan que administrar o gestionar Datos Personales.

6.13.1.6.3. Establecer, cuando se considere, como un punto a tener en cuenta en el desempeño de los empleados, su participación y resultados de la evaluación en los procesos de capacitación sobre protección de datos personales.

6.13.1.7. Oficial de seguridad de la información

6.13.1.7.1. Definir los medios para conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

6.13.1.7.2. Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.

6.13.1.7.3. Informar inmediatamente al Oficial de protección de datos personales cualquier incidente de seguridad en materia de protección de datos.

6.13.1.7.4. Establecer las medidas, procesos, controles de seguridad requeridos por la organización para cumplir con el principio de seguridad en materia de protección de datos personales.

6.13.1.7.5. Realizar controles periódicos a los sistemas de seguridad, documentarlos y ejecutar las gestiones necesarias para, si es del caso, modificarlas, ampliarlas o corregirlas.

6.13.1.7.6. Apoyar activamente al Oficial de protección de datos personales en todas las actividades o gestiones que requiera la Organización a fin de dar cumplimiento en materia de protección de datos.

6.13.1.7.7. Establecer protocolos para atender los incidentes de seguridad de la información. Estos protocolos deberán prevenir las acciones a seguir antes, durante y después de cada incidente.

6.13.1.8. Gerente de Auditoría Interna

Realizar auditorías internas para verificar el cumplimiento de la normatividad vigente y políticas internas en materia de protección de datos personales

6.14. Auditorías, controles y seguimiento

El área de Cumplimiento definirá los controles y seguimientos que se deban establecer para asegurar el cumplimiento de la ley de protección de datos personales, que la implementación al interior de la compañía se está realizando adecuadamente y los procesos para ajustar los puntos que puedan ser mejorados.

Para lo anterior deberán tener en cuenta al menos los siguientes puntos:

6.14.1. Procesos de recolección de información.

6.14.2. Actividades de uso o utilización de información.

6.14.3. Transferencia y transmisión de información.

6.14.4. Gestión de los encargados del tratamiento.

6.14.5. Eliminación y/o supresión de información.

6.14.6. Atención de quejas y reclamos.

6.14.7. Procesos y medidas de seguridad.

6.14.8. Formación y capacitación.

6.14.9. Cumplimiento reforzado cuando se realice tratamiento de datos sensibles o de menores de edad.

Así mismo, los controles y su periodicidad tendrán en cuenta el tipo de información, el tipo de tratamiento de los datos, el área encargada del tratamiento, entre otros temas que consideren adecuados.

6.15. Administración de riesgos asociados a Protección de Datos Personales

TGI garantizará mediante un Sistema de Administración de Riesgos asociados a la protección de datos personales, la identificación, medición, control y monitoreo de todos aquellos hechos o situaciones que puedan incidir en la debida administración del riesgo al que TGI se encuentra expuesta en esta materia. El Oficial de Protección de Datos Personales garantizará la administración del Sistema de Administración de Riesgos de Privacidad.

7. POLÍTICA PARA LA CIRCULACIÓN DE DATOS PERSONALES

7.1. Ámbito de aplicación

Las disposiciones contenidas en la presente política serán aplicables a todas aquellas formas de circulación de los datos personales que realice TGI, toda vez que en su calidad de Responsable del tratamiento de los datos personales deberá garantizar el cumplimiento de los principios de acceso y circulación restringida, seguridad y confidencialidad consagrados en la Ley 1581 de 2012.

7.2. Transmisión de datos personales

El Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015, define en su artículo tercero (3°), la transmisión de datos personales como aquel 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.

TGI en el cumplimiento de su objeto social podrá transmitir los datos personales de sus titulares de la información a terceros, que ostentarán la calidad de encargados del tratamiento de los datos personales objeto de la transmisión.

Atendiendo la obligación legal de gestionar los encargados del tratamiento de la información personal, la Organización ha previsto las siguientes acciones a efectos de revisar, entre otros, que los encargados del tratamiento están utilizando la información para los fines establecidos en la ley, en los contratos y en las autorizaciones; así como si se cumplen o no las medidas o estándares de seguridad exigidos.

7.2.1. Solicitud de informes o certificaciones a los encargados

7.2.2. Verificación de los estándares de seguridad

7.2.3. Otras actividades tendientes a verificar la gestión de los Encargados.

El tipo de acción a seguir y la periodicidad con la cual se realizará será determinado por el Oficial de Protección de Datos Personales, teniendo en cuenta el tipo de información remitida a los encargados, el tipo de tratamiento que se haya establecido, el tipo de encargado o empresa, entre otros.

TGI realiza Transmisiones de Datos Personales de trabajadores, oferentes, contratistas, clientes y proveedores a terceros ubicados dentro o fuera de Colombia, en calidad de Encargados, para realizar el Tratamiento de los Datos Personales por cuenta de TGI. Por lo tanto, TGI ha implementado las Autorizaciones y/o Contratos de Transmisión necesarios para tal fin, de conformidad con las disposiciones legales aplicables.

El contrato que suscriba TGI con los Encargados para el Tratamiento de Datos Personales bajo su control y responsabilidad señalará los alcances del Tratamiento, las actividades que el Encargado realizará por cuenta del Responsable para el Tratamiento de los Datos Personales y las obligaciones del Encargado para con el Titular y el Responsable.

Mediante la suscripción de cláusulas contractuales de Transmisión de Datos o Contratos de Transmisión de Datos Personales, TGI define el alcance del tratamiento que realizará el encargado, las obligaciones y deberes del encargado del tratamiento con el Responsable o con los titulares del tratamiento, las finalidades del tratamiento, el cumplimiento de la Política de Tratamiento de Datos Personales de TGI, la salvaguarda de la seguridad de las bases de datos en los que se contengan datos personales por parte del encargado, la obligación de confidencialidad respecto del tratamiento de los datos personales transmitidos, entre otros aspectos de vital importancia para la regulación de la trasmisión de los datos personales.

Estos aspectos regulados, dan cumplimiento a lo establecido por el artículo 25 del Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015, mediante el cual se definen los parámetros legales para los contratos de Trasmisión de Datos Personales o las cláusulas contractuales para la Trasmisión de Datos Personales.

Si la Organización entrega sus bases de datos a algún encargado del Tratamiento se deberán relacionar en este aparte si son personas naturales o jurídicas; cuál es la forma de entrega o acceso a la información y qué tipo de Tratamiento puede realizar el encargado. Además, se deberá: (i) determinar quién será la persona que al interior de TGI realizará las labores de seguimiento, gestión y control a los Encargados del Tratamiento; y (ii) definir si la compañía permite o no que terceros recolecten información en su nombre, a través de que documentos y cuáles serán las exigencias a estos terceros.

El colaborador responsable al interior de TGI deberá garantizar, previa transmisión de los datos personales, que medie la suscripción del Contrato de Transmisión de datos Personales. La omisión a este deber constituirá falta grave de conformidad con lo establecido en el Reglamento Interno de Trabajo.

Para el efecto, el colaborador deberá verificar si en el caso concreto aplica la minuta estándar de contratos de abastecimiento (adquisición de bienes y servicios), caso en el cual no será necesario suscribir un documento adicional, toda vez que dicha minuta contiene las disposiciones que regulan la relación entre Encargado y Responsable del Tratamiento.

En caso de que no medie un contrato estándar de abastecimiento, deberá asegurarse de que se firme el *Contrato de Transmisión*.,

7.3. Transmisión internacional de datos personales

El artículo 24 del Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015, establece las reglas aplicables para las transferencias y transmisiones internacionales de datos personales.

Respecto de la transmisión internacional de datos personales, indica el mencionado artículo que:

> *"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 cuando exista un contrato en los términos del artículo 25 siguiente."*

En cumplimiento del mandato legal expuesto, TGI como se mencionó anteriormente, cuenta con la inclusión de cláusulas contractuales o Contratos de Transmisión de Datos Personales, que permitan dar cumplimiento al artículo 25 del Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015. Lo anterior, especialmente cuando se realizarán transmisiones internacionales de datos personales.

7.4. Transferencia de datos personales

El Decreto 1377 de 2013, compilado en el Decreto 1074 de 2015, define en su artículo tercero (3°), la transferencia de datos personales como aquella que 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.

TGI en el marco de alianzas estratégicas, prestaciones de servicios, u operaciones entre nuestras compañías vinculadas, podrá eventualmente transferir datos personales de sus titulares de la información a dichos terceros, quienes ostentarán la condición de Responsables del Tratamiento de dichos datos personales, a partir del momento de la transferencia. TGI únicamente transferirá datos personales de aquellos titulares de la información que hayan otorgado su consentimiento para la transferencia de sus datos personales.

7.5. Transferencia internacional de datos personales

La Ley 1581 de 2012 consagra en su artículo 26 la prohibición general de transferencia internacional de datos personales:

> *"(…)* ***Artículo 26. Prohibición.*** *Se prohíbe la transferencia de datos personales de cualquier tipo 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:*
>
> *a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia;*
>
> *b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública;*
>
> *c) Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable;*
>
> *d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;*
>
> *e) 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;*
>
> *f) Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.*

PAR. 1º—En los casos no contemplados como excepción en el presente artículo, corresponderá a la Superintendencia de Industria y Comercio, proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. Para el efecto, el Superintendente queda facultado para requerir información y adelantar las diligencias tendientes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

PAR. 2º—Las disposiciones contenidas en el presente artículo serán aplicables para todos los datos personales, incluyendo aquellos contemplados en la Ley 1266 de 2008 (…)"

De acuerdo con lo estipulado por el artículo 26 de la Ley 1581 de 2012 existen 3 supuestos que habilitan la transferencia internacional de datos personales, los cuales son:

7.5.1. 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.

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

7.5.3. 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 la Circular 005 de 2017 la Superintendencia de Industria y Comercio ("en adelante SIC) adiciona el Capítulo Tercero al Título V de la Circular Única, precisando aspectos importantes sobre la transferencia internacional de datos personales.

En primer lugar, respecto de los estándares de medición del nivel adecuado de protección de un país receptor de datos personales transferidos desde Colombia, la SIC acató lo establecido por la Corte Constitucional en la Sentencia C-748 de 2011, la cual consideró:

"(...) Se entenderá que un país cuenta con los elementos o estándares de garantía necesarios para garantizar un nivel adecuado de protección de datos personales, si su legislación cuenta: con unos principios, que abarquen las obligaciones y derechos de las partes (titular del dato, autoridades públicas, empresas, agencias u otros organismos que efectúen tratamientos de datos personales), y de los datos (calidad del dato, seguridad técnica) y; con un procedimiento de protección de datos que involucre mecanismos y autoridades que efectivicen la protección de la información. De lo anterior se deriva que el país al que se transfiera los datos no podrá proporcionar un nivel de protección inferior al contemplado en este cuerpo normativo que es objeto de estudio (…)".

Acatando las recomendaciones de la Corte Constitucional y teniendo como base diferentes estudios legales realizados por la SIC, el ente de control estableció los siguientes estándares de un nivel adecuado de protección del país receptor de la información personal:

"(…) ***3.1. Estándares de un nivel adecuado de protección del país receptor de la información personal.***

El análisis para establecer si un país ofrece un nivel adecuado de protección de datos personales, a efectos de realizar una transferencia internacional de datos, estará orientado a determinar si dicho país garantiza la protección de los mismos, con base en los siguientes estándares:

a) Existencia de normas aplicables al tratamiento de datos personales.

b) Consagración normativa de principios aplicables al tratamiento de datos, entre otros: legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

c) Consagración normativa de derechos de los titulares.

d) Consagración normativa de deberes de los responsables y encargados.

e) Existencia de medios y vías judiciales y administrativas para garantizar la tutela efectiva de los derechos de los titulares y exigir el cumplimiento de la ley.

f) Existencia de autoridad (es) pública (s) encargada (s) de la supervisión del tratamiento de datos personales, del cumplimiento de la legislación aplicable y de la protección de los derechos de los titulares, que ejerza (n) de manera efectiva sus funciones. (…)"

Seguidamente la SIC, mediante la Circular 002 de 2018 la SIC modifica el numeral 3.2 del Capítulo Tercero del Título V de la Circular Única, establece una lista de países que cuentan con un nivel adecuado de protección de datos personales, considerando:

"(…) ***3.2. Países que cuentan con un nivel adecuado de protección de datos.*** *Teniendo en cuenta los estándares señalados en el numeral 3.1. anterior y el análisis adecuado de protección los siguientes países: Alemania; Australia; Austria; Bélgica; Bulgaria; Chipre; Costa Rica; Croacia; Dinamarca, Eslovaquia; Eslovenia; Estonia; España; Estados Unidos de América; Finlandia; Francia; Grecia; Hungría; Irlanda; Islandia; Italia; Japón; Letonia; Lituania; Luxemburgo; Malta; México; Noruega; Países Bajos; Perú; Polonia; Portugal; Reino Unido; República Checa; República de Corea; Rumania; Serbia; Suecia y los países que han sido declarados con el nivel adecuado de protección por la comisión Europea. (…)*

La Superintendencia de Industria y Comercio ejercerá, en cualquier tiempo, su capacidad regulatoria para revisar la lista anterior y proceder a incluir a quienes no hacen parte de la misma o para excluir a quien se considere conveniente, de acuerdo con los lineamientos establecidos en la ley.

PAR. 1º—Sin perjuicio de que las transferencias de datos personales se realicen a países que tienen un nivel adecuado de protección, los responsables del tratamiento, en virtud del principio de responsabilidad demostrada, deben ser capaces de demostrar que han implementado medidas apropiadas y efectivas para garantizar el adecuado tratamiento de los datos personales que transfieren a otro país y para otorgar seguridad a los registros al momento de efectuar dicha transferencia.

PAR. 2º—Cuando la transferencia de datos personales se vaya a realizar a un país que no se encuentre dentro de los relacionados en el presente numeral, corresponderá al Responsable del tratamiento que efectuará la transferencia verificar si la operación está comprendida dentro de una de las causales de excepción establecidas en el artículo 26 de la Ley 1581 de 2012, o, si ese país cumple con los estándares fijados en el numeral 3.1 anterior, casos en los cuales podrá realizar la trasferencia, o, de no cumplirse ninguna de las condiciones anteriores, solicitar la respectiva declaración de conformidad ante esta Superintendencia.

PAR. 3º—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.

PAR. 4º—Es posible realizar la transmisión de datos personales a los países que cuentan con un nivel adecuado de protección de datos personales, en los términos que rigen la transferencia de datos personales.

Teniendo en cuenta la modificación al listado de países que cuentan con un nivel adecuado de protección de datos incorporada por la Circular 002 de 2018, los países considerados seguros para la transferencia internacional de datos personales son:

Listado de países que cuentan con un nivel adecuado de protección de datos				
Alemania	Australia	Austria	Bélgica	Bulgaria
Chipre	Costa Rica	Croacia	Dinamarca	Eslovaquia
Eslovenia	Estonia	España	Estados Unidos de América	Finlandia
Francia	Grecia	Hungría	Irlanda	Islandia
Italia	Japón	Letonia	Lituania	Luxemburgo
Malta	México	Noruega	Países bajos	Perú
Polonia	Portugal	Reino Unido	República Checa	República de Corea
Rumania	Serbia	Suecia		

Teniendo en cuenta el marco legal expuesto, TGI validará de manera previa a la realización de cualquier transferencia internacional de datos personales, lo siguiente:

a) Si la operación de transferencia se encuentra enmarcada dentro de las excepciones fijadas por el artículo 26 de la Ley 1581 de 2012.

b) Si el país receptor se encuentra en el listado de países con niveles adecuados de protección de datos personales, y establecidos en la Circular 002 de 2018 de la SIC.

c) Si el país receptor no se encuentra en el listado de países, se deberá validar si este país 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.

Si producto de la verificación de los requisitos mencionados anteriormente, TGI tiene como resultado que los mismos no se cumplen, éste deberá solicitarle a la SIC que en ejercicio de sus facultades legales se pronuncie sobre la transferencia internacional de los datos personales tramitando ante esta entidad una solicitud para que le sea expedida una Declaración de Conformidad.

La solicitud de Declaración de Conformidad no deberá realizarse por TGI en el supuesto contemplado por el parágrafo primero del numeral 3.3 de la Circular 005 de 2017, el cual dispone:

> *"(…)* ***PAR. 1º—*** *Cuando los responsables del tratamiento, que a efectos de cumplir con el principio de responsabilidad demostrada, suscriban un contrato con el responsable del tratamiento destinatario de los datos o implementen otro instrumento jurídico mediante el cual señalen las condiciones que regirán la transferencia internacional de datos personales y mediante las cuales garantizarán el cumplimiento de los principios que rigen el tratamiento, así como de las obligaciones que tienen a cargo, se presumirá que la operación es viable y que cuenta con declaración de conformidad.*
>
> *En consecuencia, los responsables del tratamiento podrán realizar dicha transferencia, previa comunicación remitida a la delegatura para la protección de datos personales de la Superintendencia de Industria y Comercio, mediante la cual informen sobre la operación a realizar y declaren que han suscrito el contrato de transferencia u otro instrumento jurídico que garantice la protección de los datos personales objeto de transferencia, lo cual podrá ser verificado en cualquier momento por esta superintendencia y, en caso de que se evidencie un incumplimiento, podrá*

adelantar la respectiva investigación e imponer las sanciones que correspondan y ordenar las medidas a que haya lugar (…)".

Por tanto, si TGI suscribe un Contrato de Transferencia Internacional de Datos Personales con el receptor que contemple las condiciones que regirán la transferencia internacional de datos personales y las cuales garantizaran el cumplimiento de los principios que rigen el tratamiento, así como las obligaciones que se tienen a cargo, nuestra Organización podrá acogerse a la excepción del precitado parágrafo, y únicamente comunicará a la SIC la operación a realizar y la declaración de la suscripción del Contrato de Transferencia Internacional de Datos Personales.

7.6. Tratamiento de datos personales Transmitidos o Transferidos por terceros

TGI en cumplimiento de su objeto social podrá realizar el tratamiento de datos personales transmitidos o transferidos por terceros en el marco de alianzas estratégicas, contratos de prestación de servicios, operaciones entre compañías vinculadas, entre otros.

Nuestra Organización en calidad de Responsable del Tratamiento de los datos personales y en cumplimiento de lo establecido por la Ley 1581 de 2012, llevará a cabo todas aquellas actividades necesarias para tener la certeza sobre la legitimación jurídica respecto de la recolección, uso y circulación de los datos personales transmitidos o transferidos por terceros a su favor.

Dado lo anterior, TGI no realizará el tratamiento de los datos personales que le sean transmitidos o transferidos por terceros sin el cumplimiento de los siguientes presupuestos:

7.6.1. El Tercero que transfiera o transmita datos personales a TGI deberá estar autorizado de manera previa, expresa e informada por el titular de los datos personales para: (i) Transmitir o transferir sus datos personales a terceros; (ii) Dicha transferencia o Transmisión debe autorizarse para que el tercero receptor de la información pueda realizar el tratamiento de la misma.

7.6.2. En el evento en que los datos personales sean transmitidos o transferidos por Terceros para que TGI los utilice para fines de publicidad, mercadeo, marketing o mercadotecnia, la Organización verificará que el Tercero se encuentre debidamente facultado por el titular para dichos fines. Esta revisión deberá ser realizada por el dueño de la alianza/contrato/relación y apoyada por el Oficial de Protección de Datos Personales.

Para el cumplimiento de los supuestos mencionados TGI podrá utilizar diferentes mecanismos que le permitan efectivamente comprobar que el Tercero, en efecto se encuentra autorizado de manera previa, expresa e informada por el titular de los datos personales para el tratamiento de la información personal. Entre los mecanismos que TGI podrá utilizar para comprobar lo anterior se encuentran:

a) Solicitudes a los Terceros de las autorizaciones para el tratamiento de los datos personales otorgadas a su favor por los titulares de los datos personales que son objeto de transmisión o transferencia. TGI podrá verificar que las autorizaciones suministradas cumplan los supuestos mencionados.

b) Auditorías a los Terceros en las cuales se verifique que estos dan cumplimiento al Régimen de Protección de Datos Personales – Ley 1581 de 2012-, especialmente a los requisitos para la recolección y circulación de datos personales.

c) Declaraciones contractuales o certificaciones expedidas por los Terceros en las que se exprese el cabal cumplimiento de estos al Régimen de Protección de Datos Personales – Ley 1581 de 2012-, especialmente a los requisitos para la recolección y circulación de los datos personales transmitidos o transferidos a TGI.

En el evento en el cual el titular de los datos personales transferidos o transmitidos a TGI por los Terceros manifieste a TGI su solicitud de revocatoria a la autorización otorgada, nuestra Organización dará trámite a la solicitud conforme a nuestra Política de Tratamiento de Datos Personales y garantizará al titular el ejercicio de sus derechos.

Adicionalmente, TGI podrá implementar medidas contractuales en todos aquellos contratos, convenios o alianzas suscritas con los Terceros que propendan por el cumplimiento del Régimen de Protección de Datos Personales – Ley 1581 de 2012- durante y una vez finalizada la relación contractual o comercial.

7.7. Cumplimiento de la Ley 1581 de 2012 por parte de los terceros que transmiten o transfieren datos personales

El Oficial de Protección de Datos Personales de TGI, realizará un análisis de aquellos contratos, convenios o alianzas comerciales suscritas por TGI, las cuales, conlleven la transmisión o transferencia de datos personales de titulares de la información, para lo cual, se tendrán en cuenta el tipo de tratamiento realizado, la naturaleza de los datos personales, el volumen de la información personal y los medios de transferencia o transmisión.

De manera particular se verificará:

- La existencia de una Política de Protección de Datos Personales.
- La existencia de canales de atención dispuestos para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición (ARCO) de los titulares de la información.
- La existencia de políticas o procedimientos para garantizar la seguridad de la información.
- La existencia de políticas o procedimientos para garantizar la gestión de consultas y reclamos en materia de protección de datos personales.

En el evento en que, como resultado de la verificación del cumplimiento del tercero, se evidencie que el mismo no cumple con los estándares mínimos en protección de datos personales, el Oficial de Protección de Datos Personales proyectará un plan de acción con el dueño del contrato/alianza/relación con el propósito de alcanzar un adecuado cumplimiento.

7.8. Solicitudes de información de entidades públicas o administrativas

TGI está comprometido con el apoyo a la administración pública en todo tipo de investigaciones tanto de carácter fiscal o administrativo. En este sentido, para la atención de solicitudes de información por parte de cualquier autoridad pública se procederá de la siguiente manera:

7.8.1. La solicitud o requerimiento debe estar por escrito (correo electrónico o comunicación física).

7.8.2. Si el requerimiento implica suministrar datos personales, el área responsable debe remitir el requerimiento al Oficial de Protección de Datos Personales.

7.8.3. Verificar el tipo de entidad pública.

7.8.4. Revisar el tipo de información solicitada.

7.8.5. Si la solicitud establece la finalidad para la cual se requiere la información y las funciones conferidas por la ley para tal finalidad.

7.8.6. Señalar a la entidad pública que al recibir esta información deberá garantizar los derechos fundamentales del titular de la información, de acuerdo con lo previsto en la sentencia C-748 de 2011deberá "(i) guardar reserva de la información que les sea suministrada por los operadores y utilizarla únicamente para los fines que justificaron la entrega, esto es, aquellos relacionados con la competencia funcional específica que motivó la solicitud de suministro del dato personal; (ii) informar a los titulares del dato el uso que le esté dando al mismo; (iii) conservar con las debidas seguridades la información recibida para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento; y (iv) cumplir con las instrucciones que imparta la autoridad de control, en relación con el cumplimiento de la legislación estatutaria."

7.8.7. Los requerimientos deberán contestarse dentro del plazo de ley.

8. POLÍTICA PARA EL ALMACENAMIENTO DE DATOS PERSONALES

8.1. Ámbito de aplicación

Gestionar la información personal almacenada en repositorios físicos y digitales con medidas alcanzables que disminuyan sustancialmente los riesgos de privacidad a los que se encuentra expuesta la Organización en el ejercicio de la labor diaria. Con esto se garantizará el cumplimiento del principio de seguridad consagrado en la Ley 1581 de 2012.

8.2. Del almacenamiento en repositorios físicos

Todos los colaboradores de la Organización deberán dar cabal cumplimiento a lo dispuesto en el *Programa de Gestión Documental,* sin embargo, adicionalmente a las medidas impuestas en dicho programa, se deberá garantizar el cumplimiento de las siguientes recomendaciones, con el fin de dar cabal cumplimiento a la Ley 1581 de 2012.

8.2.1. **Acceso a los archivadores físicos.** Todo archivador o repositorio físico de información (entiéndase armario, estantería, archivadores rodantes) deberá encontrarse en áreas cuyo acceso esté protegido mediante controles de acceso que indiquen las restricciones de movilidad de estación de archivo. Se entenderá por archivo el espacio (aula, salón, cuarto, bodega o equivalente) donde se encuentran los archivadores físicos.

8.2.2. **No apertura al público.** Los archivadores físicos o repositorios de información serán ubicados en espacios o áreas que no permitan el acceso al público, entendiendo por este todo el personal ajeno al que maneja la información directamente.

8.2.3. **Responsables de los archivos físicos.** El área dueña de los repositorios físicos dispondrá que existan los controles pertinentes para él y salida de los documentos depositados en el repositorio físico.

El personal encargado de la administración documental deberá tener inventariados los documentos que se conservan en el archivo que está bajo su custodia, así como advertir a la Dirección de Servicios Administrativos o quien haga sus veces de los riesgos de pérdida o deterioro de los mismos.

Esta tarea deberá ser controlada por el área de administración de documentos de la Organización.

8.2.4. **Manejo de la información fuera del archivo.** Cuando los documentos contentivos de datos personales no se encuentren guardados en sus respectivos archivos físicos, la persona que se encuentre a cargo de los mismos deberá custodiarlos e impedir en todo momento que puedan ser obtenidos o consultados por personas no autorizadas. En el evento en que, el encargado transitorio de la custodia de la información por fuera del archivo sufra un percance con la manipulación de la misma, estará obligado a realizar un reporte de lo sucedido, en el cual se deberá indicar lo siguiente:

8.2.4.1. Fecha de ocurrencia del percance.

8.2.4.2. Los documentos/carpetas o textos involucrados con el mismo.

8.2.4.3. Recuento factico de lo sucedido, siendo lo más concreto posible.

Toda perdida de información confidencial deberá informarse a la Dirección de Servicios Administrativos o quien haga sus veces, para que se tomen las acciones correspondientes.

Adicionalmente, la Dirección de Servicios Administrativos o quien haga sus veces deberá reportar el incidente al Buzón datospersonales@tgi.com.co, de propiedad del Oficial de Protección de Datos Personales.

Información transitoria. La Información Transitoria (documentos transitorios) puede ser conservada por el término que establezca Gestión Documental, los registros transitorios los cuales son catalogados como documentos de apoyo al proceso realizado en las áreas no se encuentran registrados en las tablas de retención documental, por lo tanto es responsabilidad del líder del proceso del área conservar la información, sin que se aplique la tabla de retención documental.

8.3. Del almacenamiento en repositorios digitales

Todos los colaboradores de la Organización deberán dar cabal cumplimiento a lo dispuesto en el Modelo *de Seguridad y Privacidad de la Información de* TGI*,* sin embargo, adicionalmente a las medidas impuestas en dicho Modelo, se deberá garantizar el cumplimiento de las siguientes recomendaciones, con el fin de dar cabal cumplimiento a la Ley 1581 de 2012.

8.3.1. **Responsabilidad de los usuarios.** Todos los usuarios de los servicios de información – software- son responsables del manejo de sus datos de autenticación para el uso y acceso a los recursos informáticos de TGI. Los usuarios deben mantener en secreto su información de autenticación a los sistemas.

8.3.1.1. Los usuarios son responsables de todas las actividades realizadas con su identificador en la red ID (usuario de red).

8.3.1.2. Los usuarios deben hacer un correcto uso de la información a la cual tienen acceso.

8.3.1.3. Los usuarios no deben divulgar las claves de acceso o contraseñas de los dispositivos y sistemas informáticos de la entidad.

8.3.1.4. Los usuarios pueden hacer uso de los datos e información contenidos en los recursos informáticos de la entidad solo para fines laborales.

8.3.2. **Gestión de accesos.** La Dirección de Tecnologías de la Información o quien haga sus veces deberá limitar y controlar el uso de accesos y privilegios a los usuarios mediante procesos de autorización formal, para evitar el uso inadecuado de privilegios y prevenir fallas en la operación de los sistemas de información.

La Dirección de Tecnologías de la Información o quien haga sus veces debe revisar que los privilegios asignados estén alineados con las necesidades del rol y las responsabilidades del usuario.

8.3.3. **Pantallas limpias**

8.3.3.1. Las estaciones de trabajo fijas y los equipos portátiles, deben tener configurado un estándar de protector de pantalla, de forma que se active ante un determinado tiempo sin uso. De acuerdo con lo indicado en el Reglamento de Seguridad de la Información R-ADI-001.

8.3.3.2. La pantalla de autenticación para el acceso a la red de la entidad debe solicitar únicamente el ID de usuario y la contraseña.

8.3.3.3. Cuando el colaborador se ausente de su lugar de trabajo, debe bloquear su estación de trabajo de tal forma que proteja el acceso a las aplicaciones, servicios de la entidad y archivos.

8.4. Repositorios de la Información

TGI cuenta con los siguientes espacios de almacenamiento para las bases de datos personales:

Almacenamiento	
Forma Almacenamiento	**Lugar de almacenamiento**
Físico	Archivo de gestión centralizado Archivo inactivo
Digital	Laser Fiche, OneDrive, SharePoint Corporativo, Isolución, CGA, SAP, carpetas compartidas

9. POLÍTICA PARA LA SUPRESIÓN DE DATOS PERSONALES

9.1. Ámbito de aplicación

Mediante esta política, TGI mitiga los riesgos legales, financieros y operacionales asociados a la custodia de la información personal, garantizando a los titulares de la información, en los eventos aplicables, la ejecución de aquellas actividades que propendan por la supresión de su información personal de las bases de datos de la Organización.

9.2. Solicitudes de supresión de datos personales

Se consideran solicitudes de supresión de información, sin limitarse a ellas, las siguientes:

9.2.1. Las que realicen los titulares de datos personales en ejercicio de sus derechos sobre la información que de ellos reposa en los archivos físicos o digitales de TGI.

9.2.2. Las que sean solicitadas por los directivos de la Organización.

9.2.3. Las que se soliciten por parte de los líderes de procesos o áreas.

9.2.4. Las que deban realizarse para eliminar archivos históricos que ya cumplieron con su ciclo de vida en la Organización, de acuerdo con la legislación vigente en lo relativo a archivos físicos o digitales y las tablas de retención documental de TGI.

La supresión de la información personal es una exigencia de la ley para datos personales sobre los cuales no se cuente con una finalidad legítima para permanecer almacenados al interior de la Organización. Cuando se eliminen documentos contentivos de datos personales se deberá efectuar un procedimiento que asegure:

9.2.5. El método utilizado deberá impedir la reconstrucción y posterior uso de los datos eliminados.

9.2.6. El método deberá ser seguro y procurar ser amigable con el medio ambiente.

9.2.7. El método podrá seguir estándares establecidos en la costumbre y considerar si se elimina información de carácter física o electrónica. Para tal efecto, se podrán utilizar mecanismos de triturado, pulverización, fusión, incineración, desintegración, sobreescritura, desmagnetización, etc.

9.2.8. La información a eliminar deberá contar con medidas de seguridad que impidan su consulta o copia posterior. Por ejemplo, no estar disponible y/o visible en pasillos, espacios abiertos al público, etc.

9.2.9. Se deberá elaborar un acta de destrucción mediante la cual se haga una referencia general al tipo de información que se está eliminando, el método utilizado, la fecha, identificación y firma de los asistentes.

9.3. Supresión o eliminación de información negativa

Los datos personales que contengan información negativa deberán ser eliminados o suprimidos por parte de TGI dentro de un tiempo prudencial y en proporción a las características y elementos del contenido de la información negativa.

9.4. Vigencia de las Bases de Datos

Las Bases de Datos de TGI tendrán el período de vigencia que corresponda a la finalidad para la cual se autorizó su tratamiento y de las normas especiales que regulen la materia.

9.5. Término de Conservación de los Datos Personales

TGI sólo podrá realizar Tratamiento de los Datos Personales durante el tiempo que sea razonable y necesario de acuerdo con las finalidades que justificaron la recolección, atendiendo a las disposiciones aplicables a la materia que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

Una vez cumplidas las finalidades del Tratamiento y sin perjuicio de las obligaciones legales que requieran lo contrario, TGI deberá proceder a la supresión de los Datos Personales.

Adicionalmente, se deberá proceder a la supresión de los Datos Personales cuando así lo requiera el Titular.

9.6. Supresión solicitada por el Titular

El Titular tiene el derecho a solicitar a TGI la supresión (eliminación) de sus Datos Personales cuando:

9.6.1. Considere que los mismos no están siendo tratados conforme a los principios, deberes y obligaciones previstos en la Ley 1581 de 2012.

9.6.2. Hayan dejado de ser necesarios o pertinentes para la finalidad para la cual fueron recolectados.

9.6.3. Se haya superado el periodo necesario para el cumplimiento de los fines para los que fueron recolectados.

Esta supresión implica la eliminación total o parcial de la información personal de acuerdo con lo solicitado por el Titular en los registros, archivos, bases de datos o tratamientos realizados por TGI.

Es importante tener en cuenta que el derecho de supresión no es absoluto y TGI puede negar el ejercicio del mismo cuando:

9.6.4. El Titular tenga un deber legal o contractual de permanecer en la Base de Datos.

9.6.5. La eliminación de los datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

9.6.6. Los Datos Personales sean necesarios para proteger los intereses jurídicamente tutelados del Titular, para realizar una acción en función del interés público, o para cumplir con una obligación legalmente adquirida por el Titular.

Cuando tenga conocimiento de este tipo de solicitudes debe comunicárselas inmediatamente al Oficial de Protección de Datos Personales de TGI, quien realizará el análisis pertinente y determinará si la eliminación procede.

9.7. Supresión por la terminación de la vigencia legal

Cuando los Datos son tratados en cumplimiento de una obligación legal, estos deberán suprimirse cuando se cumpla el término de conservación requerido por la ley. Los siguientes periodos de conservación han sido dispuestos por la ley:

9.8. Conservación de documentación de los comerciantes

De acuerdo con lo establecido en el artículo 60 del Código de Comercio, los comerciantes tienen la obligación de conservar sus libros y papeles por un periodo de 10 años. Cumplido este término podrá destruirse la información.

La Superintendencia de Sociedades ha precisado que esta obligación comprende los siguientes documentos:

9.8.1. Libros de contabilidad.

9.8.2. De Actas de Asamblea y Juntas Directivas.

9.8.3. De Registro de Accionistas y de socios.

9.8.4. Comprobantes de Contabilidad.

9.8.5. Documentos que justifiquen los comprobantes anteriores.

9.8.6. Los recibos que se expidan.

9.8.7. Los comprobantes de las cuentas.

9.8.8. La correspondencia que guarde relación con los negocios que adelante la sociedad (artículo 51 del Código de Comercio y 123 y 124 del Decreto 2649 de 1993).

Adviértase que la obligación prevista en la norma es la conservación de la información. Lo anterior es relevante porque, desde la perspectiva de las normas de protección de Datos Personales, el único Tratamiento legalmente habilitado conforme a las disposiciones del artículo 60 del Código de Comercio es la conservación. En otras palabras, cualquier Tratamiento distinto al almacenamiento, como la divulgación, circulación y transferencia de la información, entre otros, no tendría Autorización legal por más de 10 años.

9.9. Conservación de la información por obligación de las normas tributarias

La información de soporte y pruebas de las declaraciones presentadas ante autoridades tributarias deberá ser conservada por los periodos previstos en el artículo 632 del Estatuto Tributario, en concordancia con el artículo 46 de la Ley 962 de 2005.

9.10. Conservación de la información por obligación de las normas laborales

De acuerdo con el Código Sustantivo del Trabajo, son obligaciones del empleador: dar al trabajador que lo solicite, a la expiración de contrato, una certificación en que consten el tiempo de servicio, la índole de la labor y el salario devengado; e igualmente, practicarle exámenes de egreso y darle certificación sobre el particular, si el trabajador lo solicita y si al ingreso o durante la permanencia en el trabajo hubiere sido sometido a examen médico.

Adicionalmente, las empresas obligadas al pago de la jubilación deben conservar en sus archivos los datos que permitan establecer de manera precisa el tiempo de servicio de sus trabajadores y los salarios devengados. Cuando los archivos hayan desaparecido o cuando no sea posible probar con ellos el tiempo de servicio o el salario, es admisible para aprobarlos cualquiera otra prueba reconocida por la ley, la que debe producirse ante el juez del trabajo competente, a solicitud escrita del interesado y con intervención de la empresa respectiva.

En consecuencia, TGI deberá conservar la mencionada información de manera que pueda cumplir con las obligaciones del Código Sustantivo del Trabajo.

9.11. Supresión ordenada por autoridad competente

Las autoridades en cumplimiento de alguna función legal pueden ordenar la supresión de cierta información. El principal caso en el que esto se puede presentar es cuando existe una investigación administrativa por parte de la SIC en la que se ordene la eliminación de Datos Personales. En este caso se deben evaluar los méritos señalados por la autoridad para realizar la supresión y proceder a realizar dicha eliminación, en caso de que se considere que está debidamente justificado.