



MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS

Código: MN-GD-001
Fecha de Emisión: nov-03-2021
Versión: 2
Fecha de Modificación: oct-15-2026
Página 1 de 25

1. OBJETIVO

Establecer los lineamientos para la recolección, almacenamiento, uso, circulación, actualización, transmisión, transferencia y supresión de los datos personales tratados por GTC Corporation, garantizando el respeto de los derechos de los titulares, la protección de su privacidad y el cumplimiento de la normativa colombiana vigente en materia de protección de datos personales.

Asimismo, definir las responsabilidades y medidas organizacionales, técnicas y administrativas necesarias para proteger los datos personales contra el acceso, uso, divulgación, pérdida, alteración o tratamiento no autorizado, asegurando que su tratamiento se realice conforme a las finalidades legítimas informadas a los titulares y a los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

2. ALCANCE

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

3. DEFINICIONES

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

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

Base de Datos: Conjunto organizado de datos personales que sea objeto de tratamiento.



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

Dato Público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o del servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.

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

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

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

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

Responsable de Administrar las Bases de Datos: Colaborador encargado de controlar y coordinar la adecuada aplicación de las políticas del tratamiento de los datos una vez almacenados en una base de datos específica; así como de poner en práctica las directrices que dicte el Responsable del tratamiento y el Oficial de Protección de datos.

Oficial de Protección de Datos: Es la persona natural que asume la función de coordinar la implementación del marco legal en protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012.

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

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

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.

Transferencia: La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del tratamiento y se encuentra dentro o fuera del país.

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

4. RESPONSABLE

- **Dirección Administrativa y Financiera:** responsable de promover el cumplimiento de los lineamientos del sistema de seguridad y privacidad de la información, dentro de su ámbito de competencia.
- **Responsable de Seguridad de la Información:** responsable de coordinar el seguimiento a la implementación, cumplimiento y mejora de los controles de seguridad y privacidad de la información.
- **Responsable de TI:** responsable de implementar y mantener los controles tecnológicos de seguridad de la información, de acuerdo con sus funciones.
- **Responsable de Infraestructura:** responsable de aplicar los controles de seguridad relacionados con la infraestructura tecnológica, los servicios y los recursos bajo su administración.
- **Líderes de proceso:** responsables de asegurar el cumplimiento de los lineamientos del manual en sus respectivos procesos.
- **Colaboradores y contratistas:** responsables de cumplir las políticas, procedimientos y controles aplicables a sus funciones y de reportar los incidentes de seguridad de la información que identifiquen.

5. POLÍTICAS

GTC Corporation establece las siguientes políticas de cumplimiento obligatorio para proteger la confidencialidad, integridad y disponibilidad de la información, preservar la privacidad de los datos personales y gestionar los riesgos asociados al uso de los recursos tecnológicos y de inteligencia artificial.

1. **Clasificación y manejo de la información:** toda información deberá identificarse y manejarse de acuerdo con su nivel de confidencialidad, sensibilidad y criticidad, aplicando los controles de acceso, almacenamiento, transmisión y disposición que correspondan.
2. **Control de acceso:** el acceso a la información y a los sistemas deberá concederse de acuerdo con las funciones y responsabilidades autorizadas. No se permitirá compartir credenciales ni utilizar cuentas de otros usuarios.
3. **Gestión de contraseñas y autenticación:** las credenciales deberán ser robustas, individuales y confidenciales. Se deberá utilizar autenticación multifactor cuando esté disponible y sea aplicable, especialmente para accesos privilegiados, remotos y a servicios críticos.
4. **Protección de datos personales:** el tratamiento de datos personales deberá realizarse conforme a las finalidades autorizadas, los principios de protección de datos y la normativa vigente. Se prohíbe el acceso, uso, divulgación o transferencia no autorizados.
5. **Copias de seguridad y recuperación:** las copias de seguridad deberán realizarse con una periodicidad definida según la criticidad de la información, protegerse contra accesos no autorizados y someterse a verificaciones y pruebas de restauración planificadas.

6. **Cifrado y comunicaciones seguras:** la información sensible deberá protegerse mediante mecanismos de cifrado y canales seguros adecuados al riesgo. No se permitirá transmitir información confidencial por medios no autorizados o sin las protecciones requeridas.
7. **Uso de servicios en la nube y terceros:** los servicios tecnológicos y proveedores que procesen información de GTC Corporation deberán evaluarse y gestionarse según los riesgos de seguridad, privacidad y las obligaciones contractuales aplicables.
8. **Desarrollo y mantenimiento seguro:** los cambios en aplicaciones, bases de datos, infraestructura y demás componentes tecnológicos deberán gestionarse de forma controlada. Los desarrollos deberán incorporar prácticas de seguridad acordes con su riesgo, incluyendo revisión de código, gestión de vulnerabilidades y separación de ambientes cuando corresponda.
9. **Gestión de cambios:** los cambios que puedan afectar la seguridad, disponibilidad o integridad de la información deberán evaluarse, documentarse, autorizarse y verificarse antes de su implementación, de acuerdo con el procedimiento establecido.
10. **Registro y monitoreo:** los eventos relevantes de seguridad, accesos, actividades privilegiadas y alertas deberán registrarse y revisarse conforme a los riesgos identificados, las capacidades tecnológicas disponibles y los requisitos de conservación definidos.
11. **Gestión de incidentes:** todo colaborador o contratista deberá reportar oportunamente los incidentes o sospechas de incidentes de seguridad de la información por los canales establecidos. Los responsables deberán gestionar su análisis, contención, recuperación y documentación.
12. **Continuidad del servicio:** los sistemas y servicios críticos deberán contar con medidas de continuidad y recuperación acordes con su importancia para la organización y los compromisos adquiridos con clientes.
13. **Uso responsable de la inteligencia artificial:** las herramientas y soluciones de inteligencia artificial utilizadas en las actividades de GTC Corporation deberán emplearse de manera autorizada y responsable, considerando los riesgos de seguridad, privacidad, confidencialidad, calidad y posibles resultados incorrectos. No se deberá ingresar información confidencial, datos personales o código fuente en herramientas de IA no autorizadas para dicho uso.
14. **Supervisión de resultados de IA:** los resultados generados por herramientas o agentes de inteligencia artificial deberán revisarse por una persona competente antes de utilizarlos en decisiones relevantes, entregables para clientes, cambios de código o actividades que puedan afectar la seguridad, los derechos de las personas o la operación.
15. **Gestión de activos:** los activos de información y tecnológicos deberán identificarse, asignarse a responsables y utilizarse exclusivamente para fines autorizados. Su devolución, reasignación o disposición deberá realizarse de forma controlada.

16. **Confidencialidad y formación:** los colaboradores y contratistas deberán cumplir los compromisos de confidencialidad, recibir orientación sobre sus responsabilidades y aplicar los lineamientos de seguridad y privacidad pertinentes a sus funciones.
17. **Gestión de vulnerabilidades y riesgos:** los riesgos y vulnerabilidades identificados deberán evaluarse, priorizarse y tratarse mediante acciones documentadas, de acuerdo con su impacto y probabilidad de ocurrencia.
18. **Cumplimiento y mejora continua:** las políticas y los controles deberán revisarse periódicamente y cuando se presenten cambios relevantes en los procesos, tecnologías, amenazas, requisitos legales o servicios de la organización. Las excepciones deberán justificarse, evaluarse y contar con la aprobación correspondiente.

6. CONTENIDO

6.1 BASE LEGAL Y ÁMBITO DE APLICACIÓN

La presente política de tratamiento de datos personales de GTC Corporation se establece en cumplimiento de los artículos 15 y 20 de la Constitución Política de Colombia; la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, en especial los literales k) del artículo 17 y f) del artículo 18, relativos a los deberes de los responsables y encargados del tratamiento; y el Decreto 1074 de 2015, en particular las disposiciones del Capítulo 25, que reglamentan parcialmente la citada ley, junto con las demás normas que la modifiquen, adicionen o sustituyan.

Esta política aplica a los datos personales que sean objeto de tratamiento por parte de GTC Corporation, en calidad de responsable o encargado del tratamiento, según corresponda, independientemente del medio o formato en el que se encuentren. Comprende las actividades de recolección, almacenamiento, uso, circulación, actualización, transmisión, transferencia y supresión de datos personales, en el marco de las actividades administrativas, laborales, comerciales, contractuales y operativas de la organización.

Su cumplimiento es obligatorio para los colaboradores, contratistas y demás personas que, por razón de sus funciones o de una relación contractual, tengan acceso a datos personales o intervengan en su tratamiento, sin perjuicio de las obligaciones legales y contractuales aplicables.

	MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS	Código: MN-GD-001
		Fecha de Emisión: nov-03-2021
		Versión: 2
		Fecha de Modificación: oct-15-2026
		Página 7 de 25

Normatividad Aplicable

La gestión de la seguridad y privacidad de la información de GTC Corporation se fundamenta en las disposiciones legales que resulten aplicables a sus actividades, procesos, servicios y obligaciones contractuales.

- Constitución Política de Colombia, especialmente los artículos 15 y 20.
- Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1074 de 2015, en las disposiciones aplicables a la protección de datos personales y al Registro Nacional de Bases de Datos.
- Ley 1273 de 2009, por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”.
- Ley 1266 de 2008, cuando resulte aplicable por la naturaleza de las actividades de tratamiento de información.
- Ley 1712 de 2014, cuando resulte aplicable de acuerdo con la naturaleza de la información y las obligaciones legales correspondientes.
- Circulares, instrucciones y demás disposiciones vigentes de la Superintendencia de Industria y Comercio en materia de protección de datos personales, según corresponda.

6.2 PRINCIPIOS DE LA PROTECCIÓN DE DATOS

De conformidad con el artículo 4 de la Ley Estatutaria 1581 de 2012, GTC Corporation aplicará de manera armónica e integral los siguientes principios en el desarrollo, interpretación y ejecución de las actividades de tratamiento de datos personales. Estos principios orientan las actuaciones de la organización y de las personas que intervienen en dicho tratamiento.

a. Principio de legalidad

El tratamiento de datos personales es una actividad reglada que deberá sujetarse a la Constitución Política de Colombia, la Ley 1581 de 2012, sus disposiciones reglamentarias y las demás normas que las modifiquen, adicionen o sustituyan.



MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS

Código: MN-GD-001
Fecha de Emisión: nov-03-2021
Versión: 2
Fecha de Modificación: oct-15-2026
Página 8 de 25

b. Principio de finalidad

El tratamiento de datos personales deberá responder a una finalidad legítima, específica y acorde con la Constitución y la ley, la cual deberá ser informada al titular. Los datos no podrán utilizarse para finalidades incompatibles con aquellas que fueron informadas, salvo que exista fundamento jurídico para ello.

c. Principio de libertad

El tratamiento de datos personales deberá contar con la autorización previa, expresa e informada del titular, excepto en los casos en que la ley establezca que dicha autorización no es necesaria. La autorización deberá obtenerse por medios que permitan su consulta posterior y deberá conservarse la evidencia correspondiente.

d. Principio de veracidad o calidad

La información personal sometida a tratamiento deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que puedan inducir a error.

e. Principio de transparencia

GTC Corporation garantizará al titular el derecho a obtener, en cualquier momento y sin restricciones, información acerca de la existencia de datos personales que le conciernan y sobre su tratamiento, de conformidad con la normativa aplicable.

Cuando se solicite autorización para el tratamiento, se deberá informar de manera clara y expresa, según corresponda:

- La finalidad del tratamiento y las operaciones a las que serán sometidos los datos personales.
- El carácter facultativo de las respuestas a preguntas relacionadas con datos sensibles o datos personales de niños, niñas y adolescentes.
- Los derechos que le asisten al titular.
- La identificación y los datos de contacto del responsable del tratamiento.

GTC Corporation conservará evidencia del cumplimiento del deber de información y de la autorización, cuando esta sea exigible.

f. Principio de acceso y circulación restringida

El tratamiento de datos personales estará sujeto a los límites establecidos por la Constitución Política, la Ley 1581 de 2012 y las demás normas aplicables. El

acceso y la circulación de los datos deberán limitarse a las personas autorizadas por el titular o habilitadas por la ley, de acuerdo con sus funciones y responsabilidades.

Los datos personales que no tengan naturaleza pública no deberán quedar disponibles en Internet u otros medios de divulgación masiva sin las medidas que permitan restringir su acceso a los titulares y a terceros debidamente autorizados, conforme a la ley.

g. Principio de seguridad

GTC Corporation deberá adoptar las medidas técnicas, humanas y administrativas que sean razonables y necesarias para proteger los datos personales contra su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Las personas que tengan acceso directo o indirecto a datos personales deberán conocer y cumplir las políticas, procedimientos y controles de seguridad aplicables a sus funciones. La organización deberá comunicar las disposiciones pertinentes y sus modificaciones por los canales establecidos.

h. Principio de confidencialidad

Todas las personas que intervengan en el tratamiento de datos personales que no tengan naturaleza pública deberán garantizar la reserva de la información, incluso después de finalizar su relación laboral, contractual o funcional con GTC Corporation.

Los datos personales solo podrán suministrarse o comunicarse cuando ello esté autorizado por el titular, permitido por la ley o corresponda al desarrollo legítimo de las actividades de tratamiento, de conformidad con las disposiciones aplicables.

6.3 AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO

De conformidad con el artículo 9 de la Ley Estatutaria 1581 de 2012, GESTIÓN TECNOLÓGICA & CONTABLE S.A.S. (GTC Corporation), en calidad de responsable del tratamiento cuando corresponda, solicitará la autorización previa e informada del titular para el tratamiento de sus datos personales, salvo en los casos expresamente exceptuados por la ley.

La autorización deberá obtenerse por un medio que permita su consulta posterior y deberá conservarse la evidencia correspondiente. Antes de solicitarla, GTC

Corporation informará al titular, de manera clara y expresa, las finalidades del tratamiento, sus derechos y los demás aspectos exigidos por la normativa vigente.

La entrega de datos personales o el conocimiento de esta política no se entenderán, por sí solos, como autorización para cualquier tratamiento. La autorización deberá corresponder a las finalidades informadas y a las condiciones legalmente aplicables.

Casos en los que no se requiere autorización del titular

De acuerdo con el artículo 10 de la Ley 1581 de 2012, no será necesaria la autorización del titular cuando el tratamiento corresponda a alguno de los siguientes casos:

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

En todos los casos en que se exceptúe la autorización, GTC Corporation deberá cumplir las demás disposiciones aplicables en materia de protección de datos personales y adoptar las medidas necesarias para garantizar su tratamiento adecuado.

6.4 RESPONSABLE DEL TRATAMIENTO

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S. (GTC Corporation) actúa como responsable del tratamiento de los datos personales comprendidos en esta política, en aquellas actividades en las que determina las finalidades y los medios del tratamiento, de conformidad con la Ley 1581 de 2012 y las demás disposiciones aplicables.

Los titulares de los datos personales podrán comunicarse con la organización a través de los siguientes canales:

- **Razón social:** GESTIÓN TECNOLÓGICA & CONTABLE S.A.S.
- **Dirección:** Carera 100 No. 5 – 169 Oficina 723B, Ciudadela Comercial Unicentro , Las Vegas, Cali, Valle del Cauca, Colombia.
- **Correo electrónico:** protecciondedatos@gtccorporation.com

- **Teléfono:** 601 915 81 99 - 310 428 4784.

Estos canales estarán disponibles para atender las solicitudes relacionadas con el tratamiento de datos personales, incluidas las consultas y los reclamos presentados por los titulares, conforme a los procedimientos y términos establecidos en la normativa vigente.

6.5 TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S. (GTC Corporation), en el desarrollo de sus actividades empresariales, realiza operaciones de tratamiento de datos personales de personas naturales, tales como recolección, almacenamiento, uso, circulación, actualización, transmisión, transferencia y supresión, de acuerdo con las finalidades legítimas, específicas e informadas que correspondan a cada actividad, en cumplimiento de la Constitución Política de Colombia, la Ley 1581 de 2012 y las demás disposiciones aplicables.

Las bases de datos utilizadas por la organización deberán contar con finalidades identificadas y documentadas, y su tratamiento deberá limitarse a dichas finalidades o a aquellas que cuenten con fundamento jurídico válido. Cuando se requiera autorización del titular, esta deberá obtenerse y conservarse conforme a la normativa vigente.

El **Anexo 1. MT-GD-002 – Matriz de Organización de Bases de Datos** identifica las bases de datos bajo responsabilidad de GTC Corporation y documenta las finalidades asociadas a su tratamiento. Esta matriz deberá mantenerse actualizada de acuerdo con los cambios en los procesos, las actividades de tratamiento y las obligaciones legales aplicables.

6.6 DERECHOS DE LOS TITULARES

De conformidad con el artículo 8 de la Ley Estatutaria 1581 de 2012 y las disposiciones reglamentarias aplicables del Decreto 1074 de 2015, los titulares de datos personales podrán ejercer los derechos relacionados con el tratamiento de su información. Estos derechos podrán ser ejercidos por:

1. El titular, previa acreditación de su identidad por los medios dispuestos por GTC Corporation.
2. Sus causahabientes, previa acreditación de tal calidad.
3. El representante legal o apoderado del titular, previa acreditación de la representación o del poder correspondiente.
4. Las personas autorizadas por el titular o habilitadas por la ley, en los casos que corresponda.

Los derechos de los niños, niñas y adolescentes serán ejercidos por quienes estén legalmente facultados para representarlos, respetando su interés superior y sus derechos fundamentales.

a. Derecho a conocer, actualizar y rectificar los datos personales

El titular podrá conocer los datos personales que sean objeto de tratamiento, solicitar su actualización y rectificación cuando sean parciales, inexactos, incompletos, fraccionados, induzcan a error o su tratamiento esté prohibido o no haya sido autorizado.

b. Derecho a consultar sus datos personales y conocer su uso

El titular podrá solicitar información sobre la existencia de datos personales que le conciernan, acceder a ellos y conocer el uso que GTC Corporation les ha dado, de conformidad con los procedimientos y términos establecidos en la normativa vigente.

c. Derecho a solicitar prueba de la autorización

El titular podrá solicitar prueba de la autorización otorgada para el tratamiento de sus datos personales, excepto en los casos en que la ley establezca que dicha autorización no es necesaria.

d. Derecho a presentar consultas y reclamos

El titular podrá presentar consultas y reclamos ante GTC Corporation para ejercer sus derechos y solicitar la protección de sus datos personales.

Los reclamos podrán tener, entre otras, las siguientes finalidades:

- **Actualización o rectificación:** solicitar la corrección o actualización de datos personales inexactos, incompletos, desactualizados o que induzcan a error.
- **Supresión:** solicitar la eliminación de los datos personales cuando se cumplan las condiciones legales para ello.
- **Revocación de la autorización:** solicitar que se deje sin efecto la autorización para el tratamiento, cuando legalmente proceda.
- **Incumplimiento de obligaciones:** poner en conocimiento de GTC Corporation presuntos incumplimientos de la normativa de protección de datos personales y solicitar que se adopten las medidas correspondientes.

La supresión de datos y la revocación de la autorización estarán sujetas a las condiciones y excepciones previstas en la ley, incluidas las obligaciones legales o contractuales de conservación que resulten aplicables.

e. Derecho a presentar quejas ante la Superintendencia de Industria y Comercio

El titular o sus causahabientes podrán presentar quejas ante la Superintendencia de Industria y Comercio (SIC) por presuntas infracciones a la Ley 1581 de 2012 y demás disposiciones aplicables, una vez se haya agotado el trámite de consulta o reclamo ante el responsable o encargado del tratamiento, según corresponda.

f. Derecho a revocar la autorización o solicitar la supresión de los datos

El titular podrá solicitar la revocación de la autorización y/o la supresión de sus datos personales cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La procedencia de estas solicitudes estará sujeta a las condiciones establecidas en la Ley 1581 de 2012 y sus normas reglamentarias.

6.7 SOLICITUD DE AUTORIZACIÓN AL TITULAR DEL DATO PERSONAL

Con antelación y/o al momento de efectuar la recolección del dato personal, GESTIÓN TECNOLÓGICA & CONTABLE S.A.S solicitará al Titular del dato su autorización para efectuar su recolección y tratamiento, indicando la finalidad para la cual se solicita el dato, utilizando para esos efectos medios técnicos automatizados, escritos u orales, que permitan conservar prueba de la autorización y/o de la conducta inequívoca descrita en el artículo 2.2.2.25.2.2. sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 7 del Decreto 1377 de 2013).

6.8 TRATAMIENTO DE DATOS DE MENORES

De acuerdo con el artículo 7° de la Ley 1581 de 2012, el Tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo lo dispuesto en el artículo 2.2.2.25.2.9 sección 2 del capítulo 25 del Decreto 1074 de 2015 (Artículo 12 del Decreto 1377 de 2013) y en cumplimiento de los siguientes parámetros y requisitos:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, GESTIÓN TECNOLÓGICA & CONTABLE S.A.S solicitará al representante legal del niño, niña o adolescente la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. El Responsable y Encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, aplicando los principios y obligaciones establecidos en la Ley 1581 de 2012 y normas reglamentarias.

6.9 ATENCIÓN A LOS TITULARES DE DATOS

El Oficial de Protección de Datos de GESTIÓN TECNOLÓGICA & CONTABLE S.A.S será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Teléfono: 310 4284784. Correo electrónico: protecciondedatos@gtccorporation.com.

6.10 PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR

Derecho de acceso o consulta

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

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

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

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a GESTIÓN TECNOLÓGICA & CONTABLE S.A.S enviado, mediante correo electrónico a: protecciondedatos@gtccorporation.com, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a Carera 100

No. 5 – 169 Oficina 723B, Ciudadela Comercial Unicentro , Las Vegas, Cali, Valle del Cauca, Colombia. La solicitud deberá contener los siguientes datos:

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

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

- Visualización en pantalla.
- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por GESTIÓN TECNOLÓGICA & CONTABLE S.A.S.

Una vez recibida la solicitud, GESTIÓN TECNOLÓGICA & CONTABLE S.A.S resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

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

Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a GESTIÓN TECNOLÓGICA & CONTABLE S.A.S enviado, mediante correo electrónico a protecciondedatos@gtccorporation.com, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a Carera 100 No. 5 – 169 Oficina 723B, Ciudadela Comercial Unicentro , Las Vegas, Cali, Valle del Cauca, Colombia. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que

lo representa, así como del documento acreditativo de tal representación.

- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

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

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

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

6.11 MEDIDAS DE SEGURIDAD

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

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

A continuación, se exponen las medidas de seguridad implantadas por GESTIÓN TECNOLÓGICA & CONTABLE S.A.S que están recogidas y desarrolladas en su PL-GI-002 Políticas Internas de Seguridad (Tablas I, II, III y IV).

TABLA I: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) y bases de datos (automatizadas, no automatizadas)	
Gestión de documentos y soportes	1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable de Administrar las bases de datos para la salida de documentos o soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.
Control de acceso	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado
Incidencias	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento de notificación y gestión de incidencias.
Personal	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos. 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre el personal de las normas y de las consecuencias del incumplimiento de las mismas.
Manual Interno de Seguridad	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, identificación de los encargados del tratamiento.
TABLA II: Medidas de seguridad comunes para todo tipo de datos (pública, privada, confidencial, reservada) según el tipo de bases de datos	
Bases de datos no automatizadas	
Archivo	1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta, que permitan el ejercicio de los derechos de los Titulares.
Almacenamiento de documentos	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.
Custodia de documentos	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.
Bases de datos automatizadas	
Identificación y autenticación	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación y caducidad.
Telecomunicaciones	1. Acceso a datos mediante redes seguras.

TABLA III: Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos no automatizadas	
Auditoría	1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento.
Responsable de seguridad	1. Designación de uno o varios Administradores de las bases de datos. 2. Designación de uno o varios encargados del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del Responsable del tratamiento en los Administradores de las bases de datos.
Manual Interno de Seguridad	1. Controles periódicos de cumplimiento.
Bases de datos automatizadas	
Gestión de documentos y soportes	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.
Control de acceso	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.
Identificación y autenticación	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados. 2. Mecanismos de cifrado de datos para la transmisión.
Incidencias	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IV: Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas	
Control de acceso	1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados. 4. Destrucción que impida el acceso o recuperación de los datos.
Almacenamiento de documentos	1. Archiveros, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas. 2. Medidas que impidan el acceso o manipulación de documentos almacenados de forma física.
Bases de datos automatizadas	
Control de acceso	1. Sistema de etiquetado confidencial.
Identificación y autenticación	1. Mecanismos de cifrado de datos para la transmisión y almacenamiento.
Almacenamiento de documentos	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede 2. Control del registro de accesos por el responsable de seguridad. Informe mensual.
Telecomunicaciones	1. Acceso y transmisión de datos mediante redes electrónicas seguras. 2. Transmisión de datos mediante redes cifradas (VPN).

6.12 COOKIES O WEB BUGS

Este sitio web no utiliza cookies o web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página web. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página web, con el fin de darle mejor servicio en la página.

Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador (Internet Explorer, Firefox, Safari, Chrome, entre otros), e inhabilitando el código Java Script del navegador en la configuración de seguridad.

La mayoría de los navegadores web permiten gestionar sus preferencias de cookies, sin embargo, se debe tener en cuenta que si elige bloquearlas puede afectar o impedir el funcionamiento de la página. Así mismo, uno de los servicios de terceros que se pueden llegar a utilizar para seguir la actividad relacionada con el servicio, p.ej. es Google Analytics, por lo que, en caso de no desear que

se obtenga y utilice información, puede instalar un sistema de rechazo ("opt-out") en su navegador web, como es: tools.google.com/dlpage/gaoptout?hl=None.

6.13 PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S establece un procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad.

Los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

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

- Cuando una persona tenga conocimiento de una incidencia (perdida, hurto y/o acceso no autorizado) que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa o alguno de los Encargados deberá comunicarlo, de manera inmediata, al Oficial de Protección de Datos, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.
- Una vez comunicada la incidencia ha de solicitar al Oficial de Protección de Datos un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.
- GESTIÓN TECNOLÓGICA & CONTABLE S.A.S, crea un registro de incidencias que debe contener: el tipo de incidencia (Fraude Interno o externo, Daños a activos físicos, Fallas tecnológicas, Ejecución y administración de procesos), fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el Oficial de Protección de Datos, remitirse al FO-GI-005 Registro de incidencias.
- Asimismo, debe implementar los procedimientos para la recuperación de los datos cuando aplica, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.
- Adicional, el Oficial de Protección de Datos debe informar a la Superintendencia de Industria y Comercio, mediante el RNBD dentro de los 15 días hábiles siguientes de haber sido detectado.
- Finalmente, GESTIÓN TECNOLÓGICA & CONTABLE S.A.S notificará del incidente a los Titulares, cuando se identifique que puedan verse afectados de manera significativa.

6.14 ADMINISTRACIÓN DE RIESGOS ASOCIADOS AL TRATAMIENTO DE LOS DATOS

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S ha identificado riesgos relacionados con el tratamiento de los datos personales y establecidos controles con el fin de mitigar sus causas, mediante la implementación de la PL-GI-002 Políticas Internas de Seguridad. Por ello, establecerá un sistema de gestión de riesgos junto con las herramientas, indicadores y recursos necesarios para su administración, cuando la estructura organizacional, los procesos y procedimientos internos, la cantidad de base datos y tipos de datos personales tratados por la organización se consideren que están expuestos a hechos o situaciones frecuentes o de alto impacto que incidan en la debida prestación del servicio o atenten contra la información de los titulares.

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

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

GESTIÓN TECNOLÓGICA & CONTABLE S.A.S en el sistema de gestión de riesgo implementará las medidas de protección para evitar o minimizar los daños en caso de que se materialice una amenaza.

6.15 ENTREGA DE DATOS PERSONALES A LAS AUTORIDADES

Cuando por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial se soliciten a GESTIÓN TECNOLÓGICA & CONTABLE S.A.S acceso y/o entrega de datos de carácter Personal contenidos

en cualquiera de sus bases de datos, se verificará la legalidad de la petición, la pertinencia de los datos solicitados en relación con la finalidad expresada por la autoridad, y se suscribirá acta de la entrega de la información personal solicitada, precisando la obligación de garantizar los derechos del Titular, tanto al funcionario que hace la solicitud, a quien la recibe, así como a la entidad requirente.

6.16 TRANSFERENCIA DE DATOS A TERCEROS PAÍSES

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

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

Se debe tener en cuenta que, en los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales.

Las transmisiones internacionales de datos personales que se efectúen entre GESTIÓN TECNOLÓGICA & CONTABLE S.A.S y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales."

6.18 TRATAMIENTO DE DATOS BIOMÉTRICOS

Los datos biométricos almacenados en las bases de datos son recolectados y tratados por motivos estrictamente de seguridad, para verificar la identidad personal y realizar control de acceso a los empleados, clientes y visitantes. Los mecanismos biométricos de identificación capturan, procesan y almacenan información relacionada con, entre otros, los rasgos físicos de las personas (las huellas dactilares, reconocimiento de voz y los aspectos faciales), para poder establecer o “autenticar” la identidad de cada sujeto.

La administración de las bases de datos biométrica se ejecuta con medidas de seguridad técnicas que garantizan el debido cumplimiento de los principios y las obligaciones derivadas de Ley Estatutaria en Protección de Datos asegurando además la confidencialidad y reserva de la información de los titulares.

6.19 REGISTRO NACIONAL DE BASES DE DATOS - RNBD

El término para registrar las bases de datos en el RNBD será el establecido legalmente. Asimismo, de acuerdo con el artículo 12 del Decreto 886 de 2014, los Responsables del Tratamiento deberán inscribir sus bases de datos en el Registro Nacional de Bases de Datos en la fecha en que la Superintendencia de Industria y Comercio habilite dicho registro, de acuerdo con las instrucciones que para el efecto imparta esa entidad. Las bases de Datos que se creen con posterioridad a ese plazo deberán inscribirse dentro de los dos (2) meses siguientes, contados a partir de su creación.

6.20 SEGURIDAD DE LA INFORMACIÓN Y DATOS PERSONALES

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

Asimismo, garantizamos que en la recolección, almacenamiento, uso y/o tratamiento, destrucción o eliminación de la información suministrada, nos apoyamos en herramientas tecnológicas de seguridad e implementamos prácticas de seguridad que incluyen: transmisión y almacenamiento de información sensible a través de mecanismos seguros, uso de protocolos

seguros, aseguramiento de componentes tecnológicos, restricción de acceso a la información sólo a personal autorizado, respaldo de información, prácticas de desarrollo seguro de software, entre otros.

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

6.21 GESTIÓN DE DOCUMENTOS

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

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

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

Los documentos tanto físicos como digitales que contengan datos personales, deben ser protegidos por agentes externos o internos que puedan alterar su

contenido, siguiendo los lineamientos descritos en el PL-GI-002 Políticas Internas de Seguridad.

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

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

7. ANEXOS

PL-GI-002 Políticas Internas de Seguridad

FO-GI-005 Registro de incidencias

8. NOTAS DE CAMBIO.

VERSIÓN INICIAL	IDENTIFICACIÓN DEL CAMBIO	VERSIÓN FINAL
01	Actualización integral del Manual del Sistema para la Seguridad y Privacidad de la Información. Se revisaron y actualizaron los lineamientos de seguridad de la información y protección de datos personales, las responsabilidades, los controles de seguridad, la gestión de incidentes y las medidas de protección de la información.	02

9. ELABORACIÓN Y APROBACIÓN DEL DOCUMENTO

Revisión:  Mónica Bastidas C.	Aprobación:  Jair Lucumi O.
Cargo: Directora de procesos	Cargo: Gerente